2022

The Evolving Challenges, Issues of Cybercrime, Law Enforcement Personnel, Preparedness, and Training

EILEEN VICTORIA MARTIN
Walden University

Walden University

College of Health Sciences and Public Policy

This is to certify that the doctoral dissertation by

Eileen Victoria Martin

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. David Milen, Committee Chairperson,
Public Policy and Administration Faculty

Dr. Donald McLellan, Committee Member,
Public Policy and Administration Faculty

Dr. Mark Gordon, University Reviewer,
Public Policy and Administration Faculty

Chief Academic Officer and Provost
Sue Subocz, Ph.D.

Walden University
2022

Abstract

The Evolving Challenges, Issues of Cybercrime, Law Enforcement Personnel, Preparedness, and Training

by

Eileen Victoria Martin

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Public Policy and Administration

Walden University

November 2022

Abstract

Cybercrime is an escalating phenomenon recognized by law enforcement personnel and others as a serious ever-increasing problem. The need is critical to equip police with cybercrime preparedness to combat and eradicate the problem. Cyber-attacks have negatively impacted the growing epidemic needing constructive solutions. The police personnel's experiences provided essential cybercrime preparedness, acquired in diverse locations, and applied in the workplace with preventive cybercrime recommendations. Moustakas provided the overall design with theoretical underpinnings of the cybercrime phenomenon with a scientific design. The sample size was eight participants who met the inclusion criteria with the underlying principles of Kolb's experiential learning theory incorporating van Kaam's extensive seven-step Modified data analyses. The inclusion required the personnel eighteen or older, a current employee, a contractual individual, or a volunteer for an agency with cybercrime preparedness. Police personnel included one captain, one lieutenant, two sergeants, one officer, one civilian, one police assistant patrol officer, and one volunteer police college intern. The data was systematically evaluated with an analysis of each research question. The literary gap was closed focusing on cybercrime preparedness enhanced by learning styles transitioning from theoretical to pragmatic. Valuable evidence-based contributions emerged to combat cybercrime with in-depth insight into critical infrastructure strategies. Additional research will assist individuals, agencies, and others to bring positive social change, mitigate cyber-attacks, and uproot cyber-terrorism with transferability.

.

The Evolving Challenges, Issues of Cybercrime, Law Enforcement Personnel, Preparedness, and Training

by

Eileen Victoria Martin

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Public Policy and Administration

Walden University

November 2022

Dedication

I acknowledge and express my sincere gratitude first and foremost to God Almighty and His Son Jesus Christ who has always guided and directed my footsteps. Through the guidance of the Holy Spirit, I am led and comforted, understanding I am protected by a host of angels. I am dedicated and determined to be always about the Father's business in all things as an obedient child of the King. I thank Jesus through the Holy Spirit for His ongoing wisdom, knowledge, and understanding in guiding me throughout this doctoral dissertation journey. I am truly grateful for my husband, Quinnon L. Martin Jr., who has constantly supported and encouraged me. I am thankful and provide special thanks and sincere appreciation for the leadership, encouragement, and dedication of my doctoral chair, Dr. David P. Milen. The strength and support were further rendered by my advisor, Dr. LaToya A. Johnson, and my committee member, Dr. Donald McLellan. I render genuine thanks to my mom, Minister Frances Helen Petty, three sisters: Minister Jeanne M. Roper, Missionary Minister Darlene D. Coursey, and Minister Sharon F. Petty, one brother, Elder Michael J. Petty, as well as Assistant Pastor Lynnice Y. Martin, Emeritus Assistant Pastor-Reverend Tammi M. R. Long, Minister Sakina Q. Griggs, and Minister Michelle A. Martin. A special thanks to Minister Earl Perry, Ministers Joaquin & Dianca Gouch, Minister Diontay Marshall, Dr. Lakisha Holified, M.D., Roderick Marshall, Alexander Long, Ed Long, Xavier Martin, Christian Martin, Courtney & Joshua Comer, Rebekah C. Long, Alva Ivory, Theresa Foster, and the CVFGI Cathedral family who always supported.

Acknowledgments

I cannot articulate the ongoing thanks, encouragement, and inspiration rendered by my Chairperson, Dr. David P. Milen, who guided and directed me with overwhelming wisdom and scholarly leadership on this long journey. I was blessed and privileged to experience the assistance of my committee member Dr. Donald McLellan, my Advisor Dr. La Toya A. Johnson, and Senior Core URR, Dr. Mark Gordon. I have experienced exciting, enriched, and energetic educational learning throughout this dissertation. I Praise God for my husband, Quinnon L. Martin Jr., family members, and the CVFGIC Congregation. I acknowledge with great gratitude my seven children, family, friends, associates, and congregational members throughout the world who constantly encouraged and assisted me. I Praise God for my students and affiliates who displayed their love, prayers, compassion, and support with continual encouragement.

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction to Study

Introduction

The complicity of cybercrime is growing in frequency and severity as countries attempt to defend infrastructures and networks (Jensen, 2012). Cybercrime has escalated with greater prevalence and awareness since 911 and the Internet has developed into a critical and essential need transforming our entire global nation. Holt (2013) expressed those cybercriminals have penetrated mobile devices, bank accounts, and credit cards. The Internet has increased rapidly resulting in counteractive revolutionary cyber transitions against victims, allowing the exploitation of illegal digital technology. It has redesigned our nation in all rudiments of communication, information systems, and power plants. Technological transactions have opened doors to procreate a wealth of knowledge as computer crimes escalate. The Internet and digital divide challenges have altered the landscape of techno-crime (PERF, 2014). A major concern of cybercrime and law enforcement personnel focuses on the expanded cost to the international economy.

Poonia (2014) asserted that cybercrime challenges are theoretical and pragmatic and a relatively new subject for researchers as it grows exponentially (p.119). The aim of the empirical qualitative study was undertaken to better understand the phenomenon of cybercrime, the lived experiences of police personnel preparedness, and the training to mitigate and uproot cybercrime. The study aligned Kolb's (1984) experiential learning theory (ELT) utilized as an underlying principle. The study analyzed perceptions of law enforcement personnel's cybercrime preparedness and learning. I delved into the essence of in-depth lived experiences illuminating cybercrime preparedness and techniques.

The research focused on the learned experiences of the law enforcement personnel, ideas, and reflections utilizing critical thinking and assessing cybercrime in comprehensive descriptions. McLeod (2013) expressed that Kolb's experiential learning ensured the designed practices were implemented in ways that offered diverse styles, especially for individuals to understand complexities in the best needed integrated skills.

Complex cybercrime problems and preparedness are dynamic aligning adult learning principles that demonstrated Kolb's (1984) theory of experiential learning. The cognitive ELT learning cycle provided rich interconnected information. I encouraged police personnel to openly express comments experienced in the learning environment of cybercrime preparedness. Experiential learning and comprehension were key components in law enforcement personnel preparedness. The study required job-related mastery to align plans to combat cybercrime. I integrated Kolb's (1984) Experiential Learning Theory (ELT) as a blueprint and an integrated foundation.

Cybercrime

Today, perilous attacks of cybercrime are on the rise due to the interconnectivity of the World Wide Web and the transitional operations of technology in cyberspace. The cloud allows extensive problems to escalate daily in the world of cyberspace. Law enforcement personnel are experiencing multiple difficulties attempting to contend with the steadfast escalating cybercrime problems (Siegel & Worrall, 2012). The lack of cyber-security and weak firewalls perpetuate critical issues, which expand cybercrime opportunities for breaches. The Department of Homeland Security (2016) argued that law enforcement performed critical work in achieving USA's cyber-security components,

especially investigating the plethora of cybercrimes, including identity theft, fraud, child exploitation, apprehension, investigation, and prosecution of responsible persons (p. 5). Local police personnel are the frontline responders and often the first individuals notified regarding cybercrime. They share facts with the Federal Bureau of Investigation (FBI). The FBI protects the USA against all cyber-based attacks and high-tech crimes, upgrades technology, and provides cybercrime information to local police personnel (Dempsey & Forst, 2013). The FBI manages an Internet site with a great amount of cybercrime data.

November 2018 emanated the largest cybercrime breach of 400 million that compromised data from the Marriot Hotel. Another data breach occurred at Target in 2014 where 40 million credit cards affected 70 million customers. JPMorgan experienced the hacking of 100 million and the following year 56 million customers were breached at Home Depot (McMahon et al., 2016). On June 4, 2015, the federal government's Office of Personnel Management (OPM), with oversight of individual background security clearance investigations, was hacked and experienced a data breach impacting 22.1 million Americans. The outcome resulted in millions of dollars in recovery costs shouldered by taxpayers (Moshiri, 2015). Other cybercrime data breaches were Neiman Marcus, T.J. Maxx, Michaels, Sally Beauty, Bank of America, Chase Bank, and other major corporations. Police department websites were also hacked, including a February 2012 intrusion where the Boston Police Department's website was taken offline. A few days later the Dallas Police Department received a cyber-attack where law enforcement officers' personal data was stolen (Dallas-NBC-FW, 2012).

There are endless cybercrimes occurring and the stolen data serve as tools and targets that result in multiple challenges for local law enforcement personnel. Cybercrime preparedness and training are critical needs to understand the lived experiences of law enforcement personnel in the acceleration of the cybercrime phenomenon. Jeffray (2015) affirmed that most crimes now have a technological component. The everyday basic cybercrimes are on the rise affecting the public in multiple complex ways. The study was quite easy to access on the Internet, which emanated revolutionary transitions to humanity and global systems. Cybercrime has opened the door to extensive criminal aberrations.

The technology and Kolb's (2014) experiential learning theory (ELT) established opportunities for rich data collected from law enforcement personnel who described their cybercrime preparedness and achievements. The study assisted in enlightening the participants regarding their prior cybercrime learned experiences. Noe (2010) asserted that learners link their learned capabilities to what they learned previously and what was encountered during the training process. The ELT cycle evoked and inculcated the participants' thoughts, skills, and creative ideas helping to reflect on cybercrime preparedness. The experiential learning theory served as a theoretical component to equip and build a foundation for the ideas of the police personnel concerning their prior cybercrime preparedness. Kolb's (1984) learning cycle theory, illustrated in Figure 1, entails taking stock of what is transpiring. I reflected on ideas or abstract notions needed to cognitively think and mentally conceptualize the training and responses essential to understanding the new cybercrime information. The law enforcement personnel utilized

what they previously knew from experience and how the learning process was applied.

Figure 1

The Learning Cycle

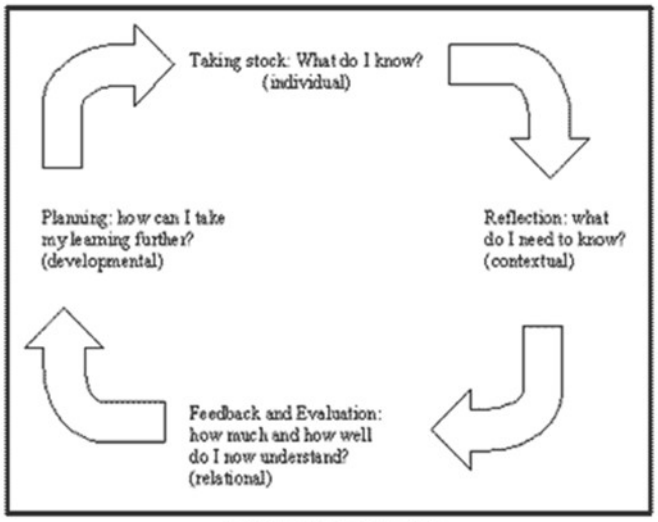


Figure 1: the learning cycle

Note. "From Experiential Learning: Experience as the Source of Learning,' by D.A. Kolb, 1984. (https://www.researchgate.net/.../235701029_Experiential_Learning), Copyright 1984. Reprinted with permission.

Kolb's (1984) learning theory is a four-stage basic learning cycle; often referred to as a training cycle, both meaningful and practical. The learning model was developed by asking the following questions: What do I know (individual)? What do I need to know (conceptual)? How much and how well do I need to understand (relational)? How can I take my learning further (developmental)? Kolb's (1984) basic learning cycle was developed to become the experiential learning theory (ELT). The design offered opportunities to understand the diverse learning styles of the participants; to explain

the cycle of experiential learning; and build on the structure to underpin the learning activities. It would fully apply to the ELT practical applications (Kolb, 1984).

The law enforcement personnel in cybercrime preparedness consisted of trainers, instructors, and professors. Self-taught and different training endeavors were utilized including many electronic devices (DVDs, CDs, Google, ZOOM, e-learning, iPods, simulations, mock applications, desktops, and virtual reality books). They were incorporated into the experiential learning process of the police personnel in cybercrime preparedness. Kolb's (1984) ELT was a meaningful concept for understanding the cognitive learning, reflective processing, and active behavior of law enforcement personnel. The process assisted in understanding prior cybercrime preparedness and experiential learning. The study encapsulated the duplicity of cyber-attacks and identified the escalating cybercrime victims.

Everyday cybercrime preparedness and training require qualified law enforcement personnel who have heightened their cybercrime skills and knowledge through interdisciplinary learning experiences and with industrious applications in the workplace. The ELT cyclic learning styles of Kolb (1984) are useful concepts; embraced in the understanding of diverse learning behaviors that could execute efficient cybercrime preparedness. The research can enhance training, problem-solving, and decision-making. The skills can serve to educate and assist police personnel, agencies, and cybercrime victims. The ubiquitous cybercrime information could assist in the constant challenges of cyber-attacks.

Cybercrime Challenges

Multiple businesses are victimized, and many cyber-attacks are not reported to law enforcement. Electrical grids and water supply systems can become totally dysfunctional through cyber-attacks. According to McCuster (2006), the world is more vulnerable than individuals recognize due to the type, quantity, information increase, and amount of cybercrime floating in cyberspace. Individuals are often not cognizant of the widespread cybercrime vulnerabilities and ulterior systematic technologies. Astronomical cyber fraud is intensified daily. Cybercrime entails the gathering of cyber knowledge and the illegal acquisition of data. Many USA infrastructures rely on the Internet and are compromised with the infiltration of cyber-terrorist attacks via the denial of service (DOS), a technique perfected by many hackers. Holt & Bossler (2013) stated, "Cybercrime has created substantial challenges for law enforcement, particularly at the local level" (p. 464). Police were often not prepared to handle the cybercrime transitions due to evolving technologies and the advanced ever-increasing illegal cyber complicities.

Cybercrime and its compelling challenges increase exponentially and there is difficulty in proficiently equipping and preparing law enforcement personnel (Berg, 2007; Siegel & Worrall, 2014). Cybercrime activities represent a wide range of growth in the escalating criminal offenses and adverse cyber-technologies that possess formative flexibilities that tap the worldwide global community. Corporations often do not desire customers to know that intrinsic data has been compromised; they work to conceal and covertly hide the data breach information within their individual powers (Sales, 2015). Cybercrime and cyber terrorism are difficult to detect, and cyber thieves conspire to

utilize computers in negative complicit ways. Despite ongoing cybercrime, it is difficult utilizing obsolete law enforcement methods (Gandhi, 2012). Cybercrimes are explosive, growing, and intensifying throughout the world. Since 2010 Internet crime has risen approximately 78% a year with more sophisticated attacks and favored cybercriminal approaches utilizing ransomware and spear-phishing (Smart, 2015).

Cybercrime continues to grow to employ innovative strategies. The control of data is shared as people and systems become more cyber-dependent in all aspects of life (Flory, 2016). Cybercrime is internationally global in nature; is not hindered by international boundaries. An attack on the USA cyber systems infrastructure and networks can implement critical devastation. A perilous catastrophic cybercrime attack could destroy the USA, resulting in the inoperable military, health care systems, educational facilities, and government entities. The Internet has become a major component in everyday life as cybercrime snowballs. Police personnel must be prepared and equipped to combat cybercrime issues (Barnett et al., 2011).

The computer era has evoked new methods, devices, and technological tools. The techniques and cybercrime systems expand daily. They are quite different from the procedures utilized by law enforcement in investigating crimes in the past (Davis, 2010). The egregious growth of cybercrime escalates each day due to the worldwide technological expansion and has no signs of diminishing. It further demands police (who are lagging somewhat behind) must become more skilled and knowledgeable to implement and overtake the emerging illegal cyber-schemes (Flory, 2016). Law enforcement personnel has emphasized that cybercrime preparedness is preeminent.

Stambaugh et al. (2000) expressed a great need to maximize police personnel with on-site training, new tools, and research focused on innovative electronic techno-crime with cyber-terrorism initiatives.

Statement of the Problem

Cybercrime is an escalating phenomenon recognized by law enforcement personnel as a serious ever-increasing comprehensive problem. Notwithstanding the need is to efficiently equip, educate, and inform law enforcement personnel in cybercrime preparedness to combat, mitigate, and eradicate the problem. Cybercrime has negatively impacted police personnel, corporations, medical, and citizens as cybercrime remains a great daily escalating trajectory becoming an epidemic needing a solution. The failure of the increased cybercrime knowledge of law enforcement personnel could be a cause of the problems or perhaps due to the preparedness and training. Experiential learning, cybercrime preparedness, and effective performance are essential. Training has much significance and value that requires the mastery of job-related competencies. The skilled knowledge of comparative behaviors is necessary to build and maintain effective work-and-job-related skills (Saks & Burke-Smalley, 2014). Perhaps a phenomenological qualitative study using Kolb's (1984) Experiential Learning Theory as a blueprint might systematically view the experiences of police personnel and cybercrime challenges. The research investigates and analyzes cybercrime preparedness.

According to Poonia (2014), there are pros and cons to the changes of cybercrime, such as the lack of trained law enforcement and cyber security not being equipped to address high-tech crimes. In addition, implementing countermeasures with limited

budgets result in challenges for cyber-security and law enforcement training (p. 120). There are ongoing problems and behaviors that intensify the failure to equip and prepare police personnel to combat and mitigate the phenomenon in question. Although there is an increase in cybercrime, it is difficult to detect the exacerbation of cyber-attacks through the older archaic police channels; and this problem has negatively affected all areas of the organizations (Cybercrime Statistics, 2014; Hinduja, 2007; Wall, 2008).

Americans are defrauded annually out of billions of dollars while cybercriminals walk unidentified in total anonymity. The empirical qualitative phenomenological study encompassed Kolb's (1984) Experiential Learning Theory (ELT) in conjunction with Moustakas (1994) and the other theorists. The research included cognitive cybercrime preparedness aligning the arrangements, classifications, and taxonomies. It focused on being equipped and trained in cybercrime preparedness. The study logistically examined the law enforcement personnel's prior cybercrime preparedness, learning styles, and experiences. The comprehensive preparedness descriptions provided structure and analysis as they further presented approaches to fight cybercrime, reduce cyber-attacks, and eliminate cyber terrorism. Daily, police personnel is inundated with challenges tracing cybercrime offenders. Some components are due to the absence of borders in cyberspace and the literary gap addressing law enforcement personnel and cybercrime preparedness.

The roles of police personnel are further hindered by the failure of corporations to promptly report cybercrimes. Anonymity plays a challenge due to the lack of visibility

and police personnel cybercrime challenges intensified daily. The need must be addressed as a central spinoff to reduce cybercrime and implement expensive proactive measures that are less than the traditional response-driven components (Walker & Katz, 2013). It is imperative to better understand the interconnectivity between police personnel and cybercrime preparedness to assist in eradicating cyber-attacks and cyber terrorism. The mobility evolves from the theoretical to the pragmatic, as cybercrime is integrated with the transfer of ELT problem solving and highly complex human science.

Purpose of the Study

The purpose of the empirical phenomenological qualitative study was to explore, discover, and understand the lived experiences of Michigan police personnel preparedness and training focusing on the phenomenon of cybercrime. Kolb's (1984) Experiential Learning Theory (ELT) served as an established tool to ascertain the participants' cybercrime learning styles with workplace achievements and recommendations. The empirical qualitative study worked to explore an in-depth understanding of the police personnel's cybercrime preparedness and experiences. The qualitative phenomenological design was the best method with the purposive sampling of the Michigan law enforcement personnel, who engaged in the informal open-ended semi-structured cybercrime data inquiries. The research objectives were to explore police personnel's experiences of prior cybercrime preparedness with recommendations. The study described the personnel's learning process correlated with Kolb's (2014) Experiential Learning Theory. The law enforcement personnel's reflections expressed their cybercrime preparedness learning styles and achievements.

The study further collected and identified the personnel's cybercrime preventive techniques and provided recommendations to mitigate cyber-attacks and eliminate cyber-terrorism. The qualitative study utilized a small purposeful sample to collect the data and understand the experiences of Michigan law enforcement personnel and preparedness in the cybercrime phenomenon.

The study addressed a gap in the literature regarding the police personnel's experiences and cybercrime issues articulated by their involvement in cybercrime preparedness in Michigan. Kolb's (1984) Experiential Learning Theory (ELT) provided the foundation for the research as a blueprint with open-ended semi-structured data inquiries focused on cybercrime preparedness and formative learning. The United States of America and each individual state rely heavily on computer-controlled systems that substantiate utilities. They include water treatment plants, electric power grids, and gas pipelines. Medical and educational facilities are cyber-regulated along with other critical infrastructures. The inadequate antiquated cyber technologies provide the propensity for cybercrime complicity and opportunities for cyber terrorism.

The weak cyber firewalls and the limited outdated electronic controlled protection prevail and provide opportunities for incidents of catastrophic devastation and disaster. The research provided the availability to collect a variety of detailed data from police personnel addressing feedback on their first-hand experiences of cybercrime. I, as the instrument of the research, worked to investigate and discover what was significant. The data collection produced rich information from the comments and proactive cybercrime recommendations.

The Experiential Learning Theory assisted in aligning the inquiry tool that led to innovative knowledge reflecting on the phenomena of cybercrime. The ELT included a cycle of the four processes: concrete experience, reflection and observation of the experience, abstract concepts as an extension of the experience, and active experimentation (Kolb, 1984). All segments of the ELT framework were present and sequentially aligned for cognitive experiential learning. The purpose of the phenomenological study established why the research was necessary.

The research goals examined prior cybercrime preparedness and the experiences of police personnel. The study evaluated the comments of the participants and reflections on actions (that occurred during the learning process by reviewing challenges and issues). I analyzed abstract thoughts (what was effective in cybercrime learning). The study researched events that transpired during the learning process. The study contributed strong concepts in individual learning styles with the interpretation of new knowledge. The final components evolved with problem-solving decision-making recommendations and strategies focusing on the cybercrime phenomenon. The feedback from the participants' inquiry data was orchestrated to provide rich information for best practices and strategies. The study rendered techniques to mitigate cybercrime complicities with positive constructive social change (Forst, 2013; Kolb, 1984; Martin, 2015; Maxwell, 2013).

Kolb's (1984) ELT theory and classifications were aligned with Bloom's (1956) taxonomies and incorporated as useful tools in applying the cognitive learning operations of cybercrime preparedness training. The knowledge and comprehension provided

analytical processing with fresh interpretations from the rich understanding of the personnel's critical thinking and insight. The threat of cybercrime is serious, escalating daily, and has penetrated multiple systems in need of immediate attention. The study focused on the gap in the literature concerning police personnel and prior cybercrime preparedness. The study harvested the participant's ideas and thoughts with experiences while integrating the ELT components. An interactional process was employed combining cognitive learning and practical workplace achievements.

The theoretical construct of the experiential learning theory (ELT) and the humanistic learning theories provided a wide range of cybercrime preparedness. The empirical phenomenological research examined and discussed the experiences of police personnel, which evoked general and universal comprehensive descriptions. The study further emanated the rich data collected from the personnel's prior cybercrime preparedness with the comparative analyses of Kolb's (1984) ELT process.

Nature of the Study

The nature, quality, and essence of the qualitative empirical phenomenological study explored the lived experiences of the law enforcement personnel as they described and efficaciously articulated their scholarly cybercrime preparedness with cognitive learning. A phenomenological study is different from a phenomenological perspective. Patton (2002) emphasized a phenomenological study focuses on descriptions of what people experience and how it is that they experience what they experience (p. 107). A perspective focuses on a point of view. The qualitative phenomenological study was determined the "best-fit" methodology and research design. Phenomenology is both a

mode of inquiry and philosophy of science describing lived experiences of participants (Moustakas, 1994). The study comprehensively aligns perceptions of preparedness and the cognitive experiential learning theory (Forst, 2013; Kolb, 1984; Patton, 2002). Empirical qualitative research is a methodology emphasizing the experiences of the participants. The textual descriptions explain scientific facts addressing what transpired and how the reflective events were experienced (McMillan & Schumacher, 2001).

Kolb's Experiential Learning Theory

Kolb's (1984) ELT was influenced by Kurt Lewin, John Dewey, and Jean Piaget and aligned in conjunction with the taxonomy of Bloom et al. (1956). The experiential learning theory (ELT) was the basis of the phenomenological design. The method of inquiry worked efficiently to investigate utilizing open-ended semi-structured inquiries. The empirical research incorporated the overarching theory of prior preparedness and ELT. The theoretical constructs of the police personnel cybercrime preparedness were employed. According to Brinkerhoff (2001), the training approach must: (1) document data; (2) identify environmental factors that impede performance; (3) diagnose issues of transfer learning; and (4) work to improve solutions. The level of the ELT and evaluation became a vital tool to improve the value of the performance with problem-solving results. The transfer of learning occurred during the awareness of cybercrime preparedness and the levels of ELT. Murphy (2007) asserted that Kolb's ELT with other taxonomies added in-depth understanding with reflections to knowledge. It focused on what did or did not work; what was learned; and how the participants would approach the same situations differently for more successful learning results.

McLeod (2013) expressed the writings of Kolb (1984) published as the Experiential Learning Theory (ELT), which established ELT in two levels: the four-stage cycle of learning and the four separate learning styles. Kolb's (1984) theory was influenced by other theorists: (1) focusing on the internal cognitive processes, (2) engaged learning, and (3) components consisting of the acquisition of abstract concepts. Flexibility was applied in a cyclic hierarchical order with a structural sequential alignment. The prior cybercrime preparedness concentrated on basic cyber requirements, which were aligned to provide knowledge and clearly understand the pragmatic skills for on-the-job abilities to advance the prevention of cyber-attacks. The learned skills and ELT cybercrime competencies were expressed by the police personnel. The cybercrime all-encompassing trainings with lived experiences were gathered and analyzed from the data inquiry instrument. The police personnel provided their understanding of cybercrime preparedness from the collected data that contributed richly to the research.

Kolb's (1984) ELT theory was an impetus for the development of innovative concepts. The initial basis was formulated, built on new learning experiences, and developed in the extended learning process. Kolb (1984) affirmed that "Learning is the process whereby knowledge is created through the transformation of experience" (p. 38). The cybercrime skills and knowledge facilitation was a process of learned competencies that ensured the cybercrime applications were utilized in the workplace. The study enhanced and filled the literary gap in the field of criminal justice relating to law enforcement personnel focusing on prior cybercrime preparedness, learning styles, and ways to mitigate cyber-attacks.

Research Questions

The research questions related directly to the empirical phenomenological qualitative study that explored the semi-structured data inquiries presented to law enforcement personnel in Michigan. It assisted in bringing meaning and contributed to closing the literary gap between police personnel and cybercrime preparedness with a variety of workable solutions. The responses allowed new information to emerge. It worked to analyze and assist in solving some of the practical problems in cybercrime preparedness. The feedback from the research data inquiries provided techniques to combat and mitigate cybercrime. The basic qualitative phenomenological research questions explored the law enforcement personnel's perceptions of obtaining prior learned cybercrime preparedness and training. The research questions were aligned to procure: (1) What are the police personnel's perceptions and experiences concerning prior cybercrime preparedness? (2) How efficient was the cybercrime preparedness in relation to cybercrime knowledge, competence, and skills applied in practical ways in the workplace? (3) Did the participants comprehend, reflect, and pragmatically apply the cybercrime preparedness and experiential learning proficiencies? The three research questions were broken down into 10 smaller data inquiries. The data was collected with in-depth insight that assisted in emanating ways to uproot cybercrime, cyber-attacks, and cyber-terrorism. The three research questions are listed.

Q1. What are the law enforcement personnel's perceptions, lived experiences, thoughts, and ideas regarding the prior cybercrime preparedness, training, and experiential learning; and in what ways was it meaningful, relevant, and interesting?

Q2. Where did the law enforcement personnel acquire the prior cybercrime preparedness and experiential learning; and how was the cybercrime preparedness training applied in a pragmatic manner in the law enforcement workplace?

Q3. In what ways have cybercrime professionals applied the preparedness and list workable recommendations to combat, mitigate, and uproot cybercrime?

The police personnel's preparedness provided affirmed perceptions and thoughts that strengthened, better equipped, and assisted in describing trajectories to combat, mitigate, and eliminate cybercrime. The study examined the police personnel and their preconceived notions and conjectures regarding the challenges in the phenomenon of cybercrime preparedness. The themes from the study formulated patterns and structures as it explored critical thinking in the experiences and actions of police personnel. It analytically processed the preparedness, learning, and conundrums to combat, and uproot cyber-attacks, and cyber terrorism.

The police personnel statements and reflections governed the alignment of prior cybercrime preparedness feedback. It empowered and provided workable procedures for creative ways to actively oppose and eradicate cybercrime. The theoretical cycle of Kolb's (2014) experiential learning was integrated with the cognitive theory of Bloom's (1956) taxonomy. It served to evoke the prior preparedness and training of police personnel that provided great insight. The key definitions were imperative to understanding the practical terms in the scientific world for comprehension in phenomenological qualitative research.

Definitions of Key Terms

Antivirus software: Software detects viruses and notifies users that the virus is present and maintains a database of "fingerprints," a set of characteristic bytes from known viruses on file (Schell & Martin, 2004).

Botnet: Network of private computers infected with malicious software, controlled as a group without the owner's knowledge (Schell & Martin, 2004).

Cloud computing: Cyber technique used as a basic platform to centralize and connect a network of hardware, software, and storage media to function as a cloud and allow users to process, send, store, and retrieve information; it makes services and applications available over the Internet and can be utilized by a number of users simultaneously (Furht & Escalante, 2011).

Combat: To battle, fight, oppose, or struggle (Miller et al., 2014).

Corporate espionage: Trade secrets are stolen by the competitor of a company or corporation via computer fraud and/or another electronic device, either domestic or foreign; the objective is to increase the rival company's competitive edge in the global marketplace (Siegel & Worrall, 2012).

Crackers: Cracker is a person who breaks the security on a computer system to browse through the information and manipulate or damage files; crackers develop and implement computer viruses or new illegal ways to break into computer systems (McCaghy et al., 2008).

Cyber-attacks: Vulnerable to corporate security breaches, social media, and spear phishing (Department of Homeland Security, 2016).

Cybercrime: Theft and/or destruction of information, funds, and resources via computers, the Internet, or computer networks (Siegel & Worrall, 2014).

Cyberspace: The cyber control system of the country is composed of thousands of interconnected computers, servers, routers, switches, and fiber optic cables allowing our critical infrastructure to work (Department of Defense, 2011).

Cyber-terrorism: The hacking activity attempting to harm innocent persons and create a sense of fear or terror among the general population for the purpose of achieving a political agenda; intimidation of civilian enterprise utilizing high technology to bring about religious, political, or ideological actions resulting in disabling and deleting critical infrastructure information and data (Barnett, 2011; Tafoya, 2011).

Conflict Paradigm: The idea that groups in society have fundamental differences and that those in power control societal elements, including law (Pollock, 2007).

Cyber-stalking: Use of the Internet, computer, e-mail, or other electronic communicational devices to harass or stalk another person (Siegel & Worrall, 2014).

Cyber theft: The use of computer networks for criminal profits with copyright infringement: identity theft, fraud, warez, and Internet securities are examples of cyber theft (Siegel & Worrall, 2017).

Cyber vandalism: Malicious attacks aimed at defacing, disrupting, and destroying technology with the use of cyberspace for revenge or destruction; examples are website defacement, worms, viruses, cyberbullying, and cyberstalking (Siegel & Worrall, 2014).

Cyber warfare: Politically motivated attacks designed to compromise the electronic infrastructure of an enemy nation and disrupt its economy; examples are the use of logic bombs to destroy or disrupt secure systems or networks; Internet use that communicates covertly throughout the world; cyber war network tools can shut down critical national infrastructures or intimidate a government (Siegel & Worrall, 2017).

Dark-Market: The group was a website founded in 2005 providing infrastructure where buyers and sellers of credit card and banking details met; ordinary members traded information and sought to keep a low profile; the forum was infiltrated by an FBI agent and the apprehension and investigation resulted in 60 worldwide arrests (Broadhurst, 2006; Glenny, 2011; Davies, 2010).

Denial of Service: (DOS) attack: Condition in which a website or another Internet resource is disabled by an attack from an overwhelming number of inbound messages (Barnett et al., 2011).

Experiential Learning Theory (ELT): Knowledge, skills, and/or abilities attained through observation, simulation, and/or participation that provide depth and meaning to learning by engaging the mind and/or body through activity, reflection, and application. Learning is the process whereby knowledge is created through the transformation of experience (Kolb, 1984).

Hacking: Originally utilized to assist local governments, businesses, corporations, and other entities in positive constructive ways to enter networks and computer systems. Cracking was the negative term. Hacking was a positive term and later became a negative term for gaining access to a computer or computer system without the proper authorization (McCaghy et al., 2008; Siegel & Worrall, 2012).

Identity Theft: Criminal access through the Internet to obtain a person's data via social security number, bank account, credit cards, debit cards, and/or other sensitive information to siphon money or purchase items online in the victim's name. It can result in major financial losses and destroy the victim's credit history (Cross Domain Solutions, 2013).

Inductive thinking: Involves applying what is already known about one or a few cases and applying it to an entire group (Fritsch, Trulson & Blackburn, 2014).

Keystroke loggers: Computer a.k.a. key-loggers, that results in a significant number of cybercrime. Key-loggers record a victim's every computer keystroke and instantly transmit the information to the malicious actor; after malicious actors have the information, they utilize the victim's login information to transfer money from the victim's bank account (Pelgrin, 2013).

Malicious code: Programs exploit weaknesses in computer software, replicating, and/or attaching themselves to other programs, such as viruses and worms (Schell & Martin, 2004).

Mitigate: To make or become less severe (Miller et al., 2014; Van Voorhis et al., 2007).

Paradigm: A way of thinking and efficiently making sense of the real world embedded in the socialization of practitioners; a worldwide view that offers what is stable, workable, coherent, reasonable, important, and legitimate; model or analytical school of thought where concepts explain a complex set of data and organizes information within a particular discipline (Fritsch, Trulson & Blackburn, 2014; Patton, 2002; Pollock, 2007).

Phenomenology: To explain, systematically structure, and scientifically expands the richness of experiences of qualitative awareness with essential parameters. The study focuses on descriptions of what parameters are experienced and how the participants experience what they experience. Critical textures emerge and provide themes, patterns, and relationships with new perspectives and meanings (Patton, 2002).

Phenomenological paradigm: Example or model focusing on descriptions of what people experience or how it is that they experience what they experience (Patton, 2002).

Phishing: A form of identity fraud where the focus is aimed at stealing personal information; dangling bait in front of unsuspected (Rosenzweig, 2013).

Point of Sale (POS): Money transfers from a buyer to a seller. It includes physical tampering with pin-pads, debit cards, PINS, cash registers, or credit card information where local actors use stolen information to create fake credit cards (Pelgrin, 2013).

Reflection: Process through which the "stream of experience" with all its manifold events (phases of experience) can be grasped and analyzed in the light of its own evidence" (Husserl, 1964).

SCADA: Supervisory control and data acquisition used to control industrial processes, such as automobile manufacturing; might be controlled by other computer operating systems (Rosenzweig, 2013).

Skimming: A method in which a device is placed in a card reader, such as an automatic teller machine (ATM), to record sensitive information, such as bank account numbers, credit card numbers, and passwords (Orthmann & Hess, 2013).

Spear-phishing: A phishing attack that is targeted at a specific recipient; the name comes from using a spear to catch a particular item or thing (Rosenzweig, 2013).

SWATting: Occurs when a malicious actor plays a prank call to 911 for a full-scale law enforcement response, such as a bomb threat, hostage situation, plane crash, or terrorist attack. SWATting can involve spoofing, Voice over Internet Protocol (VoIP), phone network compromises, and social engineering (Pelgrin, 2013).

Transnational Organized Crime: Use of illegal tactics to gain profit in the global marketplace, involving cross-border sale and distribution; human trafficking is a rapid expansion example of transnational organized crime (Siegel & Worrall, 2012).

USA Patriot Act: Federal administrative law, passed by Congress in the wake of the September 11, 2001, terrorist attacks to better enable law enforcement officials to track and punish individuals responsible for terrorism and to protect U.S. citizens against further attacks; Patriot is the acronym for *Providing Appropriate Tools Required to Intercept and Obstruct Terroris*m; act designed for easier communication among law

enforcement, although it eroded America's civil liberties threatening the First, Fourth, Fifth, Sixth, Eighth, and Fourteenth Amendment Rights (Barnett et al., 2011).

Voice over Internet Protocol (VoIP): Transmission of voice communications over Internet Protocols (IP), i.e. telephone calls over the Internet (Pelgrin, 2013).

Web Patrol: Internet Crime Bureaus established by the US Department of Justice and the Computer Security Institute estimate that financial losses from computer crime were approaching $100 billion and would exceed $1 trillion by 2010; referred to as "cyber police" or "cyber sheriffs" (Inciardi, 2010).

419 Scams: The name cybercrime refers to Section 419 of the Nigerian Criminal Code. It is a reworking of the classic "bait and hook" scheme where personal information is lured from the e-mail recipient (Roberts et al., 2010).

The definitions of key terms were analytically assessed and verified for clarity throughout the qualitative study. One additional term was preparedness, which encompassed readiness in prevention, adequate training, and proficiency equipped with competent development against potential cybercrime emergencies. The definitions provided comprehension and insight throughout the research and inquiry process. Patton (2002) argued that the in-depth data inquiry with the engagement of naturalistic inquiries encompasses both benefits and risks with the personal reflections of the researcher. Cybercrime preparedness worked to gain the experiences of police personnel. The underpinnings and opportunities obtained wise perceptions of the police personnel

orchestrated in collecting the cybercrime preparedness data. It focused on how it was applied in the workplace and ways assisted in emphasizing the study's significance.

Significance of the Study

The significance of the empirical phenomenological study explored the human experiences and meanings of police personnel focusing on the phenomenon of cybercrime preparedness. Participants further recommended tactics to combat, mitigate, and uproot cybercrime. There are extensive problems with the increase of cybercrime and the failure to efficiently equip police personnel with efficient cybercrime preparedness (Berg, 2007). Cybercrime is an evolving threat becoming a worldwide epidemic. Despite ongoing cybercrime development, it is hard to detect and control through obsolete police channels (Gandhi, 2012). Police personnel must be equipped to address cybercrime due to the increase in illegal cyber activities. There is an overwhelming need to understand the police personnel and cybercrime preparedness embodying the experiential learning theory (ELT). The significance of the study assisted in: (1) closing the literary gap between police personnel and cybercrime preparedness; (2) contributing valuable cybercrime learning data; and (3) launching the prevention of cyber-attacks.

Pragmatic Application of ELT

Kolb's (1984) Experiential Learning Theory's (ELT) pragmatic application consists of Why, What, How, Where, or What if? The empirical phenomenological study's practical *Concrete Experience* (CE) entailed: **Why**- Procure a better understanding of cybercrime and the lived experiences of participants' perceptions,

experiences, and thoughts regarding prior cybercrime preparedness, training, and ELT. *Reflective Observation* (RO) entailed: **What**- Ways participants reflected and applied cybercrime preparedness, training, and learning in everyday actions in the workplace. *Abstract Conceptualization* (AC) entailed: **How**- Participants built and learned from cybercrime preparedness experiences creatively to implement on-the-job actions. *Active Experimentation* (AE) entailed: **Where-** Creative innovative ideas that participants recommended and where proactive procedures might combat, mitigate and uproot cybercrime. **What if-** Demand nipping the illicit cybercrime in the bud and identifying the importance of effective cybercrime preparedness and cybercrime elimination?

The integrated classification of Bloom et al. (1956) assisted in assessing the prior learning utilizing ELT. The process determined whether participants gained knowledge and competence from cybercrime preparedness. The learning process and procedures were integrated with Bloom's (1956) taxonomy in three basic learning domains. They were cognitive (mental skills-knowledge), affective (growth in feelings/emotional areas/attitude of self), and psychomotor (manual or physical skills). The investigation revealed how police personnel learned and applied the techniques in the workplace. The cybercrime preparedness research was established on the principles of Kolb's (1984) Experiential Learning Theory (ELT), which was interwoven throughout the study.

The challenges and problems of cybercrime continue to procreate and affect the lives of many. A study was necessary to obtain data from the police personnel explaining cybercrime preparedness and experiential learning with projected techniques and actions

that mitigate and uproot cyber-attacks. Kolb's (1984) ELT theory provided a solid foundation to build on. It focused on the ELT with clarity, comprehension, and critical thinking. The study explored the experiences and behaviors of police personnel regarding cybercrime preparedness. The open-ended semi-structured data inquiries collected rich feedback to combat and mitigate the phenomenon.

The study focused on cybercrime preparedness, hacking, cyber breaches, and the billions of dollars compromised due to cybercrimes, cyber-attacks, and cyber terrorism. The law enforcement personnel expressed their thoughts and ideas indicating their cybercrime preparedness and learning experiences. The systematic investigation study filled a literary gap concerning police personnel and cybercrime preparedness. The research provided an understanding focused on the participants' constructive viewpoints on personal actions and achievements (Fenwick, 2001; Forst et al., 2013).

Cybercrime preparedness emanated a greater understanding of the lived experiences and learning of police personnel. The prior cybercrime preparedness provided much evidence bringing about positive social change with real-world recommendations. According to Fowler (2007), experiential learning is a bridge between the theoretical and the practical, linking the skills from lectures and literature to real-life pragmatic situations. It is important not to lose sight of the experiential learning theory (ELT) and to garner thoughts and reflections of the police personnel. The research emerged and provided categories and themes with analytical insights captured from the law enforcement personnel. The cybercrime preparedness data inquiry instrument

provided great knowledge and skills with a wide range of descriptive dimensions.

Summary

The empirical phenomenological qualitative research produced a rich understanding of cybercrime preparedness provided by the law enforcement personnel with experiential learning achievements. The study gathered the lived experiences of the police personnel and the phenomenon of cybercrime. The research filled the literary gap by focusing on law enforcement personnel and cybercrime preparedness. Productive in-depth data emerged from the open-ended data inquiries with rich transferability. The transferability can be extrapolated and utilized in a variety of other professions. The rich results promulgated utilizing the experiential learning theory with strong proactive strategies to combat cybercrime, cyber-attacks, and cyber terrorism.

Chapter 1 presented and detailed the introduction, problem statement, purpose, and nature. The study explains why it was necessary and its essential worth. The areas addressed were the cybercrime challenges, law enforcement personnel preparedness, and training. Kolb's (1984) experiential learning theory (ELT) provided a blueprint and framework with key definitions and phenomenological qualitative research questions.

Chapter 2 provides the relevant literature review focusing on issues of cyber-attacks, cyber-terrorism, critical infrastructure, and the cybercrime environment. The literature review contains the limited interconnectivity with the significant lack of police personnel and cybercrime preparedness. The foundation aligns a better understanding of the cybercrime challenges. The research of Kolb's Experiential Learning Theory (ELT)

addresses the growth and complexities of cybercrime. The study explains cyber breaches, cyber leaks, and the complicities of cyber-attacks. The cyber-technological training and social media are orchestrated to assess cybercrime preparedness, cyber-security, and the perceptions of police personnel.

Chapter 3 provides descriptions and details of the research methodology, design, and population. Purposeful sampling strategies and recruitment are addressed. Noema, noesis, and data collection are described with understandable meanings. The role of the researcher is articulated focusing on the scope and limitations with ethical considerations. The epoche, reduction, imaginative variation, and synthesis are explained. The theoretical underpinnings of Moustakas (1984) with data collection were established. The analytical data assessments are processed by van Kaam's Modified data analyses, which are further explained with assumptions and trustworthiness.

Chapter 4 presents the findings, assesses the data, and discusses the empirical phenomenological qualitative study results. The goals and objectives are explicated with the challenges and diverse issues. I, as the instrument of the research, discuss the approach, data collection process, findings, and analyses. The demographic results and data feedback are provided with written verbatim statements from the police personnel. The research questions are critically evaluated with the analyses of the data inquiry instruments. The inductive inquiry analyses are systematically examined and aligned depicting the cyclic parameters. The evidence of trustworthiness is explained with anonymity, insight, and skilled experiences in the findings.

Chapter 5 provides the discussion, interpretation of the research, and implications in the value of the study. It discusses the significance of the experiences, challenges, and quotations. The research findings are explained with limitations. The study elucidates the concepts with an understanding of cybercrime preparedness and the implications for social change**.** The qualitative data inquiries address rich in-depth cybercrime issues of police personnel and their experiential learning styles. The narrative describes the advantages, disadvantages, and meaningful significant findings. It provides preventive and proactive tactics with a variety of strategic techniques. The projected strategies are listed with ways to combat cybercrime and mitigate cyber-attacks. It provides additional recommendations to uproot cyber-terrorism. Positive social change emanates from ideas and conclusions for workable transferability to other entities. The imminent need for future cybercrime studies is strongly articulated.

Chapter 2: Literature Review

Introduction

The Internet has grown exponentially and is increasingly ubiquitous opening the door for expanded cybercrime. The literature review aligns the worldwide proliferation of cybercrime and how it poses a threat to the confidentiality and integrity of computer users, computer systems, and the security of critical infrastructure (Jeffrey, 2011; Patton, 2002). Computer crimes are crimes that are different from real-world crimes committed 50 years ago. The phenomenological study is conducted to better understand cybercrime and law enforcement personnel's prior preparedness. It addresses ways to combat and mitigate cybercrime preparedness established on the blueprint of Kolb's (2014) experiential learning theory (ELT).

There is a gap in the literary research regarding local law enforcement personnel and preparedness. Focusing on everyday pragmatic issues could perhaps mitigate and uproot the cybercrime phenomenon. The study procured the many challenges of cybercrime and police personnel preparedness. Kolb's (1984) ELT was utilized to garner data from the participants through semi-structured inquiries. The police personnel shared their ideas, knowledge, and insight on handling the cybercrime challenges in preparedness. The literature review provided a great rationale for the qualitative research. The study focused on cybercrime and police personnel preparedness addressing the individual understandings and critical competencies that engaged the ELT theory of Kolb (2014). The police personnel worked to deter (while assisting in the detailed experiences of retrospective reflections and conscious thoughts) the expressed advances in the

ongoing increase and vicissitudes of cybercrime, cyber threats, and cyber-terrorism. Director James R. Clapper (2013) of the National Intelligence asserted to the Senate Select Committee on Intelligence that cyber threats surpassed terrorism threats.

Organization of Literature Review

Cybercrime has embraced the current communication technology and increased greatly with cyber-criminality becoming a distinctive criminalistics research field. The Internet began as an extensive computer network for educators, engineers, and scientists with the initial interconnected computer network system established in 1969. It was never realized that cyberspace environmental crime would exploit globally with such magnitude. The Internet is the medium of choice providing an extensive range of international global services from individual communication, entertainment, research, law enforcement, medical, and education (Siegel & Worrall, 2012). Local law enforcement personnel are often the first responders discovering cybercrime due to investigation and citizenry reports concerning the illegal cyber-activities.

The literature review of the empirical qualitative study allowed much information to emerge involving cybercrime vulnerabilities, critical infrastructures, and limited police personnel preparedness for cybercrime challenges. Pisaric (2017) asserted that cybercrime preparedness requires specific skills and knowledge. Due to the constant evolutionary technological process, police personnel must become more cognizant and creative in developing proactive means to offset the ever-evolving and escalating cybercrime. The study effectively explored law enforcement personnel and the lived

experiences procured from the semi-structured inquiries regarding prior cybercrime preparedness and training. It focused on the knowledge, comprehension, and skills to handle the excessive demands of cybercrime in the workplace. Poonia (2014) affirmed that: (1) cybercrime is increasing rapidly as technology grows; (2) cybercrime investigation is highly complicated, and (3) a wide range of different types of cybercrime demands a particular problem and solution for each case.

The qualitative study critically reviewed and examined peer-reviewed articles, journals, and documents. It provided comprehensive research on cybercrime, law enforcement personnel, and preparedness focusing on the analytical competence of experiential learning (ELT) with workplace applications. Such competence might work as an integral component to eradicating the upheaval of cybercrime and cyber-terrorism. The police personnel's experiences described and explained cybercrime preparedness with recommendations. There was a lack of literature research and no peer-review articles specifically focused on police personnel, cybercrime preparedness, and ELT experiences.

This study worked to efficiently answer the research questions. It concentrated on the phenomenon of cybercrime and cyber-attacks with the experiences, thoughts, and ideas of police personnel's preparedness to combat cybercrime entities with the proclivity to enhance learning and to bring about social change utilizing Kolb's (2014) ELT. The research viewed the scale of cybercrime issues, the law enforcement preparedness, training, and achievements in the workplace integrating the integrity of Kolb's (2014) experiential learning theory (ELT). The transfer of learning involved in the cybercrime

training and development revealed value with effectual reasoning. It further supplemented and supported the skills, knowledge, and abilities (SKA) with an understanding of cybercrime preparedness to bring about positive social change.

Cybercrime, Cyber-Attacks, and Cyber Terrorism

The proliferation of cybercrime, cyber-attacks, and cyber terrorism is increasing due to the Internet, and cyberspace threats are open to proprietary with a storehouse of data and sensitive information (Siegel & Worrall, 2014). Thousands of breaches occur daily, and the illegal profits are enormous as cybercrime activities continue to grow. Cybercrime concentration extends to the somewhat obsolete 2001 USA Patriot Act and other cybercrime legislation, which attempted to bring about cybercrime change (Dempsey & Forst, 2013). The *USA Patriot Act* demanded the need for further cybercrime research, police personnel preparedness, and collaborative actions. Viable information sharing and cyber intelligence were necessary; however, many cybercrime components of the USA Patriot Act were challenged and deleted.

Since 1998 in Linthicum, Maryland the Defense Computer Forensics Laboratory (DCFL) has been ground zero in the nation's fight against cybercrime to combat the multiple cyber-attacks by thieves, hackers, and hostile invaders (Siegel & Worrall, 2017). However, effective change is often controversial, time-consuming, and critical. It is necessary to work with cyber-transnational, organized proactive cybercrime systems, police personnel, and forensic centers with the additional essential cybercrime systematic logical approaches (Etges, 2008; Geers, 2010; Gerdes, 2005).

Cybercrime Environment

The term cybercrime is an ambiguous term that refers to any felonious activity that utilizes computer networks as the key means of commission (Martin, 2015). The cybercrime environment addresses electronic digital devices that perform complexities rapidly intermingling data with unique and innovative compilations as an extension of the ubiquitous Internet. Finnie et al. (2010) defined cybercrime as, "any criminal offense that is committed or facilitated through the use of the communication capabilities of computers and computer systems" (p. 10). Cybercrime has increased with extensive proliferation and high-level interconnectivity throughout the world, while focusing on cyber criminals, such as hackers, crackers, phishers, vishers, cross-site scripters, bot-netters, and other criminal activities utilizing the Internet as a source of illegal complicit activities (Finklea & Theohary, 2013). Police personnel often serve as first responders occupying a crucial role in the investigation and apprehension of cyber criminals.

The cybercrime environmental problem identified the literary gap, need, and rationale for the qualitative phenomenological study. It provided a reflective analysis depicting the essence of the police personnel's preparedness. It encompassed opinions focusing on the phenomenon of cybercrime preparedness and ELT. The empirical qualitative phenomenological study's primary theory aimed to utilize the ELT descriptive reflections as a foundation. It aligned a blueprint integrated with the law enforcement personnel and prior cybercrime preparedness. In addition, cybercrime further concentrated on what transpired and how it has evolved.

Ever-Evolving Cybercrime

The technological development of computers and cybercrime moved rapidly during the last 50-plus years. In the 1960s, transistor-based cyber systems were vacuum-tube-based machines (Gercke, 2012). In late 1969, a fire caused by a student riot destroyed the computer and data. In the 1970s, there were approximately 100,000 mainframe computers in the USA. The illegal use and criminal activity increased against the mainframes with multiple distortions in electronic data theft and computer-related fraud that resulted from weak or inadequate firewalls (Siegel & Worrall, 2014). The Bulletin Board System (BBS) was born in 1978 incorporating the landline telephones, coaxial lines, and modems that communicated internationally through cyberspace.

In the late 1970s, police agencies were investigating multimillion-dollar losses in computer-related fraud cases and at that time the USA considered a draft bill to address cybercrime (Gercke, 2012). However, the draft bill did not become a reality. The issue of computer-related fraud was birthed, and more cases were investigated by police agencies. In the 1980s personal computers (PCs) became popular opening a window of opportunity for criminals and their targets, including the focus on critical infrastructures (Gercke, 2012; Levi et al., 2015). The computer network environment enabled cyber-criminals to enter computer systems anonymously from diverse locations throughout the world. Software piracy became prevalent and malicious with increased viruses.

In the 1990s the graphic interface, the Worldwide Web (www), was introduced and followed by extensive Internet users with new additional challenges for local law enforcement personnel. The Internet challenges were broad with global information

exchanged and police investigations of expanded transnational crimes (Gercke, 2012; Levi et al., 2015). Cybercrime focused on online services utilizing websites and Internet services as the 21st century opened doors for new sophisticated cybercrime methods with escalated challenges for law enforcement personnel. The highly sophisticated illegal cyber-trends consisted of botnet attacks, phishing, voice-over-IP (VoIP), cloud computing, Dark-Markets, and intense innovative cybercrime technologies. The anonymity made it difficult for police to identify and investigate. The police computer crime investigation term evolved and was referred to as "cyber forensics" or "cybercrime forensics." Forensic cyber-criminology addressed cybercrime studies and investigations.

The Advancement of Cybercrime

The rapid advancement of cybercrime and information system technologies escalated society to another level (Chernukhin, 2014). The entire cyberspace and global systems are targets for cybercrime. The USA is the main focal point for illegal cybercrime activities (Siegel & Worrall, 2012). In fact, most of our daily systems are tied into and controlled by cyber-networks, which expand the opportunities for the increased anonymity of cybercrime. Cybercrime retains previous, current, and future data with critical factors, elements, and experiences that transpire at a moment's notice (Martin, 2015). The Internet is an intense and powerful ever-changing tool. Cybercrime occurs in the global arena of worldwide crimes growing rapidly and is intensified by the constant use of the Internet utilized by individuals, private sectors, corporations, and governments-local, county, tribunal, state, and federal (Hinduja, 2007; Wall & Williams, 2007).

This study required the police personnel questioned to describe, clarify, and elucidate their prior cybercrime preparedness. The learned procedures, comments, and concerns were necessary. Police personnel expressed experiences and reflective details regarding the cybercrime training. The qualitative approach entailed a return to the lived experiences and conscious awareness of police personnel. Their pertinent perspectives reflected and comprehensively articulated their thoughts and descriptions regarding the prior cybercrime preparedness, training, and ELT. The data provided strategies and a viable understanding of the outstanding experiences of participants and cybercrime.

Cybercrime and the Digital Divide of Technology

Cybercrime has become a sophisticated cyber-domain in recent years; however, the solutions for solving the crimes are complex and unresolved (Siegel & Worrall, 2014). The study addressed the evolving cyber-attacks as police personnel revealed their prior preparedness enhanced by Kolb's (1984) ELT. The threat of cybercrime is serious, escalating daily with the penetrated multiple systems and infrastructures. Taylor et al. (2010) contended that cybercrime is a diverse problem encompassing a range of difficulties with emotional and economic results. It has been affirmed that cybercrime is well-entrenched in criminal enterprises and has a marked impact on the daily crimes that are ever-present (Jeffray, 2015). Cybercrime is growing at rapid rates with diverse encounters incorporating many traditional crimes utilizing the Internet. Complex investigations with the complicity of cyber criminals and the failures to arrest due to anonymity allow maneuvers across invisible borders. Unique preparedness and

innovative simulated training is recommended with strategies that might be essential to offset the ever-increasing cybercrime phenomenon in question (Martin, 2015).

The scientific digital divide between technology and human engineering predisposed our lifestyles and resulted in a prevailing cybercrime epidemic. Stambaugh et al. (2000) noted particular interest and difficulty in the disparity between police technical training (state/local level) with advanced technological skills of cyber-criminals. Tremendous proportions of innovative cyber-criminality continue to flourish. The daily cybercrime transitions expand, while perpetrators possess low risks of being identified even with today's many video-cam pictorial cameras and towers. A great concern of uncertainty exists among police personnel and the increase in cybercrime (Dempsey & Forst, 2013). The escalating cybercrime challenges promote the need for excellence in police personnel preparedness and scientific designs including high-level modalities.

Cybercrime requires that law enforcement personnel are prepared to rapidly combat, mitigate, and uproot cybercrime. The immediacy to eradicate the ongoing escalation of cyber-criminal activities must be addressed with preeminence (Dempsey & Forst, 2013). The global cyberspace market is constantly changing and continues to expose innovative vulnerable environmental infrastructures. The increased highly volatile illegal cyber offenses could work efficiently with the coordinated efforts of community policing (Siegel & Worrall, 2014). Collaborative efforts in the symbiotic community and law enforcement personnel can work to coordinate problem-solving and decision-making avenues in cybercrime proactive prevention. Enhanced cybercrime and high-level

technological skills are designed and developed daily. Koppel (2016) argued that the USA tends to be a reactive culture "we wait for bad things to happen and then assign blame; despite mounting evidence of cyber-crime and cyber sabotage" (p. 56). The USA cannot effectively work the cyberspace domain alone to prevent cybercrime. The cyber domain has escalated tremendously and is empowered by focusing on a vast array of innovative cybercrime actors and technologies (Cilludo & Cardash, 2013). Advanced cybercrime technologies are discovered, and the demand is enhanced and integrated with the learning process and riveting cybercrime. The Internet and cyberspace have evolved presenting criminals with an intense pool of communication, technological transactions, and elevated knowledge as cyber-attacks continue to rise exposing critical data.

Cyber-Attacks

Cyber-attacks identify and gather vulnerable data (hacking hospitals, banks, retail organizations, corporations, and educational institutions). It illegally harvests data as it compromises networks and infrastructure systems. Cyber-attacks are defined by the Department of Homeland Security (2016) as electronic devices vulnerable to inculcating security breaches, social media, and spear phishing. Cybercrime is paramount and the ever-increasing cyber threats emanate daily. Wexler (2014) emphasized that the new cyber-attacks have increased, and law enforcement agencies have been unable to meet the needs of the victims or effectively prepare and identify their roles in adequate prevention and investigation. Cyber-attacks depict a conglomerate of divisive hacks. Siegel and Worrall (2014) asserted that instead of robbing a bank at gunpoint, there is a new breed of contemporary thieves that find it easier to hack bank accounts and transfer funds to

offshore accounts. Many cyber-attacks now consist of perpetrators attacking banks and educational systems by spear-phishing: increasing financial balances or changing grades in major educational institutions (Clinard & Meier, 2016). Koppel (2015) affirmed that an attack on the three USA electric grids could disable our infrastructure.

A cyber-attacker might hack the banks' firewalls, remove funds, transfer money, or maliciously destroy an individual or corporate account. Spear-phishing is a phishing attack that is targeted against a specific recipient or corporation; whereas the name is derived from utilizing a spear to catch a particular item or thing (Rosenzweig, 2013). The cyber assailant might erroneously justify the crime by indicating the bank "was asking for it" due to weak inferior firewalls. Not only are cyber-attacks the concern of police, but businesses, universities, hospitals, and governments. Each must remain knowledgeable and vigilant against sophisticated hackers to understand the many cyber-attacks. The three posited concerns in the cyber-intelligence domain that demand proactive cyber-attack awareness are: people, technology, and policy (Cilluffo & Cardash, 2013). Illegal transitions open doors to increased cyber-attacks in multiple high-level pinnacles.

Liberman (2017) affirmed that hacking and cyber-attacks present the propensity for elevated harm that can be activated against a country's infrastructure from a computer on the opposite side of the world, and Internet has emerged as a dangerous tool. The need is mandatory for law enforcement personnel to be equipped and knowledgeable in addressing cyber-attacks due to the surmounting criminal activity and the anonymity of the perpetrators. Hinduja (2004) found that over three-quarters of the Michigan law

enforcement agencies declared a need for training. Preparedness and training are forthcoming with other innovative technological resources developed to mitigate and combat cyber-attacks. Broadhurst (2006) mentioned that the globalization of cyber-attacks was on the rise and required the USA to take the appropriate action to address challenges. It demands proactive ways to disarm the cyber-attackers, rather than reactive.

Siegel and Worrall (2014) identified two escalating cyber-attack challenges. The two were the rapidly evolving plan focused on obsolete schemes and the enhanced work to control the development of innovative attacks. It demanded that police personnel develop evolving technical skills to compete with cyber-attackers. The cyber-attack activities have affected many focusing on personal, corporate, and government accounts with adverse consequences. Many corporations fail to report compromised cyber-attacks to the public, and their clients are unaware they have been attacked until weeks and months later. Sagacious cyber-attacks grow and exacerbate daily in the cyber world.

Escalating and Evolving Cyber-Attacks

Cyber-attacks are real and escalating. Immense hacking attacks transpired in one of the three major USA credit agencies. In July 2017, the EQUIFAX Credit Agency was attacked and affected over 143 million individuals, businesses, and corporations. It exposed personal data, such as names, addresses, driver's license data, social security numbers, dates of birth, and other pertinent information. The integral constituent of law enforcement personnel cannot compete with the emerging cyber-attacks in the escalating acclaimed challenges. There were steadfast increases in cyber-attacks that were unique,

unparalleled, and unprecedented. The illegal cyber-attack opportunities gathered individual, business, and government susceptible information and proprietary data. Gray (2015) from the *Detroit Free Press Lansing Bureau* contended that the daily hacker attacks are besieging the state of Michigan's government computer network systems, which were staggering and escalating in both cost and incidents.

Cyber-attacks are evolving; and the "so-called lone wolf" who learned from others or from the Internet is a vexing challenge to law enforcement personnel (Cillufo and Cardash, 2013). Due to the digitally stored data, cyber-attackers are provided greater opportunities to illegally undertake a magnitude of data in one attack and erase traceable records of their online actions (Gonzales et al., 2016). The future is filled with potential cyber-attacks, threats, and opportunities for cyber-attackers which intensify the work of law enforcement personnel. Broadhurst (2006) explained that many cyber-attacks become extremely difficult when multiple jurisdictions and diverse regions are involved. The antiquated law enforcement personnel methods are no longer sufficient for the multiple cyber-attacks. It was asserted by Koppel (2016) that many transactions are conducted in cyberspace with technological dependencies not thought of a generation ago.

The need is imperative for police personnel to become computer-savvy in a cyber-attack investigation to efficiently activate measures and conquer the illegal cyber-attacks and scams transpiring daily. Cyber-attacks occur in the global arena of worldwide crimes intensified by the requisite use of the Internet. Proactive cybercrime utilization is mandatorily activated by personal, private, and government usage (Hinduja, 2007;

Wall, 2007). The multitudinous electronic devices promulgated opportunities for cyber-attacks and cybercrimes. The utilization of the Internet includes e-commerce, e-health, e-government, e-mails, social media, mobile tablets, iPods, i-pads, smartphones, and other electronic intelligence units (Clinard & Meier, 2016). Electronic devices can create serious cyber-attacks and threats with vulnerabilities including incessant accelerations.

Cyber-attacks argued by Koppel (2013) tended to be less visible because the perpetrator and victim were not inclined to publicize the cybercrime. It resulted in online piracy costing the USA economy billions of dollars [and moving towards trillions] each year. Thousands of cyber-attack breaches occurred daily, and illegal profits were enormous and continued to grow. The state of Michigan stops each day approximately 739,000 attacks on the IT network, ranging from phishing, spam, and malicious bots designed to hamper or shut down a computer network system (Gray, 2015).

The escalating cyber-attack challenges promoted the need for local police personnel. The IT experts initiated and incorporated workable investigation techniques and other procedures to mitigate and combat cyber-attacks. Cyber-exploited intelligence servers with potential cyber-attack networks have crippling effects on financial dealings. They come in waves with a controlling intensity, not understanding how extensive the attack was and whether it was ongoing (Levi, 2015; Kelly et al., & Almann, 2009). Great damage and devastation resulted in cyber-attacks with horrendous and detrimental difficulties. The federal government plays a critical role in cyber-attacks.

Government Entities

The Department of Homeland Security (DHS, 2011) was established with 22 merged federal government agencies after the USA experienced the most catastrophic 911 event. Koppel (2013) argued that DHS did not have the capacity to defend the national infrastructure against cyber-attacks, nor the ability to retaliate. The DHS does not include the CIA, FBI, or the National Security Agency (NSA); these agencies share their cybercrime with the department's intelligence center. Criminal cyber-attacks are the oversight of the Federal Bureau of Investigation (FBI, 2002); however, many cyber-attacks are discovered by local police. The Department of Defense (DOD, 2011) has jurisdiction and oversight over the external/internal infrastructures of a nation or state.

The FBI has three priorities to protect the USA: terrorist attacks; espionage and foreign intelligence operations; and cyber-attacks including high technology crimes (Dempsey & Forst, 2013). Each law enforcement agency has personnel attempting to track the excessive cyber-attacks and threats to the USA's infrastructure. FBI is an agency defending many cyber-attacks derived from the *Dark Web* that understands the contingencies existing in the challenging confrontations (Ionita et al., 2016). The FBI works with local law enforcement and intensifies the critical need for local law enforcement personnel's preparedness to mitigate, combat, and eradicate cybercrime. Koppel (2016) emphasized the appalling dependency on many transactions conducted in cyberspace making the USA vulnerable. The exploited Internet resulted in the USA being indifferent to potential catastrophic well-targeted cyber-attacks. The International Chiefs

of Police (IACP, 2005) argued that the critical need for law enforcement cybercrime preparedness was due to the increase of cyber-attacks and potential cyber terrorism.

The Federal Bureau of Investigation (FBI, 2002) defined cybercrime terrorism as terrorism that initiates or threatens the exploitation or attack of any information system. The horrendous critical attacks or damage to a USA computer technological system can place the entire nation's safety and security in jeopardy; cybercrimes can transpire in the world anywhere and at any time (Gercke, 2012; Levi et al., 2015). Cybercrime can devastate the entire USA infrastructure systems without proactive standards appropriately implemented. In fact, almost all systems are interconnected or tied to cyberspace technology-federal, state, and local. Local levels cannot exist without the Internet-health care, banking, police, fire, private agencies, and individuals (Broadhurst, et al., 2014). Government entities have various forms of cybercrime consisting of cyber thefts, cyber vandalism, cyber war, and many more. The Defense Computer Forensics Laboratory (DCFL) provides the Defense Department with digital search assistance, investigative services, and expert court testimonies; the information is shared with numerous law enforcement agencies (Clinard & Meier, 2016).

The CIA is precluded by law to operate within the USA; however, effectively maintaining national boundaries in cyberspace may be impossible (Koppel, 2016). Criminal cyberspace is the worldwide interconnected digital divide of global communication. The Internet, cyber-infrastructure, and information network result in difficulties in the important role of the law enforcement communities and the cyber-

evolution (Koppel, 2013; McCaghy, et al., 2008). Czescik & Siemianowski (2014) argued concerning the evolution of law enforcement cybercrime:

> Nowadays, in order to commit an offense, one does not need to leave one's place of residence, it is enough to have a computer, a particular idea and access to the Internet. Knowledge of masking and hiding on the Web greatly increases the chances of success and confounds the instruments of law enforcement and justice. Law and order, when disrupted by various types of crime, generate in society a sense of fear, injustice and lack of state control. (p. 72)

Today, the cyber system is controlled by the Internet. According to Dempsey and Forst (2013), the Secret Service preserves the integrity of the nation's infrastructure by utilizing preventive methods to combat cyber-terrorists who attempt to defraud and undermine American industries and consumers. Condoleezza Rice (Former President Bush's National Security Advisor in 2002) denoted that the cyber-economy is the economy; and when cyber-networks became corrupt, the entire nation is disrupted.

Cyber Terrorism

One of the earliest cyber terrorism attacks was in 1996 on an ISP in Massachusetts; the individual deleted records, disabled ISP's service, and left a horrendous threat (Clinard & Meier, 2016). Worldwide cyber terrorism is devastating and oblivious. It entails politically highly destructive monetary motivation. Cyber Terrorism, according to Schiff (2017), is a real threat that cannot be ignored with increasing availabilities and cybercrime technologies evoking havoc due to the open cyberspace and

anonymity. It provides opportunities for other countries to destroy the USA's water and food, bringing in unknown diseases and illnesses utilizing cyber terrorism.

Former President Barack Obama stated that cyber terrorism was perhaps one of the greatest and most intense threats against the USA. Cyber terrorism might very well become a central component of the terrorist environment soon. The need for police personnel to become more knowledgeable with proactive cyber skills is imperative to uproot and conquer the emerging cyber terrorism schemes transpiring daily. Deep conceptual cyber-terrorist actions continue to emerge and escalate with the high-technological factors as cyber terrorism continues to grow (Smallridge et al., 2016).

Cyber terrorism has involved serious attacks on Sony and Microsoft with the Stuxnet in June 2010, which became the world's first digital weapon and moved on to become a virtual world, capable of destroying a large portion of physical aberrations. Iran announced that the computers at the Natanz Nuclear Facility were under attack and the enemy was apparently the United States, which turned out to be the Stuxnet computer worm that wiped out one-fifth of Iran's nuclear centrifuges used for fissionable material (Siegel & Worrall, 2017). It did not destroy Tehran's capacity to make nuclear arms; however, it assisted in delaying the making of its first nuclear arms. According to Norman (2018), the North Korean attack caused the Internet infrastructure to become dysfunctional for nine-and-a-half hours and resulted in potential threats to International terrorism. Eighty-two percent of Americans agreed that North Korea and the development of nuclear weapons posed critical threats to the USA and vital components, such as cyber terrorism that continue to rise. The Gallup poll revealed for the last five to

six years, cyber-terrorism posed a critical threat to the USA (Norman, 2018). The Internet is the most potentially dangerous non-lethal weapon that destroys millions of lives. Although, Weimann (2004) asserted the Internet is a valuable and critical counter-terrorism cyber tool that allows the understanding of terrorists and is constantly utilized for ongoing cyber-terrorism.

A word to the wise with sagacious pondering thoughts acknowledges the question, according to a *Washington Post* newspaper article on March 13, 2018, titled-"Is U.S. prepared for Cyber Terrorism?" One might observe the critical infrastructures in Michigan focusing on the Great Lakes, which are the only fresh waterways in the world that builds and authenticates a target for potential USA cyber terrorism. During the 911 crisis, it was projected that one of Michigan's Great Lakes might be the identified target for contamination of fresh water. Raj J. Patel (05.21.2013) in t *Crain's Detroit Business News* asked the question-"How prepared is Michigan for a cyber-attack affecting our critical infrastructure?" The state of Michigan has established a unique centralized entity to prepare, respond, and recover from cyber-terrorist incidents or disruptive events referred to as "Cyber Disruption Response" (CDRP, 2016) embodied as an approach with fusion centers in all local and federal public safety agencies.

Disruption of Infrastructure

Cyber terrorism can result in the disruption of the infrastructure that would endanger lives from contaminated widespread poisoned water and infested foods resulting in lingering chronic illnesses and radio-active deaths. The crucial infrastructure is the power utilized in our homes: water, electricity, and the Internet, to name a few.

Other daily uses are gas station pumps and transportation with other potential terrorist components cyber-controlled. All can be destroyed in a matter of seconds by cyber terrorism utilizing chemical, biological, radiology, and nuclear (CBRN) that could attack our infrastructure controlled by computers. It could shut down this country and destroy entire schools, corporations, and cities in the USA. Much of the USA's infrastructures are antiquated with open opportunities for cyber-attacks and illegal cyber-operations.

Liberman (2017) asserted that the Internet has the potential for terrorism in multiple ways, such as Google Earth utilized to study locations and activate possible attacks. Terrorists do not have to totally rely on the Internet to spread propaganda; instead, terrorists utilize the Internet to achieve and even surpass the media's functions. Cyber-terrorism propaganda from ISIS or ISIL (violent extremist groups) has produced over 90,000 posts on Twitter, Facebook, and other social media every day (Liberman, 2017).

The future of cyber terrorism is critical, especially due to the number of connected interfaced devices that escalate daily setting up the USA for a physical cyber terrorism world attack. There are cyber-controlled missiles and drones that could result in devastating cyber terrorism. Schiff (2017) asserted that cyber terrorism is a genuine threat that cannot be ignored due to the lack of effective oversight in power, transportation, communication, water systems, and infrastructures that present qualities a terrorist may desire; therefore, cyber defense must become a priority. Cyber terrorism provides a foundation to analytically assess and effectively evaluate possible vulnerable targets. There is a tremendous gap in the research of law enforcement personnel focusing on the

knowledge and understanding of the phenomenon of police personnel's cybercrime preparedness. Prior research studies further support the need for this study.

Research of Bossler and Holt

A somewhat contrasting quantitative research study with similarities was conducted with law enforcement patrol officers and cybercrime. Holt and Bossler (2013) asserted that cybercrime had created substantial challenges for law enforcement, particularly at the local level and most scholars and police administrators believed that patrol officers needed to become more efficient first responders to cybercrime calls. The evidence illustrated that many patrol law enforcement officers were neither adequately prepared nor strongly interested in taking an active role in addressing cybercrime at the local level. The research study examined factors that predicted patrol officers' interest in cybercrime training and investigations in two southeastern USA cities.

The study of Holt and Bossler (2013) specifically examined only patrol officers. The focus was on relationships between demographics, cybercrime exposure, and computer training with the views of patrol officers and their interest in cybercrime investigation training. It addressed conducting cybercrime investigations in the future concentrating on patrol officers' views and cybercrime. The strongest predictors in the cybercrime efforts were officers who valued cyber-attack investigations and believed cybercrime would change policing by utilizing computer skills (Holt & Bossler, 2013).

The patrol officers who received prior computer training were less interested in additional training and conducting investigations. The research findings support the

argument that more command and departmental meetings are necessary to focus on the value of investigating cybercrime to increase the patrol officers' interest. The study surveyed factors regarding patrol officers, cybercrime training, and investigations in Georgia and North Carolina. Holt & Bossler (2013) examined the sworn law enforcement patrol officers who had received previous computer training and their relationship between cybercrime exposure, computer training, and proficiency. The quantitative study's surveys, findings, and conclusion resulted in patrol officers expressing they were less interested in additional cybercrime training or investigations. Holt & Bossler (2013) concluded that there was an essential need for emphasis on the necessity and value of cybercrime investigation to peak the patrol officers' interest (p. 464).

This empirical phenomenological qualitative study is different focusing on the challenges of police personnel and not only on patrol officers. The qualitative study collected thoughts, perceptions, and understanding of police personnel's prior cybercrime preparedness, training, and experiential learning. The research filled the literary gap in cybercrime preparedness and law enforcement personnel. Participants cited enhanced preparedness with recommendations to mitigate cybercrimes and uproot cyber terrorism bringing about positive social change. This study concentrated on police personnel, such as civilians, police reserves, police technicians, law enforcement assistants, auxiliary police, adjunct police, police staff, and sworn officers. The selected target population emanated diverse opinions and cybercrime preparedness and experiential learning. Cybercrime continues to evolve with escalating growth and diverse complexities in the Worldwide Web of cyberspace.

Cybercrime Growth and Complexities

Cybercrime has continually increased in the world of cyberspace. The Internet has become an essential component in the lifestyle and existence of everyday people as cybercrime intensifies. Dretzin et al. (2010) explained that over the past two decades the Internet has changed from a thing one does; to the way a person lives. There is continual virtual cyber connectivity with exposed vulnerabilities for cybercrime. The unlawful activity of cybercrime exploits daily and is a horrendous threat to safety and security. The computer in its original sense was to educate, provide knowledge, exchange information, and perform interactions with great intelligence. Cybercrime is evolving in an upward spiral trajectory as law enforcement personnel tend to lag somewhat behind.

Evolving Escalation and Techniques of Cybercrime

Pelgrin (2013) expressed common cybercrime techniques threatening law enforcement. It was reinforced by the need to know and understand cybercrime's technical components. The keystroke loggers record every keystroke with primary targets being small businesses, government agencies, and schools. The focus is on personal retirement and investment accounts with money-mules transferring funds to locations while advertising illegal activity online. Point of Sale (POS) compromises are common with local actors who use stolen information to create fake credit cards. SWAT-ting techniques involve spoofing, VoIP, phone compromises, and social engineering that initiate the prank 911 calls to manipulate people into sharing information. Ransomware locks a computer, requesting ransom as cyber security experts work to clean and remove the malicious software. Cybercrime is evolving with critical infrastructure issues, cyber

threats, and the need for efficient police personnel preparedness. It is an increasing reality that the local police personnel must become more proactive and cognizant of cybercrime with innovative and expansive technologies (Dempsey & Forst, 2013).

The prevalent cyber-intrusions argued by Glennon (2012) were that of botnet attacks, which are made up of extensive amounts of compromised computers that are "infected" with malicious codes (p. 100). Botnet attacks can infect comports without the owners' knowledge. Kelly and Almann (2009) argued that in 2007 Estonia was a victim of a cyber-attack that almost shut down the entire country's digital infrastructure; the attack was carried out by "hacktivists" who were incited by the Russian websites (Levi, 2015 et al., McMahon et al., 2016). Botnets can be extremely large and circulate as new zombies that join other cybercrime attacks on the Internet. Botnets can perform untold damage and might be classified as E-WMDs-Electronic Weapons of Mass Destruction (Kelly & Almann, 2009).

Microsoft in the Microsoft Security Intelligence Report (2008) affirmed that 10 percent of all Windows computers were infected with malware. The daily cyber transactions are dependent on cyberspace and provide opportunities for cybercrime. Stolen data is digitally stored and converted for illegal use later (Levi et al., 2015). Often computer firewalls are weak and fail to provide the necessary cyber security protection.

Cybercrime Typology Categories

There are multiple issues in the original developmental definition of cybercrime. Broadhurst (2006) defined cybercrime development in seven offense typology

categories, which stipulated specific cybercrimes in each segment. Broadhurst (2006) asserted that there were seven identified cybercrime offenses: (1) interference with the computers' lawful use, such as-cyber-vandalism, cyber-terrorism, viruses, and malicious codes; (2) threatened communication including cyber-stalking and extortion; (3) dissemination of offensive online material, such as gambling, pornographic, and hate-racist material; (4) forgery and counterfeiting including identity theft, IP offenses, phishing, and copyright violations; (5) fraud encompassing Internet credit card theft; (6) illegal compromised e-funds; and (7) other types of cybercrime-electronic money laundering, criminal conspiracy, commercial, and corporate espionage.

Cybercrime can transpire anyplace in the world and the responsibilities increase the law enforcement personnel's everyday workload and investigations. The ever-changing cyberspace and rapid operational use of the Internet have increased cybercrime problems and negatively impacted individuals, companies, and organizations. It has affected cities, states, countries, and nations. It is difficult for local police personnel to efficiently address cybercrime due to the multiple cyber-attacks and cyber-transnational crimes. The heightened cybercrime challenges, security risks, and daily vulnerabilities threaten people, places, and situations. It increases the need for highly competent police personnel with experiential learning cybercrime preparedness. At this time, law enforcement agencies are mandated to share their cybercrime data with the United States of America Government Department's Intelligence Center emitting an enormous conglomeration of cybercrime information.

Cybercrime Information, Thoughts, and Expressions

In 2000 U.S. Attorney General Janet Reno expressed that whether technology benefits us or injures us, it is dependent almost entirely on the fingers on the keyboard. The proliferation of cybercrimes originates anywhere in the global market of cyberspace affecting law enforcement agencies. Stambaugh et al. (2000) addressed the concern in the gap between the training, preparedness, and available technologies incorporated by state and local police departments and focused on the technological advances used by individuals committing illegal electronic crimes. Perpetrators of cybercrime may commit crimes anywhere in the worldwide cyberspace network and hide their identities. At times organizations fail to immediately detect, expose, and report cybercrime intrusions.

Cybercriminals rely on advanced Internet technologies to commit crimes and perform illegal corrupt activities. Cybercrimes include traditional crimes of personal and property offenses, identity theft, and credit card fraud. It is inclusive of illegal drug distribution, cyber-stalking, and sex trafficking. It further includes illegal cyber-control of infrastructures, such as gas stations, traffic lights, and power plants. School walkways, railroad crossings, and transportation systems are cyber-controlled. Cybercrime continues to escalate and shows no signs of diminishing, whereas cybercrime perpetrators often view cybercrime as a teleological argument. A teleological argument is expressed that the end justifies the means (Pollock, 2007). Many cybercriminals justify their illegal criminal cyber skills and behaviors in adverse ways, such as insurance agencies reimbursing the victims. However, cybercrime continues to escalate with great complications.

Cybercrime Statistics and Social Economics

In 2011 cybercrime statistics divulged that there were 431 million adult victims of cybercrime in 24 areas and over a million were affected each day (Cybercrime Statistics, 2014). Cybercrime in terms of engineering entails sophistication; and elaborate analytical cyber- techniques. The surreptitious scope is growing throughout the world at exponential rates. Cybercrimes cost approximately 114 billion annually and these were only the reported cybercrimes. Many corporations never report the cyber-attacks and breaches that hacked their computer security system (Cybercrime Statistics, 2014). There are many white-collar cyber criminals who perform cyber fraud and beat Americans out of huge funds that are never convicted or punished. Waters and Doll (2012) argued that cyber scam artists understand local law enforcement agencies are too busy to investigate and prosecute due to the lack of personnel, time constraints, and cyber training skills.

Today cybercrime technologies are embedded in the very essence and foundation of crime. The fundamental motivation of cybercrime tends to focus on personal gain, power, and position (McCaghy et al., 2008). Large numbers of cyber-criminals work freely in anonymity, especially as white-collar crimes are committed. Billions of dollars are scammed as cyber-criminals walk with totally invisible hidden identities. Koppel (2016) expressed that in less than a generation, cyber-criminals have become adept in the proficiency of the Internet for robbery on an almost unimaginable scale. One key to cybercrime is the role played by those affected by the crime and potential victims. The three essentials are the volume of the crime, the speed of the crime, and the distance cybercrimes can be committed (Levi, et al., 2015). Over the years the Internet has

expanded and evolved with rich pools of technology and constant change with much knowledge and impunity (no punishment).

Complex Cybercrime

Cybercrime has multiple criminal offenses and incidents, which constantly intrude in unauthorized illegal areas (Gordon & Ford, 2006; Pladna, 2009). The local police personnel are challenged with variegated cybercrime because the locations are not static due to the worldwide cyberspace. Cybercrime transcends boundaries and is more problematic in the advent of (1) evolving increased cyber schemes; (2) employing compelling engineering challenges difficult to detect through traditional police methods; (3) expanding capabilities of police personnel often not equipped with the advanced technical computer savvy; and (4) not as well-versed and articulate as the cybercrime perpetrators (Berg, 2007; Gandhi, 2012; Siegel & Worrall, 2014).

There are a variety of cybercrime components and exigencies established that affect our daily lives. Financial funds can be rapidly transferred into different accounts and grades can be changed in the registrars' offices in universities. Schjolberg (2008) stated that "Cyberspace has made a new environment for criminal offenses" (p.1). The Internet is linked with powerful computers and electronic global technological services. The cyber-theft capabilities are intensified by weak firewalls. Wexler (2014) argued that cybercrime is a new issue and changes the fabric of local law enforcement. It provides opportunities for cyber-attacks to extensively procreate from criminals who live on the opposite side of the world to become a problem in one's own background. Victims are

evoking NIMBY -"not in my backyard;" although it extends in many backyards-affecting multiple lives (Miller et al., 2014).

Criminal offenses have resulted in greater issues for local police personnel with increased citizens' cyber-attack complaints. Tafoya (2011) affirmed that the utilization of high technology results in deleting and destroying critical infrastructure cyber data and information. The lack of skilled law enforcement personnel's cybercrime education, knowledge, and training has resulted in numerous compelling challenges (Berg, 2007; Finklea & Theohary, 2013). Cybercrime was developed from the cyber-evolution with computer complicit issues and cyber terrorism. Wall (2008) asserted that the origin of the term "cybercrime" was initially coined from media and the science fiction forums that were interconnected to cyberspace. There are exponential complex challenges regarding cybercrime. Gonzales et al. (2016) affirmed that cybercriminals are global. They are rarely restricted to a single nation's border and investigations encounter an impediment of anonymity on the Internet. Police personnel capabilities must be strengthened by implementing up-to-date training, and advanced technology, and encouraging problem-solving values (Clark & Eck, 2003; Siegel & Worrall, 2012).

Cybercrime Threats and Risks

The cyber-threats expressed by Borum et al. (2016) asserted that cyber threats are risks poorly understood when focusing on "technical" dimensions, rather than the human dimensions. The cybercrime actors with illegal intentions are unique. Police personnel are confronted with cybercrimes, such as denial of services (DOS) and data espionage.

Siegel and Worrall (2012) maintained that the basic forms of cyber-threat risks are cyber theft ranging from identity theft to illegal copyright infringement. Cyber-vandalism consists of destruction with cyber-warfare disrupting social, political, and economic systems. It destroys electronic infrastructures and steals secrets from foreign nations.

Cyberspace remains the highest source of cybercrime threats as an extension of the diverse illegal activities. Wall & Williams (2007) cited the police as a body responsible for maintaining and preventing crime challenged by new cyber threats emerging daily. There is an increase in cyber communication technologies. Cybercrime issues are the extension of adverse illegal behavior. McMahon et al. (2016) cited that the tech-savvy criminal behavior illustrated more sophistication located throughout the globe that accesses data, steals identity, and confiscates money, and private information.

Cybercrime and Espionage

The crux of cybercrime and espionage is learned and suggests that individuals learn negative cybercrime attitudes and techniques from their relationships with criminal peer groups and associates. Cillufo and Cardash (2013) argued the main worldwide actors that dominate cybercrime espionage behavior are Russia and China, and they both have been labeled as the greatest strategic threats to the USA. The cyberspace domain works with great sophistication, anonymity, and interconnectivity. Broadhurst et al. (2014) affirmed that cybercrime hotspots have potential links to Eastern Europe and the former Soviet Union with increasing concern regarding cybercrime in China.

The Worldwide Web (www) has opened the door to worldwide cybercrime. Chabinsky (2014) asserted wireless is not worry-less; cyber spies and cybercriminals incorporate wireless networks with Wi-Fi hotspots that appear to be legitimate and are set up by hackers (p. 29). It is paramount to ensure secure passwords are reinforced on the Internet, employing HTTPS and not HTTP. The "S" confirms 'security' and reinforces safeguards for social networks, e-mails, online retail purchases, and banking.

Cybercrime and Constant Change

Cybercrime is constantly changing and has an intensity to grow with increased vulnerability in the anonymity of cyberspace and innovative technologies. McMahon et al. (2016) expressed that cybercrime was increasing with losses in the USA totaling 18 billion and individuals were putting every possible thing on the Internet without properly securing the data and information. Wide-open data and availabilities are resulting in increased cybercrime escalation and proverbial opportunities. McCourt (2014) contended that cybercrime is the number one threat and is finally gathering attention to mitigate risks, eliminate vulnerabilities, and prepare for resilience (p. 31). The critical need is to address proactive cybercrime plans, assess the problem, evaluate possible risks, and establish collaborative teams with workable procedures and contingencies to reduce and eliminate software theft, computer fraud, salami-slice fraud, and corporate espionage. It demands identifying potential vulnerabilities, rather than after-the-fact to protect and secure the multiple cyber-assets. Innovative Internet global cybercrimes, systematic cyber schemes, and cyber scams are established in cyberspace throughout the day.

Since 9/11, the ever-changing cyberspace and the innovative Internet have resulted in enormous challenges for police personnel. Clarke and Newman (2007) cited that after 9/11 the USA changed everything, and local law enforcement demanded partnerships, coalescent collaboration, and intelligence-led police. The computer-aligned interconnected Internet electronic infrastructures provided opportunities for the escalation of cybercrime with greater challenges to police personnel. The first responders have a multitude of challenges in protecting vulnerable cybercrime targets by utilizing cybercrime skills, knowledge, and understanding. The Internet has evolved presenting cyber criminals with a rich pool of anonymous cyberspace communication, a storehouse of vulnerable data, high-level technological transactions, and an exponential amount of ongoing knowledge (Miller, et al., 2014; Siegel & Worrall, 2017).

Broadhurst et al. (2014) affirmed that today most organized cyber-attacks are skilled technicians who apply their knowledge to criminal activity (p. 2). Individuals tend to think they control their actions; however, due to the open available global Internet, there are unprecedented cyber-criminals focusing on illegal data-gathering activities. The Internet predicts what an individual enjoys, purchases, and garners from entertainment to work; the journey can be positive or negative. It opens and avails the data and information to a wide range of cybercrimes and cybercriminals. Cybercrime has evolved from the foundation of sharing knowledge and intelligence-sharing to multiple cybercrime challenges, cyber-attacks, and cyber-terrorism (Siegel & Worrall, 2017).

Cybercrime Challenges and the Experiential Learning Theory

The compelling challenges and ever-changing global cybercrime encompass cyber-technological economies rapidly evolving with the trajectory of new Internet vulnerabilities permeating daily. It affects entire communities, cities, and nations as cybercrimes escalate. Kolb's (1984) paradigm shift of experiential learning theory (ELT) efficiently works when applying the growth, development, and experiences of police personnel in a sequential cyclic learning process. It functions to obtain wealth and knowledge regarding cybercrime challenges in a pragmatic manner. Kolb's (1984) ELT was established to: provide the foundation in the *concrete experience* (doing and having the cybercrime learned experience), move to the second cycle of *reflective learning* (reviewing and reflecting on the learned experience); build on the third cycle of *abstract conceptualization* (summing up the learned cybercrime training experience); and arrive at the fourth sequential cycle of *active experimentation* (planning ahead, achieving, and activating what has been learned). ELT is a learning process that moves sequentially from theory to pragmatic achievements. It confronts cybercrime issues and expresses workable strategies for police personnel to eliminate cyber theft and mitigate cybercrime challenges. It requires integrating intelligence, information, and experiences in diverse modalities (Dempsey & Forst, 2013; Kolb, 2014; Martin, 2015).

Siegel & Worrall (2014) maintained that cybercrime presents multiple police controversial confrontations. Today, cybercrime is on the rise due to the scientific collaboration of the global economy and the expansive operations of technology. They extend perpetually in the global world. Pelgrin (2013) confirmed that cybercrime

complicities escalate. It is essential to know what constitutes cybercrime risks and how to reduce the increase. It is essential to understand the intimidating fear of cyber threats and what are possible preventive measures. Police personnel experience difficulties attempting to contend with the escalating cybercrime challenges.

New challenges to cybercrime were expedited by the introduction of Wi-Fi which posed an increased threat to information security (Chernukhin, 2014). The convenience of the cyber-Wi-Fi provided adverse cyber-advantages with extreme susceptibility. McCourt (2014) maintained that cybercrime is a business and not an Internet technology problem. It challenges and interconnects the unprotected with defenseless access to cybercrime points. Unprotected smartphones increase cyber-attacks. Chernukhin (2014) asserted that the main disadvantages of the Wi-Fi cyber security networks were the unauthorized access due to the low-level protection. Opportunities perpetuate hackers to "crack" cyber-Wi-Fi networks through the anonymity of the Internet, weak firewalls, and the global worldwide cyberspace. Kolb's (2014) ELT established the detailed alignment of the cybercrime evidence-based qualitative phenomenological research. It played a major role in design as it assisted in orchestrating cybercrime research.

Wall (2008) emphasized that the cybercrime term described crimes that transpire within virtual environments and many components of the critical infrastructures (p. 47). Throughout the years' cyber technology has grown tremendously; although, the critical infrastructures have substantially lagged behind and become outdated (Dempsey and Forst, 2013). The encumbrances of cyber-security updates are limited. Obsolescence cyber technologies are dysfunctional and can damage the cyber-controlled critical

Infrastructures, such as the energy, water, and traffic lights (Levi, et al., 2015).

Critical Infrastructure

The critical infrastructure includes cyber-controlled connections which affect and control all components of the USA's interconnected systems. Singh et al. (2013) stated the "urban infrastructure is now under constant threat of cyber-attack with a vast array of disasters-both natural and man-made" (p. 22). Each day the broken infrastructures are somewhat inoperable. Singh et al. (2013) argued that one of the largest vulnerable cyber-driven infrastructure systems was derived from wireless supervisory control and data acquisition [SCADA] (p. 23). There are many unseen catastrophic cyber systems utilized to control the infrastructures of communities, cities, and countries.

The cyber-technology systems activate and control substations, which flow through pipelines, water, and sewer systems. The gas and electrical power flow through the grid, which controls the timing of traffic signals and other Internet operations exposed to cyber-attacks (Levi, 2015; McCaghy et al., 2008; Sund, 2007). The cybercrime technological landscape has evolved tremendously. Its growth and capabilities have expanded and exposed evincible conditions. Telecommunication switches and cellular towers with underground fiber-optic cables provide vulnerable cybercrime attack opportunities (Czescik & Siemianowski, 2014; Sund, 2007).

Cyber-controlled infrastructure connections are currently deficient and open to momentous and weighty inadequate consequences. Czescik and Siemianowski (2014) affirmed how cybercrime threats were geared toward critical infrastructure with problems increasing daily. The Internet does not have the capability to readily provide

the comprehensive information to identify where and who are the anonymous perpetrators committing the cyber theft, fraud, or cyber-attacks.

Unauthorized telecommunication, cyber-attacks, and cyber warfare can ravage main infrastructures. Illegally accessed cyber infrastructures can result in raw sewerage pumped into drinking water systems, derailing of trains, and shutting down elevators. It can delete or replace medical data in hospital databases, disorient 911 systems, and sabotage air traffic control. It can launch failures in heating and cooling systems and deploy erroneous information to airports and hospitals (Czescik & Siemianowski, 2014). In addition, the critical infrastructure includes power plants, roads, water systems, and transportation controlled by cyber-installation facilities. Cybercrime has increased technologies to power, jeopardize, and destroy aircraft, airfreight, and even airlines.

The expansion of the Internet has exploited and jeopardized online cyber vulnerabilities attacking many major infrastructures. Koppel (2016) asserted in what ways the exploited Internet furnished instant access to operations: poor rail systems' safety and security; enabled critical infrastructure to inappropriately function; inadequate healthcare systems; and contaminated communications networks. Critical services are endangered by the vulnerable exploits of cybercrime hackers shifting potential threats to weak cyber security systems. Cyber threats and law enforcement, along with the legal framework, are often not maintaining pace with the evolution of technological cyber threat globalization (Broadhurst et al., 2014). The cybercrime threats continue to challenge local law enforcement personnel and their preparedness in the cybercrime infrastructure issues. Miller et al. (2014) indicated that damage to the USA's critical

computer systems could devastate the entire nation. It would place it in jeopardy and pose a debilitating catastrophic threat to our national security. Koppel (2016) indicated that the Internet provides instant access to computerized systems and maintains equilibrium for electric power grids. The very structure flows through controlled computers to balance supply and demand. Cyber-attacks could destroy electrical grids.

USA Electric Power Grids

The United States has three electric power grids that distribute and generate electricity throughout the USA depending absolutely on computers; taking down any part of a grid would scatter millions of Americans into darkness (Wexler, 2014). The aging cyber-grid is fragile and open to major cyber-attacks. Koppel (2016) argued that if a sophisticated hacker gained access to one of the systems, the consequences would evoke total devastation. Protecting critical infrastructures is essential and an integral component for police personnel to discover perpetrators. Identification and investigation of potential offenders are imperative to protect the economy and the cyber-oriented technical world. Ionita et al. (2016) contended that in the Internet world, cyber security assurance is critical to protect critical infrastructures and defend against cyber-attacks that arrive from the Dark Web or Dark Tor. The infrastructure has not maintained new innovative cyber-technological excellence with current cybercriminals' scientific digital skills. There are challenges that view the Internet as a major concern in illegal activity and profitability proliferating losses in the billions (Siegel & Worrall, 2012). Some cybercriminals have a corrupt and pertinacious focus on ulterior cyber activities.

The prominent growth of cybercrime has failed to circumvent cybercrime and protect the infrastructures. Hinduja & Schafer (2009) expressed that owing to the boundless Internet architecture, police contend with computer hardware-software theft; and network security breaches. It includes electronic commerce fraud and high-tech deviance, as well as the propagation of the extremists' agendas (p. 279). Cybercrime challenges heighten the increase of criminal activity and the need for cyber-security. Pisaric (2017) asserted the great need for cyber knowledge and learned skills with well-trained police personnel. Cyber technological preventive tactics are necessary to protect electrical grids and eradicate the proliferation of cyber-attacks.

According to Koppel (2016), many individuals remain oblivious to the potential well-targeted cyber-attack catastrophe. The cyber-attacks and cyber-terrorism phenomenon have astronomical challenges that have the capability to devastate and destroy a vast array of crucial vulnerable entities. The study provided culpable phenomenological research to efficiently work with police personnel and collect cybercrime data. It researched cyber-criminalities and provided potential inductive scientific investigations. The study added pertinent information to protect people, places, and agencies/ Constructive preventive measures evolved focusing on infrastructures and other cybercrime challenges. The Stevens Institute of Technology (2012) emphasized the need for comprehensive cybercrime security capabilities with critical thinking and understanding. Issues and egregious confrontations have arisen from the vulnerabilities of cybercrime as it tends to grow and metastasize. It requires proficient law enforcement personnel equipped with basic cybercrime knowledge, preparedness, and instructions.

Meaningful and scholarly law enforcement cybercrime preparedness provides police personnel to perform the essential skills for the study.

Law Enforcement Personnel Preparedness

Law enforcement experts are concerned that anonymity and vulnerability made it difficult to catch cyber-criminals (Sund, 2007). Cybercriminals are well-hidden. Czescik and Siemianowski (2014) referred to cyber-criminal activity as invisible threats and noted entire cities must be involved in the fight to protect critical infrastructures because police actions may not be sufficient. The police personnel's actions are not engaged enough to combat cybercrime as the Internet is exploited throughout the day. Flory (2016) argued the inability of law enforcement to communicate with other cybercrime investigators during real-time investigations has created exponential difficulties. Local police personnel are confronted with escalating cyber-attack challenges promoting the need to obtain cyber tools, advanced technologies, and investigative programs to combat cybercrime (Miller et al., 2014). A conflict paradigm plays a critical role in understanding that individuals in society have fundamental differences and those in power often control laws and societal elements. In essence, cybercrime legislative laws and policies are controlled by the powers that are in authority.

Henceforth, it is known that many law enforcement personnel, not sworn and certified by MCOLES (Michigan Commission on Law Enforcement Systems), often receive lower pay and less money than sworn personnel. Law enforcement personnel preparedness and mandated cybercrime ramifications are essential to combat and eradicate cyber-attacks (Berg, 2007; Walker & Katz, 2013). Cybercrime is evolving

on an explosive upward trajectory, changing daily, and resulting in challenges to law enforcement personnel. Creative cyber understanding plays a critical role in the preparedness of police personnel. It is oriented toward evolving cybercrime strategies that align the systematic structure and scientific phenomenology explanations. The study revealed the phenomenological paradigm evoking what law enforcement personnel revealed concerning the cybercrime preparedness experiences. It was essential that the cybercrime training was explained addressing the positive and negative learning processes and procedures. Cybercrime preparedness focused on what worked and what did not work. It identified inductive thinking and any underlying unknown challenges.

Challenges and Performing More with Less

Quintessentially, due to government budget cutbacks in 2007 and 2008, law enforcement agencies began operationally to perform 'more with less.' Financial cutbacks affected law enforcement departments and the first entities reduced and eliminated were preparedness and training (Siegel & Worrall, 2014). New innovative cybercrime preparedness is needed to strengthen and provide the best practices to police personnel to equip and reduce cyber-attacks. Stevens Institute (2012) indicated that cybercrime awareness is not a static or fixed entity, but a dynamic process.

Much of the USA is confronted with cybercrime in a variety of ways. In accordance with the Los Angeles Sheriff's Department, hackers, and crackers infiltrated the agency at least once every day. The article, "Cyber Terrorism: Preventing Online Assault: Is Your Agency's Network Ready to withstand Cyber Terrorism Attacks from Anonymous" (2014) expressed that it is now more critical for police to become cognizant

and protect themselves against cyber-terrorist attacks, which are mainly financial and/or political. Articles have asserted that anarchist hackers caused multiple city website crashes. The cyber-attacks eliminated law enforcement departments' radios for several days. At times it required police personnel to have only access to communications utilizing text messages (Dempsey & Forst, 2013; Jordan, 2016).

Law enforcement personnel preparedness training has not been equipped due to the increased evolution of cybercrime and budgetary constraints (Miller et al., 2014). Police personnel has received constructive feedback and comments from citizens regarding cybercrime incidents. Many have indicated enhancing cyber-security measures. The state of Michigan spent $22 million a year on innovative cyber security and proactive cybercrime measures. The allocated budgetary funds were increased by an additional 7 million in the allocated budget for 2015 and 2016 (Gray, 2015).

Certain parameters were required to participate as qualified police personnel skilled in cybercrime preparedness. They had to be equipped with certain protocols and with the necessary cybercrime training (Instructor, Google, Video, DVD, CD, ZOOM, YouTube, Internet, or Self-taught). The cybercrime skills and knowledge at the police agency had to incorporate a certain amount of cybercrime technology (Siegel & Worrall, 2017). Many police budgets are limited. Law enforcement personnel have at times faltered in cyber preparedness and practical skills to handle the emerging illegal cyber-attack schemes (Broadhurst et al., 2006). Cybercrime scams transpire daily. Wall (2011) argued that realistic expectations of cybercrime training are needed, especially concerning what police can and cannot do. Cybercrime and illegal scientific forensic

technology continues to escalate. Cybercrime intersects numerous jurisdictions simultaneously. They consist of hate crimes, consumer fraud, cyber stalking, security theft, software piracy, corporate espionage, bank fraud, and terrorism (Podgor, 2002; Schjolberg, 2008). The police personnel research focused on cybercrime preparedness that provided rich results from the collected data. It was critically assessed and evaluated listing the changing transitional cybercrime technology and social media.

Technology and Social Media

Technology and social media play critical components in cyberspace and cybercrime. The 21st century demanded that brick-and-mortar (local, state, and federal) governmental organizations and professional agencies possess an active Internet-based website with cybercrime gains from many accounts. They include Twitter, FaceBook, Apple, and Google. Other doors were opened as an array of cybercrime utilizing artificial intelligence evoked with ongoing consistency, such as pornography and identity theft. In 2014, Apple and Google established several diverse plans in social media to strengthen data stored on smartphones to encrypt the data using their operational systems and generate illegal cybercrime activities (Dempsey & Forst; 2013). The Internet's two operating systems with encrypted messaging applications were popular with ISIS and ISIL were extremist violent groups in the Islamic State. McMahon et al. (2016) asserted that most cybercrimes are motivated financially and in various forms. One of the common threads utilized was social media facilitating illegal anonymous Internet activities.

According to McMahon et al. (2016), the basic thread of cybercrime is the utilization of social media to facilitate negative cybercrime Internet activities. Law enforcement agencies require digital technological methods and mediums. There are specialized cybercrime units and task forces. The advent of the Internet and high-technological social media engages high-level ultra-density in cyber security within urban cities (Singh et al., 2013). Social media has played a critical role in cybercrime, while engaging, disseminating, and entertaining information. Many ethical issues arise with real-world strategies when addressing the relationship between social media, cybercrime, and police personnel. Siegel & Worrall (2014) attested that cybercrime consisted of the integrated system of smartphones, online banking, and operational cyberspace which are key components of social media in our society; it provides pervasive anonymity to cybercriminals. Pelgrin (2013) acclaimed the use of social networking websites gathered cybercrime information and was an invaluable tool for police personnel, as cybercriminals used social media with complicity against law enforcement daily.

The expansion of social media has provided adverse opportunities due to the exposure of personal data and information (Miller et al., 2014). Social media has the power to report and publish cybercrime activities, whether it promotes excessive public fear or has a negative effect to reinforce and strengthen illegal cybercrime activities. It exposes information that instills criminal opportunists provoking danger to commit cybercrimes and cyber-attacks by viewing the locations and Geo-tags. Miller et al. further contended that social media and websites are changing the ways and means that law enforcement agencies. This entails communicating with society. It includes the utilization

of Facebook, Twitter, YouTube, Nixle, Snap-Chat, Google, and Geo-tagging. Social media assists greatly in obtaining cybercrime tips in criminal investigations. The advent of social media websites includes the world's top social networking sites.

Geo-tagging is a process that combines the Global Positioning System (GPS) with information technology (Miller et al., 2014). GPS utilizes military satellites that orbit the earth, providing a constant stream of data locations that can result in potential devastation and danger. Ramirez et al. (2016) asserted that Geo-tagging has become prevalent on electronic social media website devices, as well as smartphones and cameras equipped with built-in GPS. The Wi-Fi plays a major role. The Wi-Fi wireless networks, MAC (media access control), Apple iPhone, and other tracking software are only a few that identifies consumers' locations with viable information (Chernukin, 2014). Identifying locations can pose threats to victims and result in devastation as victims attempt to hide from perpetrators in domestic violence and sexual assault cases.

Horrendous criminal actions are provided through unauthorized and illegal use of Wi-Fi, often unprotected without secure passwords. A beacon can be embedded to send a signal from sensitive digital cyber-ware; it tracks and identifies the individual's location and personal addresses (Ramirez et al., 2016). The cyber tracking device can assist police personnel in locating a criminal and it might emanate havoc to hidden victims. Social media shares crucial information resulting in great financial, personal, and physical vulnerabilities. Koppel (2013) cited that social media reports the extensive costliness of online cybercrime piracy and inconvenience to victims. Social media has evoked

accelerated information resulted in exposed irremediable victimization. Rosenzweig (2013) identified five gateways of Internet cybercrime vulnerability: (1) instant action at distance permeable and unlimited cyber borders; (2) asymmetries of cyberspace with many weak limited firewalls; (3) anonymity in the phenomenon of cyberspace that is part of our culture; (4) borderless operations without USA checkpoints; and (5) the difficulty and nightmare scenario in being unable to identify codes.

Comments in the police personnel preparedness factors can equip and prepare preventive cybercrime measures before it happens. It requires upfront implementation with necessary actions to mitigate cybercrime. Police preparedness activates the entry-level role using necessary steps in apprehension, investigation; and combating cybercrime (Siegel & Worrall, 2014). There are multiple changes necessary to combat cybercrime focusing on integrity, ethics, and information gathering (Broadhurst et al., 2014; Miller et al., 2014). The anticipation of cybercrime problems demands strategies.

After the horrid catastrophic tragedy of 9/11, the symbiotic unity of intelligence, information sharing, and systematic training occurred and embodied the collaborative approaches among all law enforcement agencies. This included cybercrime in federal, state, tribunal, county, municipal, hospitals, colleges/universities, and other agencies. Hinduja & Schafer (2009) asserted that during the last two decades local police worked with the advent of increasing public awareness. It united a coordinated collaboration in the understanding of police personnel with shared teamwork and investigative intelligence. In earlier research, Hinduja (2004) heartily emphasized training as necessary

for front-line officers (first responders) working with cybercrime investigation units, interrogations, computer evidence, and proper paperwork (p. 352).

Cybercrime is paramount and a constant increasing cyber threat with cyber-attacks escalating with the advent of social media. Cyber-attacks have increased and expeditiously developed (Miller, et al, 2014). Cybercrimes continue to grow daily at an astronomical rate. Wexler (2014) emphasized that new cyber threats increased at such a rapid rate that police departments have not had sufficient opportunities to prepare and identify their roles in the prevention and investigation of cybercrimes. It elicits eminent cybercrime challenges as social media plays a critically significant role. The 9/11 incident impacted the transitional cyberspace as police personnel worked to eliminate the hidden distortions within the USA by sharing data, collaborating, and becoming more transparent (Dempsey & Forst, 2013). The Internet computer-aligned social media cyber-threats are intertwined and continue to increase. The Internet's interconnected electronic infrastructures exposed potential cyber-threats in social media and provided opportunities for intense escalation of cybercrime and cyber-attacks (Siegel & Worrall, 2014).

Social media is a wide-open range on the Internet that transforms daily presenting criminals with rich pools of data, communication, and a wealth of knowledge (Jordan, 2016; Miller et al., 2014). Today, cybercrime is tied into the continuity of social media and has escalated becoming a pandemic. Due to the global economy, operations of technology extend the problems perpetuated daily in the world of cyberspace (Siegel & Worrall, 2014). Law enforcement personnel experience multiple difficulties attempting to

contend with the growing cybercrime challenges. The lack of cyber security is one of the heightened critical risks of cybercrime in addressing criminality (Chabinsky, 2014; Chernukhin, 2014). The role and anonymity of social media promulgate egregious and detrimental opportunities increasing cyber terrorism and ongoing cyber breaches.

Role of Popular and Social Media

The role of popular social media created a strong interconnection to learning that shaped the actions and presence of messages (Van Voorhis et al., 2007). The cybercriminal activity affected many personal and business accounts. Multiple corporations never reported the acts of the complicit cybercrimes. Many operations denied the compromised contacts the cyber-attacks. The Internet, social media, and other digital divides exposed a magnitude of public and private information extending the availabilities to additional compromised incidents (Siegel & Worrall, 2014).

Multitudinous social media and challenges have altered the landscape of technology for law enforcement personnel. The extended role of social cyber-media and popular media includes Instagram. It has allowed increasing technologies in the realm of electronic interactional cyber-media, opening doors, and increasing pernicious activities to exacerbate cybercrime and cyber-attacks. Cyberspace promulgates extensive opportunities for the daily increase in cybercrime. The reflections and criminal thoughts on cybercrime on the Internet have provided information that is beneficial in law enforcement communication and collaboration in the world of social media. However, many cybercrime websites have provided viable accessible links to profit and non-

profit corporations making them susceptible and penetrable to malware attacks (Hinduja & Schafer, 2009; Siegel & Worrall, 2014). The role of the Internet's social media emits opportunities that provide significant openings for cyber-attacks. In essence, it allows police personnel to prepare and establish a need for the sense of complicit social media, which critically investigates and shares transparency emitting information in all areas. It works to expose the truth, as well as erroneous cyber information (Martin, 2015).

An additional documented source is the Federal Bureau of Investigation (FBI), which indicated that in 2014 the Internet Crimes Complaint Department (IC3) received cybercrime complaints totaling over $800 million dollars; each month approximately 22,000 cybercrime Internet complaints were received (FBI, 2014). Social media and Internet cyber-technology change throughout the day. Cyber-attacks increased as social media was utilized as the medium to commit more extensive, insidious, and long-range crimes (Hinduja, 2007). It is essential to stay abreast of cybercrime with the new cyber-applications, cyberspace techniques, and innovative technologies. Sales (2015) expressed that intelligence systems rely on technology to protect classified cyber-technology and prevent leaks; however, no technological bullet will prevent all leaks. Core cyber-engineered technologies are necessary to work and explore new methods and devices.

Exploring Cybercrime Technology

Broadhurst et al. (2014) emphasized the importance of exploring technology and the scope of cybercrime in conjunction with the theoretical and empirical challenges. Cyber technology is changing, and cyber security must work to adequately establish an

innovative paradigm that protects the vulnerable; not resulting in fear, but enabling the victim to visibly view the perpetrator (Siegel & Worrall, 2012). Dempsey and Forst (2013) indicated the need for cybercrime collaboration with police departments and other agencies due to the escalating partnership of wrongdoing in the cybercrime landscape.

According to McCuster (2006), the world is much more vulnerable than is recognized in the quantity of information that floats in cyberspace with tremendous amounts of escalating cyber-attacks and cyber-terrorism. The Internet continues to expand with social engineering and control of insurmountable data shared throughout the world as individuals and systems become more cyber-dependent. Since 2010, Internet crime has increased at exponential rates (Siegel & Worrall, 2017; Smart, 2015).

Exposed Attacks, Threats, and Social Media

One of the exposed attacks resulted in billions of individuals' data being hacked in a yahoo attack that occurred in 2013 and was not revealed until December 2016. There are extensive problems with the increase of cybercrime and the failure to report immediately the cyber-attacks to victims. The exposed victims are targets for additional cybercrime. Cybercriminals exemplify their knowledgeable skills in the daily activities of cybercrime, cyber-attacks, and cyber terrorism in worldwide cyberspace. Forst (2013) contended that there was a particular concern about the need to provide the necessary technology and training to law enforcement personnel. There is a critical need to become more knowledgeable to compete with the cybercriminal's advanced social technologies as perpetrators continue to commit high-level engineered electronic cyber-attacks.

Cybercrime is an evolving and expanding threat. Broadhurst et al. (2014) asserted that the insurgent and extremist groups are tied in politically and economically to the fear factors of cybercrime. Banks are being compromised. Innovative cybercrime technology is engaging in penetrating banks throughout the world with data compromised and funds stolen (Sales, 2015). Due to advanced cybercrime development, it is difficult to investigate and regulate through obsolete police channels of cyber-attacks (Siegel & Worrall, 2012). Some police personnel are cybercrime trained, although many are not equipped for the high-level quintessential cyber technology.

Cybercrime and cyber-attack technology dominate imminently and invincibly in the USA system as cyber technology increases. The pivotal factors of technology involve human precisions, worldwide cyberspace, and the heightened speed of cybercrime execution (Broadhurst et al., 2014). It is surmised that high-level engineered cyber security is necessary to prevent unprecedented cyber breaches, cyber leaks, and cyber terrorism. It is a reality that the weakest link in an organization opens greater opportunities for cybercrime devastation. At times it is difficult for police personnel to understand and prevent cyber-attacks without basic cybercrime preparedness, training, and experiential learning. Law enforcement personnel have great opportunities to provide the essentials to mitigate and uproot cyber-attacks. Skilled and competent preparedness renders opportunities to provide preventive cyber breaches and cyber leaks. The research might allow police personnel to align and orchestrate workable ways to assist in eliminating the constant commission of cybercrimes and cyber-attacks with viable cyber security.

Cyber Security, Breaches, and Leaks

The lack of cyber security is one of the extreme risks of cybercrimes and reveals a great depth of cyber data encouraging opportunities for multiple breaches (Wexler, 2014). Cybercrime security represents an immense continuity besieged by data placed online without the proper security, and weak with easily targeted firewalls that can be easily penetrated. Hammond (2015) affirmed that cyber security was the key issue raised by global policymakers and discussed it with global and cyber representatives. The cyber-security issues continue to emerge. Proactive cybercrime security issues are necessary and must be deployed through a broad sense of sophistication (McMahon et al., 2016). Cybercrime in the digital ecosystem has evoked threats throughout the global spectrum. Cilluffo and Cardash (2013) affirmed the digital revolution provided power to a host of new cybercrime actors in the domain of national and international security.

Cybercrime training and security are greatly needed. The rapid immediacy in proficient cybercrime training and security assists in eliminating the escalation of cybercrime activities (Dempsey and Forst, 2013). It is necessary to confront cybercrime challenges and ensure proper investigation. In accordance with Cilludo and Cardash (2013), the status of cyberspace is viewed as a domain, explained as a battlespace, which is analogous to the sea, land, air, or outer space. It constitutes the cyber-threats and conflicts in the digital architectural landscape. Strategic innovative cybercrimes increase daily. The intelligence and military officials currently utilize cyber security technology to protect classified information with strengthened firewalls making it difficult to compromise protected data (Sales, 2015). Police personnel must regulate, rethink, and

reinvent the approach to cyber security with established workable proactive methods.

In accordance with Gercke (2012), cyber-security and cybercrime issues cannot be separated in an environment that is interconnected. There are many aspects of cybercrime impervious to cybercrime security that implements technological cyber security paradigms. Cyber security evidenced the need for better plans, preventive actions, and procedures that can more efficiently equip and prepare police personnel (Siegel & Worrall, 2012). Cyber security, along with policies and procedures is necessary to prevent cybercrime incidents, analogous to cases like Edward Snowden.

Edward Snowden-NSA Contractor

Edward Snowden was a contractor for the National Security Agency (NSA) who leaked classified government cyber-surveillance documents to the press (Pearson & Smith, 2013). Many governments employ the Internet for cyber operations. Snowden disclosed that the USA engaged in massive cyber-surveillance programs (Broadhurst et al., 2014). Snowden's case was referred to as an *insider threat;* as Snowden infiltrated and shared huge amounts of diplomatic military and intelligence documents with other nations (Sales, 2015). An insider threat is a former or current employee or business partner that utilizes malicious intent against an agency or organization. The individual has authorized access to the organization's data, network, or systems; and the insider utilizes the organization's data or information to negatively access, expose, and affect the integrity and confidentiality of the classified data belonging to the organization or agency (Capelli et al., 2012). Snowden initially fled from the USA to Hong Kong with espionage information. Finn & Horwitz (2013) asserted that the USA federal prosecutors charged

Snowden with espionage and the theft of government property. Snowden then left Hong Kong and took refuge in Russia. The United States Attorney General Eric Holder generated a letter to Russia and requested Snowden to be extradited to the USA. Attorney General Holder indicated in the letter to the Russian Minister of Justice that the USA would not torture or render a death sentence against Snowden when he returned to the USA (Cillufo et al., 2013). It was to no avail. Snowden did not return to the USA and took up residence in Russia.

There was no extradition treaty between Russia and USA; therefore, it was a federal case that did not transpire and was non-operational. It accentuated the imperativeness for the USA to implement greater federal cyber security laws and mandates to prevent a repeat Snowden espionage incident. Cybercrime security threats continue to challenge police personnel. Since 2005, the federal government has reinforced the Espionage Act of 1917, making it a crime for government employees or contractors to reveal national defense information (Sales, 2015). Cybercrime security breaches are leaks with sedulous cybercrime security constantly coming into question.

Cybercrime Breaches

A cybercrime breach is the failure to abide by the laws or mandated rules and regulations. It is obligatory and binding when applied to the stated stipulated laws, ordinances, policies, and procedures. Sales (2015) contended that there are two kinds of cyber-leaks, the supply, and the demand. The supply side is where government restricts revealing entrusted secrets and might prosecute employees or contractual persons; whereas the demand side entails government could restrict leak recipients from

distributing classified information and might file criminal charges against the identified individual, journalist, or press. Cybercrime statutes edit and decree-laws with ordinances are compulsory in precluding and averting cybercrime. Mastery and skillful cyber security laws with cyber-technology are essential to protect cyber information.

Czescik and Siemianowski (2014) referenced the importance of addressing cyber security, whereas cryptographic techniques and steganography were believed to be primary sources of espionage. Cryptographic techniques are encryptions that involve the use of algorithms that change plain text into a form that cannot be read without the enabling key (Broadhurst et al., 2014). Steganography is the method that is encrypted and hides information; it involves hiding it among other publicly available data storage or retrievable captured digital technological information within electronic devices.

Several well-publicized cybercrime attackers, hackers, and leakers were identified by Sales (2015). They were: (1) Donald Sachtleben 2013, an FBI agent who leaked information regarding a foiled Yemen terrorists' plot to bomb commercial airlines; he pleaded guilty and was sentenced to 3.5 years in prison; and (2) David Petraeus in 2015, retired general and CIA director who shared classified information with his biographer-mistress. He pleaded guilty to a misdemeanor and was sentenced to probation for two years and a $100,000 fine. Police personnel often gather information and are at the frontline in the awareness of cyber-attacks and cyber-terrorism; they bring invaluable access to millions (Dempsey & Forst, 2013). Cybercrime leakers are surreptitious, egregious, and extremist in sharing locations and diehards in illegal cybercrime relations.

Cybercrime Leakers

Government officials continue to disclose, and leak classified cyber-information; persons such as Bradley "Chelsea" Manning and Edward Snowden divulged huge military and diplomatic documents of intelligence (Sales, 2015). The Espionage Act was utilized by President Barak Obama nine times to regulate the cyber-leaks for disclosures of unauthorized classified cyber-crime information. In June 2017, Reality Leigh Winner, a 25-year-old federal contractor with top-secret clearance and military background was charged with sending classified reports of Russia's interference in the 2016 presidential election. The file sent to a reporter at *The Intercept* was discovered and led investigators to Winner. The FBI received a confession. It was the first criminal leak case of President Trump's era. Winner's case exposed the vast array of persons who held government clearances with access to secrets due to the security expansion since the 9/11 attacks.

Approximately four million persons, including contractors and government employees, hold security clearances. It is inclusive of another 1.3 million individuals with top-secret clearances, analogous to Winner. The federal cases depicted and exemplified the elements of espionage under the Espionage Act. Chernukhin (2014) further alluded to the information security challenges of cyber-attacks and Wi-Fi cyber-technologies with low-level protection against unauthorized access. It exposed the great need for additional cybercrime mandates and cyber-security techniques. Additional workable strategies and laws are necessary to prevent the ongoing illegal cyber-hacks, cyber extortions, and Internet predators utilizing the tools of Wi-Fi networks and the Dark Web.

The Wi-Fi, Dark Web, and Cyber-Security Strategies

Chabinsky (2014) emphasized that cyber-attackers and cybercriminals have successfully targeted wireless cyber networks for years. Identity is critical in assessing, understanding, and prioritizing the risks when Wi-Fi networks are deployed. It is necessary that law enforcement personnel are prepared, equipped, and trained to adequately recognize and mitigate cybercrime. It is asserted that equipping police personnel with high-competence cybercrime preparedness and cyber-security entails greater progress in experiential learning (ELT), awareness, and investigation. Ionita et al. (2016) argued that cybercriminals often move their operations to the Dark Web to protect and add anonymity. The "going dark" challenge hinders police progress in the ability to collect data from pernicious persons, criminals, or terrorists (Rosenzweig, 2013, p. 103).

Talmadge (2017) argued that there were several things in May 2017 regarding the *WannaCry* cyber-attacks that occurred in cyberspace. It touched over 200,000 systems in more than 150 countries including the USA. It was the largest cyber-attack in history purported to cost over $4 billion. It was not known if it was committed by North Korea, Russia, or another entity. However, despite the indicators, there was no clear cyber-attacks evidence concerning the culprits' identity. Ransomware is also a criminal hostage power-play. In 2016, the Ransomware cyber-attack victims received computer warnings; if they did not pay within three days, the cost doubled. It was not revealed how many corporations paid the ransom (Talmadge, 2017). A ransomware cyber-attack indicates that no network is 100% safe. All are defenseless vulnerable entities and ransomware can transpire at any time and is a true devious digital-divide technological trajectory.

Many corporations and business assets have established their entire core operations on cyber networks without focusing on sufficient cyber-security plans or futuristic proactive cybercrime strategies. Cyber-security strategies and police preparedness are critical when addressing cybercrime issues. General Motors in 2019 expressed the excessive cost factor of approximately $3,000.00 per month for each cyber-employee to ensure cyber-security.

This empirical phenomenological qualitative study focused on police personnel, cybercrime preparedness, cyber-attacks, and cyber-terrorism. The research data was garnered from Michigan's frontline law enforcement personnel. Cybercriminals continue to discover widespread methods to gather illicit profits with anonymity. Police personnel cybercrime issues arise from the computer revolution and the Internet including the acquisition. Collaborative cyber efforts are addressed by utilizing jurisdictions and content analysis of multiple agencies (Hinduja, 2009). The synergistic police personnel and cybercrime preparedness were the constructive driving forces necessary for Kolb's (2014) experiential learning theory (ELT). It added assurance and applications as an extension of the initial cybercrime preparedness and training utilized in the workplace.

Kolb's Experiential Learning Theory

The important experiential learning theory (ELT) provided the best structure and principles for cognitive alignment in designing, organizing, and selecting the best architectural format and theory for the study. Building upon Kolb's (1984) ELT provided the appropriate paradigm is a systematic plan. It focused on the literature review and research approaches integrated throughout the study. The Experiential Learning Theory

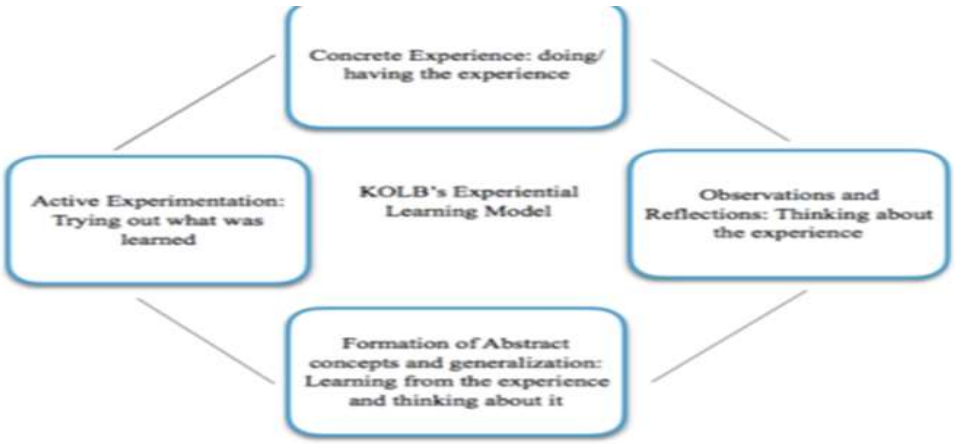
of Kolb (1984) established theoretical adherence as the blueprint to explore the learning experiences of police personnel and cybercrime preparedness in various learning styles with recommendations to uproot the problems. Kolb's (1984) theory-driven thinking and practical achievements required learning levels that built one on another. It initially required one must complete the first to move to the next cycle.

The ELT theoretical model explored and evaluated the data described by the law enforcement personnel's lived experiences while integrating positions in the diverse cybercrime classification and taxonomy. The police personnel explained cybercrime preparedness and reflections. Thoughts and perceptions produced rich in-depth meanings concerning cybercrime preparedness with proactive recommendations. Saks & Burke-Smalley (2014) cited that training required mastery competencies in knowledge and behaviors. The study established and built experiences with meanings for the personnel's cybercrime achievements. The police personnel emanated rich concerns regarding the preparedness with achieved skills applied in the workplaces and communities.

Kolb (1984) viewed experiential learning as an integrated process with each stage being mutually supportive and feeding into the next cycle. However, Kolb (1984) initially expressed, it was possible for an individual to enter the cycle at any stage and follow the logical sequence. Figure 2 entitled Kolb's (1984) *Experiential Learning Theory* occurred when a trainee was able to execute all four stages of the model. No one stage of the cycle was effective as a learning procedure; all were sequentially aligned.

Figure 2

Kolb's (1984) Experiential Learning Theory (ELT)

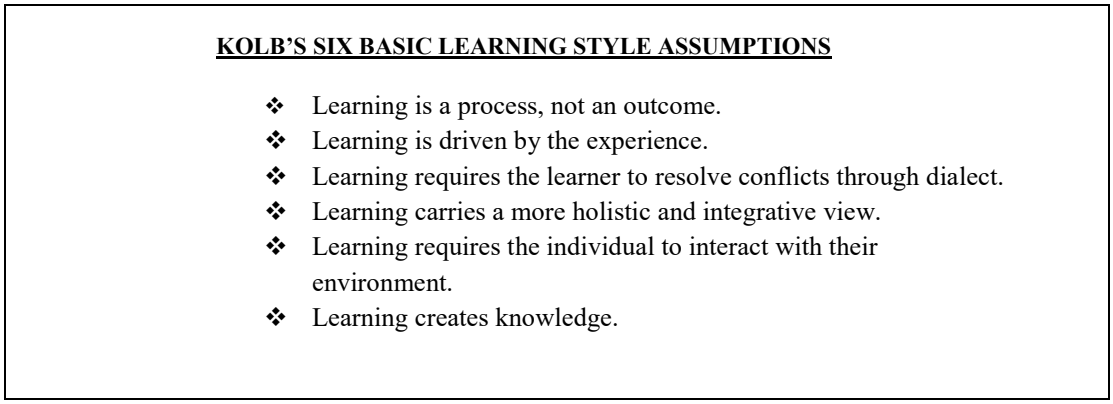


Note. "From Experiential Learning: Experience as the Source of Learning," by D.A. Kolb, 1984. (https://www.researchgate.net/.../235701029_Experiential_Learning), Copyright 1984. Reprinted with permission.

Kolb's (1984) model of experiential learning theory (ELT) was designed and developed to determine the best practices in learning by experience. The six learning assumptions were the basic learning cycle designed by Kolb in the initial theory. The ELT extended holistic procedures in the adult learning process with a multi-linear style and design. Kolb (1984, p. 38) argued that "Learning is the process whereby knowledge is created through the transformation of experience." Both procedures were consistent in what an adult knows and how they learn, reflect, and develop understanding. ELT is a process. Figure 3 entitled *Kolb's (1964) Six Basic Learning Style Assumptions* affirmed knowledge is established through experience and basic assumptions.

Figure 3

Kolb's (1964) Six Basic Learning Style Assumptions



Note. From Experiential learning: Experience as the source of learning, by D.A. Kolb, 2014. (https://www.researchgate.net/.../235701029_Experiential_Learning), Copyright 2014. Reprinted with permission.

The Six Basic Learning Style Assumptions of Kolb (1984) provided descriptive learning statements. It was later realigned as principles and procedures of Kolb as an enhanced version of the four ELT learning styles. Kolb confirmed the six basic learning styles were the expression with assumptions. Learning is a process, not an outcome. In essence, learning continues with growth as actions change. It is not a result or consequence. Learning is driven by experience allowing opportunities for growth and development. Learning requires the learner to resolve conflicts through spoken language. A person has a great ability to resolve inconsistent struggles through articulate learning and communication. Learning carries a holistic integrative view. The individual is wiser from previous learning experiences, becoming more integrative in a holistic approach. Learning requires persons to interact with the environment exposing an intense execution

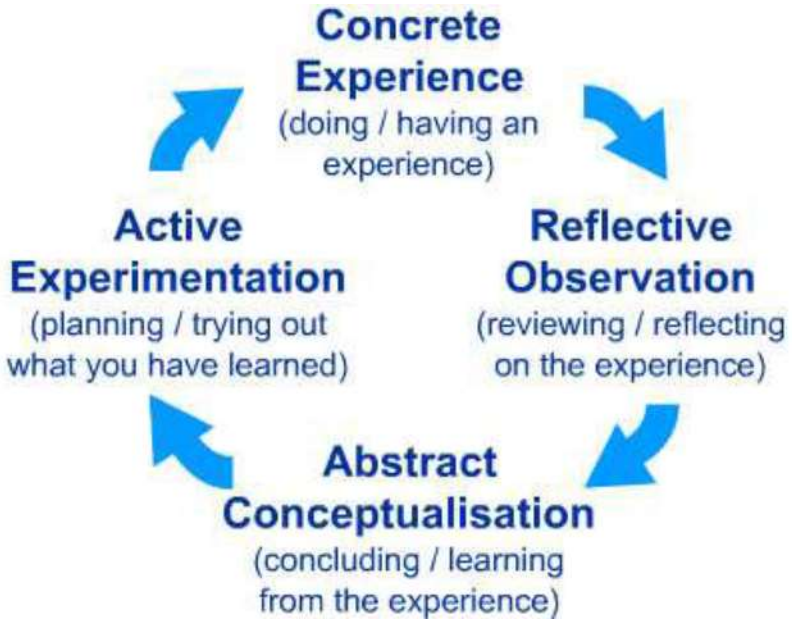
of thoughts and actions. Learning creates knowledge and allows information to stimulate enhanced intelligence. The transition of the six learning styles is prevailing and the extrapolation of Kolb's four ELT cycles.

The four-stage learning cycle of Kolb (1984) was well-designed. It provided both a process to understand the six learning assumptions explaining the cycle of the ELT for effective learning. According to Fenwick (2001), the ELT Cycle required each segment to be learned in sequential order. Fenwick further emphasized there was incongruence with Kolb's experiential learning theory (ELT) and it was refuted by Fenwick because it did not cover all essential parameters. The four-stage learning styles consisted of an extended adjuration to improve Kolb's (1984) ELT Model. Fenwick's (2001) styles enhanced Kolb's (1984) ELT Model. It included four inner and outer environmental circles: the psychodynamic, enactivist, critical cultural, and situative. Fenwick identified deficiencies, including the four learning segments missing from the ELT Model.

The four additional components consisted of the psychoanalytic, situative, critically cultural, and enactivist. The four additional components were built upon Kolb's (1984) initial ELT Cycle. They were divided into progressive environmental ideas and designs including internal and external. The progressive conceptualization of Fenwick (2001) engaged, expanded, and enhanced Kolb's (1984) initial Experiential Learning Theory (ELT) Cycle. Figure 4 depicts the four components in *Kolb's Cycle of Experiential Learning Theory (ELT)*, which aligns the progression with the cyclic sequential events.

Figure 4

Kolb's Cycle of Experiential Learning Theory (ELT)



Note. From "Experiential Learning: Experience as the Source of Learning," by D.A. Kolb, 1984. https://www.researchgate.net/.../235701029_Experiential_Learning, Copyright 1984. Reprinted with permission.

Kolb's (1984) Cycle of Experiential Learning emphasized all four experiential learning forces that influenced police personnel during the learning process. It enlarged and stimulated the igniting force of ELT providing a greater adaptation in learning. McLeod (2010) explained that Kolb's (1984) ELT Cycle evoked empowered clarity. Fenwick (2001) focused on the four-stage learning styles and added four additional components. Kolb's (1984) ELT was identified as the four-cyclic segments. Initially, the *Concrete Experience* was an experience encountered in a new situation or a reinterpretation of existing experiences-having an experience. Secondly, the *Reflective*

Observation of the new experience was of critical importance; it was reviewed and reflected on the experience. It reviewed and reflected upon inconsistencies between experience and understanding. Thirdly, *Abstract Conceptualization* was the reflection that offered an innovative idea or a modified existing abstract. It entailed learning from the experience. Finally, the fourth was the *Active Experimentation* where the police personnel performed the learning in the real world and achieved results in the workplace.

Kolb's (1984) effective learning theory (ELT) was activated when a person progressed through all stages in sequential order, if possible: having a concrete experience; observation and reflection of the experience; formation of analytical abstract concepts with active learned generalizations or conclusions; and the achievement applying police personnel preparedness in the workplace or other entities. It embraced and incorporated innovative thoughts and creative ideas energizing substantive ways to combat the phenomenon of cyber-attacks, or cyber terrorism. It stimulated the problem-solving and decision-making extension of the experiential learning cycle. Kolb's (1984) Experiential Learning Theory (ELT) appeared to be a valuable tool for law enforcement personnel in the cybercrime preparedness study. It worked in understanding the modalities of ELT. It tended to be considered the blueprint for the cybercrime preparedness model, which illustrated the nature of the experiential learning theory.

Cybercrime preparedness and training can enlarge the atmosphere for critical thinking, as well as problem-solving (Wozencroft, Pate, & Griffiths, 2014). The framed experiential learning design conceptualized law enforcement personnel's prior skills, cybercrime preparedness, and the ELT learning styles with procedures. The Experiential

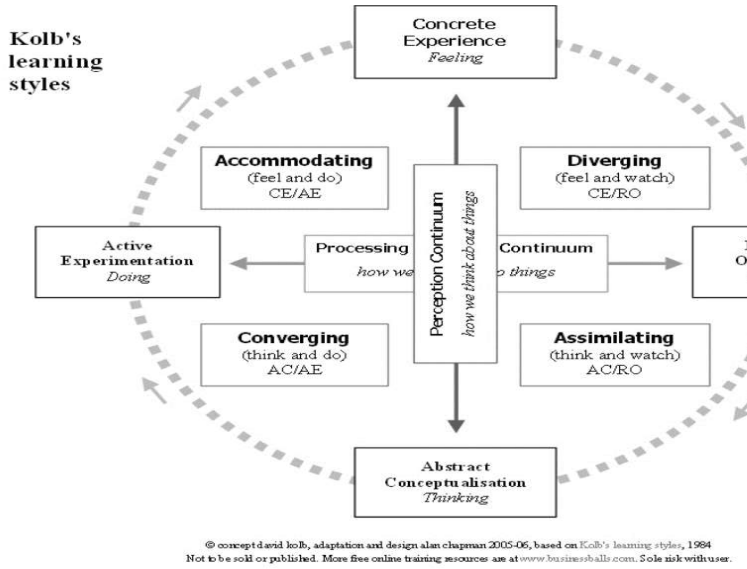
Learning Theory (ELT) of Kolb (1984) was utilized as the theoretical framework for the research building on the principles that learning is a process and valuable tool that enhances and promotes experiential learning and critical thinking. The Experiential Learning Theory (ELT) was initially published by Kolb in 1984. It represented the four-stage learning theory working on two basic levels: the four-stage learning cycle and four separate learning styles (McLeod, 2013). Kolb's (1984) ELT theory touches all bases: Concrete Experience (CE), Reflective Observation (RO), Abstract Conceptualization (AC), and Active Experimentation (AE). The Experiential Learning Theory (ELT) was concerned with the internal cognitive perceptions involving the acquisition of abstract concepts. It was built on the structure to underpin learning with achievements.

The phenomenological empirical qualitative research was an inquiry with the rationale of designs inclusive of the assumptions, goals, roles, and context sensitivity. The theoretical framework was the critical component, and the integrity of the empirical qualitative design was integrated throughout the research. Kolb's (1984) Experiential Learning Theory (ELT) is the blueprint and architectural design serving as a guide and direction to support and build the learning process. The theoretical framework was the foundation for decisions that focused on the approach to answering the basic question: What are the ideas and perceptions of police personnel and prior cybercrime preparedness to combat, mitigate, and eliminate cybercrime? The research methodology of Moustakas (1994) orchestrated the impetus in the foundation to explicate and integrate the learning

styles that are exemplified in Figure 5 entitled *Kolb's (2014) Expanded Experiential Learning Styles* with new concepts in the theoretical paradigm framework.

Figure 5

Kolb's (2014) Expanded Experiential Learning Styles



Note. From "Experiential Learning: Experience as the Source of Learning," by D.A. Kolb, 2014. https://www.scirp.org/reference/ReferencesPapers.aspx?ReferenceID=18937 Reprinted by Permission.

The learning styles were an expanded learning cycle that was built on Kolb's (1984) original four-stage cycle. The styles were inferences of Fenwick (2001) that expanded Kolb's initial learning theory. The ELT Model required a holistic approach involving the ideas, thoughts, and opinions of police personnel in their natural setting. The learning styles and principles focused on the experiential learning theory (ELT) that demanded certain criteria. The training required goals with structured learning

and feedback with evaluation and understanding of the individual diversity during the learning process (Cross, 1976; Martin 2015). ELT began with concrete experiences followed by reflections on prior cybercrime experiences leading to the abstract concept. The reflections on the lived experiences of police personnel assisted in forming the learning foundation with a variety of styles. The focus was on prior preparedness encompassing the new knowledge and prior experiences.

The Experiential Learning Theory (ELT) consisted of knowledge, skills, and abilities procured through the cybercrime preparedness process. The data inquiries collected provided in-depth rich meanings to the learning process. Experiential learning and styles of learning engaged the mind and body through a well-spring of thinking, reflections, and engagement of inquisition actions (Craig, 2006). Whereas Kolb (1984) asserted that learning is a process; where knowledge is established, and a catalyst activated moves towards the evolutionary transformation of the experience. The experiential learning theory (ELT) of Kolb (1984) was built on principles and the blueprint that learning is a process. First, one must focus on the concrete experience and then act on the experience. Second, the person evokes reflective observations with constructive contemplations on the learned skills and knowing experiences. Third, one performs abstract conceptualizations that consist of learning from all prior experience. Fourth, then one evolves into active experimentation that analytically applies to what was previously learned. The Experiential Learning Theory (ELT) was a valuable comparative tool for police personnel in their cybercrime preparedness

and training. ELT enhanced the atmosphere for critical thinking, as well as problem-solving with recommendations (Wozencroft, Pate, & Griffiths, 2014).

The model for experiential learning employed retrospective reflections and analytical comprehension by law enforcement personnel during the learning process of cybercrime preparedness. The ELT was based on the experiences with the formulation of thoughts and ideas incorporating Kolb's (1984) four components of experiential learning. Bruner (1960) initially expressed that if an idea was basic or a part of fundamental learning, it should be introduced on an experiential level and developed after it is subjected to additional exposure, which facilitates an opulence of comprehension.

The concrete experience was initiated with police personnel exploring their perceptions and lived experiences concerning prior cybercrime preparedness. Reflective observation required law enforcement personnel to review, examine, and reflect upon concrete experiences to conceptualize or review various perspectives. Reflections allowed a genuine thought process of experiences that provided meanings to the cybercrime preparedness experience. The abstract conceptualization provided the law enforcement personnel to build upon their reflective experiences. They examined, inferred, and drew logical conclusions as an extension of the cybercrime preparedness experience. The final component entailed the active experimentation that catapulted the police personnel into making decisions and implementing how and in what ways the cybercrime preparedness was taught and actively applied. It required applying the concepts of creative problem-solving and integrating the decision-making solutions. The

process served as a catalyst and evolved into cybercrime preparedness experiences with accommodated applications (Dunlap, Dobrovolny, & Young, 2008; Martin, 2015).

Kolb (1984) asserted that experiential learning is a process, where knowledge is created through the transformation of experiences. It requires perceptions and cognitive behaviors. It was viewed with understanding and individuals created the learning environments. Participants interacted and linked ideas and experiential learning with life's learning activities, inside and outside of the workplace. It established diverse environments that enhanced and improved with applied critical thinking. Kolb's (2014) experiential learning incorporated the best use of the ELT process. The proactive thoughts and reflections of the police personnel established what worked during and after cybercrime preparedness. Kolb's (1984) experiential learning progresses in the process of understanding that knowledge is created through the transformation of experience. It requires a conglomeration of diverse experiences. It was retrospectively viewed with the understanding that created many learning environments and learning styles. The law enforcement personnel learned in the activities of everyday life established as a combination of diverse environments, which was enhanced and improved with critical thinking. ELT represented Kolb's (2014) learning process incorporating the best use of the four-segment process. The thoughts and reflections of police personnel efficiently worked to enhance the future of cybercrime preparedness by incorporating the theories of others. The study provided rich proactive recommendations to fight cybercrime, reduce cyber-attacks, and eradicate cyber terrorism.

Lewin's Model and Dewey's Model

Kolb's (1984) ELT was established on Lewin's Model (1939) that emphasized learning was a perceived four-stage cycle were the immediate concrete experience was the basis for reflection and observation. Observations emanated into two aspects that determined the model. The first was the personal experience of the participants; the second was for the efficient learning outcome of participants. Dewey's Model (1938) served as a foundation in an environment with interactions based on experiences including thinking, knowledge, and judgments for procedures that evolved into information, understanding, and insight given the new learning experiences. The judgment phase was related to discernment, which was perceived as the knowledge or developmental experience of meanings. They resulted in valuable pragmatic feedback and results (Kolb, 1984; Martin, 2015). It was analogous to Piaget's (1933) work where the classification or taxonomy of each stage was characterized by the unique developmental process affecting efficient learning. Kolb (1984) established the work and analogies that were a constant interaction between the environment and the individual. Essentially, we learn, grow, experience life, and develop until the day we exit this world. The prior police personnel preparedness worked to bring about social change with Kolb's (1984) experiential learning theory (ELT). It was utilized as a rich powerful tool to transfer practices in learning in diverse agencies. The ELT was referred to as scientific evidence. Kolb's (2014) ELT was applied with flexibility incorporated into a range of components. Learning is always a process using everyday experiences (Griggs, 2018). The study presented police personnel integrating the ELT into the empirical

qualitative study with views related to cybercrime preparedness. Kolb's (1984) Experiential Learning Theory (ELT) was correlated with Bloom's (1956) Taxonomy focused on the practical use of prior learning. It moved the police personnel beyond the superficial to gain an in-depth understanding and scientific analysis of cybercrime preparedness (Kolb, 1984; Forst, 2013). Reflections on prior training stimulated the intellectual creative process with prescribed actions. It evaluated activities and described approaches that occurred during the learning process of cybercrime preparedness and experiential learning. In the research study, police personnel were asked semi-structured inquiries concerning their prior cybercrime preparedness. The inquiries inferred: What was learned? What worked? What did not work? How was it presented? Who were the presenters? What could have enhanced the preparedness and cybercrime achievements? In what ways was the cybercrime experiential learning utilized? Where the preparedness might have been more effective? Were they taught on social media, the Internet, brick-and-mortar, or Self-taught? How a different approach might have worked more efficiently? What different techniques might have had better results?

Experiential Learning Theory and the Michigan State Police

In 2011 the Michigan State Police (MSP) with the assistance of the United States Department of Justice Smart Policing Initiative designed and established a change utilizing Kolb's (1984) Experiential Learning Theory (ELT). The targeted designated areas were neighborhoods in the Secure Cities Partnership (SCP) that were cities deployed with Michigan State Police Troopers. The Secure Cities Partnership was formed in March 2012 by Michigan's governor in response to the high level of crime in four

cities (Detroit, Flint, Pontiac, and Saginaw). The focus was to reduce crime through the coordination of law enforcement, prevention, community involvement, and prosecution. The State Administrative Agency (SAA) was financed by Byrne Justice Assistance Grant for the Michigan State Police (sworn officers, trained, and certified by MCOLES). They were augmented by associations and links occurring at local levels. It worked effectively embodying Kolb's (2014) experiential learning theory (ELT).

ELT and the Current Study

Kolb's (1984) ELT worked efficiently in the current study to fill the literature gap regarding police personnel and prior cybercrime preparedness in conjunction with experiential learning practices. It was built on the principles addressing the four ELT components of concrete experience, reflective observation, abstract conceptualization, and active experimentation. The focus was on the lived experiences, and perceptions of police personnel and cybercrime preparedness. The culmination of the research was fulfilled with recommendations and suggestions to mitigate and uproot cybercrime. It procured rich data and in-depth tactics from the participants capable of bringing productive social change. Howarth (2010) affirmed that a member of the Cambridge Parliament once stated that good research findings are like money in the bank.

Kolb's (2014) theory has moved proficiently in the United States and the United Kingdom. Since 1998 the law enforcement departments have utilized proactive cybercrime maneuvers to reduce cost and people-power (Dempsey, 2013). There are multiple collaborations that allowed the ELT to move forth in positive ways.

The constructive analysis was intertwined as an integrative cognitive learning domain. Strategically combining Kolb's ELT (1984) and Bloom's (1956) provided the cognitive learning taxonomy allowed with workable cognitive learning analogies.

Cognitive Learning Analogies

The correlation and pragmatic components intertwined the array of similar cognitive learning proximities in relation to the law enforcement personnel's cybercrime preparedness. Bloom's (1956) taxonomy was a forerunner of Kolb. Each level depended upon the completion and succession of the prior level. Kolb's (1984) ELT had close similarities with Bloom's (1956) taxonomy. It was a hierarchical pyramid structure that addressed the cognitive learning process and then extended into cake-like layers in the learning process. It required the movement from basic cognitive learning to the next higher level. Both were directly dependent on retrospective reflections focusing on prior cognitive learning and knowledge. It was essential that the basic knowledge and cognitive learning skills were comprehended and understood with listed achievements. The cybercrime preparedness environment demanded basic learning with commitment and coordinated collaboration to enhance the experiential learning theory.

Bloom's six levels of taxonomy moved from basic cognitive learning to the advanced level. Each level was built one upon another and was necessary to arrive at the cognitive learning of critical thinking. The original six hierarchical structures were built from theoretical to pragmatic achievements. Bloom (1956) and Kolb (1984) have many similar comparative analyses with quality interactive connections. The ELT learning

process expanded into knowledge with acquisitions derived from Bloom's (1956) cognitive taxonomy and the congruence of Kolb's (1984) ELT. The experiential learning theory (ELT) was predicated on the four components and correlated with Bloom's (1956) six levels: knowledge, comprehension, application, analysis, synthesis, and evaluations. Kolb's concrete experiences required police personnel to reflect upon cybercrime preparedness. Knowledge entailed reflective observations with contemplation, consideration, and comprehension. The abstract conceptualization encapsulated the represented realistic organization of investigation and analytical diversification. Kolb's (1984) final cognitive component consisted of active experimentation that engaged assessments, constructive criticism, and critical thinking. Both theorists provided in-depth real-world cognitive learning procedures. Kolb's experiential learning theory laid the groundwork that was analytically assessed in the process as an evolving synthesis.

The basic level was the police personnel's foundational cybercrime preparedness learning, which embodied the primary cognitive level. It focused on the reflection of remembering, recognizing, and recalling the information. Kolb's (1984) learning process and styles correlated the basic extended collaborative complexities with the specificities of Bloom's taxonomy. The law enforcement personnel's cybercrime preparedness yielded an overarching scientific undertaking in the analyses of Kolb's (1984) ELT and Bloom's (1956) taxonomy. Kolb's experiential learning theory considered the cybercrime preparedness activities aligned with the police personnel's learning styles integrated

as basic skills. The ELT enhanced Kolb's learning and comprehension encapsulated and integrated with the prior cybercrime preparedness. Figure 6 entitled *Law Enforcement Personnel's Cybercrime Preparedness* bridged a gap in experiential learning achievements.

Figure 6

Law Enforcement Personnel's Cybercrime Preparedness

Concrete Experience (CE) Doing and Having an Experience	**Introduce the cybercrime preparedness problem and relate it to an experience (The question is why?)**
Reflective Observation (RO) Reviewing and Reflecting on the Experience	**Present pertinent facts, theories, principles, and problem-solving methods to reflect upon (what?)**
Abstract Conceptualization (AC) Concluding and Learning from Experience	**Provide hands-on methods, practices, and how participants learned from preparedness (how?)**
Active Experimentation (AE) Planning and trying out what you have learned	**Allow encouraging exploration of the applications and consequences of learned material (what if?).**

Note. "From Experiential Learning: Experience as the Source of Learning," by D.A. Kolb, 1984. https://www.researchgate.net/.../235701029_Experiential_Learning, Copyright 1984. Reprinted by Permission.

I aligned a cybercrime preparedness paradigm figure charting the information from Kolb's (1984) basic experiential learning theory (ELT) to Kolb's (2014) ELT. It orchestrated the related experiences (answering the question why?); presented pertinent facts, theories, and principles to reflect upon (what?); provided hands-on procedures and practices (how?); allowed exploration of the practical applications and consequences

of the learned material (what if?). The ELT learning cycle was presented with a challenge of **why** it was necessary for police personnel to better understand prior cybercrime preparedness. It presented certain pertinent facts, theories, and principles of **what** other cybercrime preparedness components were needed. It aligned with hands-on cybercrime preparedness training and **how** it was presented. The results of the learned cybercrime preparedness were the application in the workplace and other places. **What if** consisted of recommendations and best experiential learning practices to enhance preparedness with significant strategies and techniques to efficiently work to mitigate and uproot cybercrime? The definition of experiential learning is essential to determine the best pragmatic learning asserted by Lewis and Williams (1994, p. 5):

> In its simplest form, experiential learning means learning from experience or learning by doing. Experiential education first immerses learners in an experience which encourages reflection about the experience to develop new skills, new attitudes, or new ways of thinking.

The study of police personnel and cybercrime preparedness was necessary to close the gap in collecting the much-needed data. Kolb's (2014) experiential learning theory (ELT) worked to provide significant data and assisted in providing principles to bridge the literary gap. The qualitative study described the lived experiences of police personnel and cybercrime preparedness utilizing the ELT for research. It worked to eradicate the trajectory of ever-increasing cybercrime. The research worked to identify the targeted group, collect essential data utilizing the data inquiry tool, and incorporate the principles

of Kolb's experiential learning practices. In addition, further recommendations were provided by police personnel to combat and eliminate cybercrime. The results were critically analyzed by van Kaam's Modified data analyses. It was supported by Wall (2011), who emphasized how the global extensive nature of the Internet continued to add to the complexities of cyber-attacks and cyber-terrorism. The study revealed in-depth results to assist in bringing about positive social change with transferability to other agencies and entities.

Summary

Chapter 1 presented the introduction, problem statement, nature, why the study was necessary, and the worth of the study. It addressed the evolving cybercrime issues, challenges, and law enforcement personnel preparedness. Kolb's (1984) experiential learning theory (ELT) provided the blueprint and framework. Chapter 2 provided the literature review concentrating on a better understanding in the duplicity of cybercrime threats and cyber-terrorism. It expounded upon the escalating cost that transcends national cyber-borders. A better understanding evolved while addressing the cybercrime environmental issues, challenges, and the literature gap. The chapter presented one somewhat similar police patrol officers' quantitative research study by Bossler and Holt (2013). The chapter provided an overview of the critical infrastructures, cyber-breeches, cyber leaks, and cyber security. It discussed the evolving complicity of cyber-attack factors and actions that articulated the need to combat, mitigate, and uproot cybercrime. It addressed the police personnel's prior preparedness for technology. It explicated Kolb's (1984) experiential learning theory (ELT) and Bloom's taxonomy. It expounded on the

work of others focusing on cybercrime, social media, and challenges facing critical infrastructures. Chapter 3 presents the research design and methodology with descriptions and details of the empirical qualitative phenomenological study. It addresses why the study was necessary, its theoretical design, and its essential principles. It focuses on the population, purposeful sampling, and recruitment of law enforcement personnel with prior cybercrime preparedness. It presents the research questions, data collection, and data analysis. It explains the underpinnings of Moustakas and the Modification of van Kaam's data analyses that clarify the explanation of phenomenology, intentionality, noema, and noesis. Additional information aligns with the empirical qualitative research assumptions, scope, and limitations. It elucidates the selected role of the researcher and other ethical considerations.

Chapter 4 focuses on the summary of the findings and results. The chapter evokes the great challenges, issues, and data collection process. It describes the sample and the data analyses. It articulates the categories, patterns, and identifying themes revealed from the inductive analysis design. It employs the narrative explaining the evidence of trustworthiness and experiences of findings. It provides clarity with a better wealth of understanding through analytical processing. The police personnel's data inquiries are transcribed from verbatim statements that reveal proactive strategies and techniques. It articulates recommendations to mitigate and uproot cybercrime, cyber-attacks, and cyber-terrorism. Chapter 5 provides a detailed summation of previous chapters with the conclusion and results of the research study. It presents the empirical phenomenological qualitative study and police personnel's cybercrime experiences. The discussion of the

findings and the limitations express the great need for future studies focusing on cybercrime preparedness and experiential learning. The results evoke rich workable information to better understand the experiences of the police personnel, cybercrime preparedness, and experiential learning. The research assisted in fulfilling a segment in the literary gap regarding police personnel and cybercrime preparedness. The significance of the procured data provides rich information concerning police personnel and cybercrime preparedness. It aligns the principles and strategies to build upon with a wealth of workable ways to combat, mitigate, and uproot cybercrime. All research components express and address the plethora of great knowledge and recommendations to bring about productive social change with transferability. The study provides a rich framework and foundation for future research.

Chapter 3: Research Methodology and Design

Introduction

This empirical phenomenological qualitative research is a naturalistic inquiry, in which the researcher (instrument of the study) collected the data with semi-structured inquiries from the law enforcement personnel in their natural settings. The design, methodology, and approach defined how the phenomenon was studied. The research was inductive with humanistic qualitative methods. This researcher understood the perceptions of the police personnel and encompassed a systematic logical study. The study captured the perspectives and descriptive data that employed rich theoretical underpinnings of Moustakas (1994). I based the work of Husserl (1970) and others with concepts and understandings on the insight and patterns developed from the data. The qualitative methodology entailed the basic areas of interest with the design and approach guiding the study (Dawidowicz, 2016). The research consisted of quality criteria gathered from the experiences of police personnel and prior cybercrime preparedness utilizing experiential learning. The objectives explored the police personnel's perceptions of prior cybercrime preparedness and training. They described the law enforcement personnel's learned views of cybercrime preparedness and examined the police participants' perceptions of their learning styles and achievements. The research study identified the law enforcement personnel's suggestions and recommendations focused on cybercrime preparedness and workable ways to mitigate cyber-attacks and eliminate cyber terrorism. The empirical qualitative study utilized a small purposeful sample to understand the lived experiences and perspectives of Michigan law enforcement personnel and the cybercrime

phenomenon.

Moustakas (1994) emphasized core concepts with conscious perceptions, acts, intentional experience, and inter-subjective validity that were the primary source of the never doubted knowledge. Whereas Husserl's (1965, p. 45) phenomenology afforded knowledge as a science that was logical in its affirmation that the only thing, we know for certain is that which appears before us in consciousness. The study captured direct quotations from the data inquiries, rather than the interpretations of experiences often formulated by that particular researcher (Moustakas, 1994). The captured data provided the researcher the opportunity to view the perceptions of cybercrime preparedness and training along with Kolb's (1984) experiential learning theory (ELT). The police personnel described preparedness experiences and ways to mitigate cybercrime. The gap in the literature was due to the lack of research addressing police personnel and cybercrime preparedness. The quantitative findings indicated the lived experiences that contributed rich insight focusing on the literary gap in cybercrime preparedness.

The phenomenological qualitative study obtained and examined perceptions of police personnel enhancing social change with transferability. Weiss (1994) asserted that qualitative inquiries enabled us to learn perceptions and reactions with tremendous value contributing to the knowledge and understanding of the phenomenon (p. 10). The lived experiences focused on the rich detailed phenomenon of prior cybercrime preparedness, training, and learning data from the semi-structured inquiries. The research method and design assisted in understanding the human factors involved in the learning experiences

(Dawidowicz, 2016). The data gathered was based on the principles and blueprint of Kolb's (1984) Experiential Learning Theory (ELT) and the theoretical underpinnings of Moustakas (1994). The study worked at understanding meanings in the experiences of the police personnel's preparedness. Dawidowicz (2016) cited the participants' perceptions can change and evolve as they reflect upon the inquiries of the phenomenon in question.

Kolb's (1984) theory provided the framework for the critical components of the empirical phenomenological study and aligned the challenges in observing, integrating, and understanding the theoretical underpinning of Moustakas (1994). The qualitative research methodology and design sketched the foundation and the systematic methodology for collecting and analyzing the data. I orchestrated a plan describing purposeful sampling, site selection, data collection, and analysis aligning the processes in how the study was conducted. It provided comprehensive descriptions for a structural analysis that portrayed the essence of experiences asserted by Moustakas (1994, p. 13).

The theoretical underpinnings of Moustakas were coordinated by Husserl (1931), Giorgi (2009), and similar theorists. The empirical qualitative research design was the most appropriate design for this study. The researcher was allowed to actively read, listen, and gather concise meanings of the participants' experiences (Patton, 2002; Quick & Hall, 2015). The framework of the phenomenology study emphasized the lived experiences of the police personnel and their prior cybercrime preparedness, views, learning styles, and experiences. The insider's views were emic, unique, and distinctive to the participants, whereas, etic was the outsider's views. Pike (1954) coined the

terms emic and etic. The study was aligned in accordance with the language and categories utilized by the people in that culture. The categories were created by this researcher in contrast to the cultural distinctions. The analytical outcome was dependent on the etic approach-standing outside the group. Patton (2002) expressed the need to capture the true perspective referred to as the emic or insider's view. The etic is aligned with a higher level of conceptual analysis and abstraction. However, the verbatim statements and quotations provide the emic perspective, expressed from the hearts of participants. The study yielded the foundation in the theoretical research framework of Moustakas (1994), Husserl (1931), and van Kaam (1966) with the personnel's experiences providing data and credence for additional research. According to Dawidowicz (2018, p. 203), a phenomenology design assists in understanding the human factors in the experience. Inquiries are answered with the phenomenon of the context serving to understand human perceptions. Further examinations express how transferable the responses are from the experiences of one participant to another.

The empirical research design orchestrated the police personnel preparedness and gathered the data analyzed by van Kaam's (1966) Modified data analyses. The study provided in-depth data serving to bridge the literary gap and bring about practices for positive social change. The research design analysis allowed dimensions to emerge from a variety of patterns evolving with insightful details. The components of Moustakas (1994) were implemented and research entailed experiences guided by the data, evidence, and sources. Moustakas (1994) expressed that human scientists worked to determine the underlying structure of each experience in interpreting the initial descriptors.

Epoche demands eliminating prejudgments to open the study with unbiased ubiquity where everyday judgments and suppositions are excluded. The semi-structured inquiries were of top priority. However, additional data were obtained utilizing emails and other electronic devices to gather clarifications and specificities. The research and design were all-encompassing exploring the shared experiences of the police personnel's perceptions and the phenomenon of cybercrime preparedness employing Kolb's (1984) experiential learning theory (ELT). The study focused on cybercrime preparedness and the personnel, which articulated an array of rich data skills and learning styles, as well as tactics to combat cybercrime.

Methodology of Research and Design

Empirical phenomenological qualitative research is a methodical systematic process that collects and analyzes the data; whereas research methodology is ways and approaches to data collection in an organized purposefully arranged manner. According to Patton (2002), the qualitative methods may be perceived as personal with humanistic values that undergird core principles. The study with the documented IRB confirmation was extensively researched. The study explained the cybercrime phenomenon with valuable data retrieved from the literature research and police personnel that expressed their beliefs and opinions on cybercrime preparedness and experiential learning. The methodology consisted of an evolutionary design of collected data.

Qualitative methods are often viewed as somewhat personal due to their inductive nature. On the contrary, quantitative research provides numerical and statistically

assembled results with a methodological approach and results. Quantitative research consists of a single objective reality measured by an instrument; established relationships between measured variables; procedures ordered before the study begins; experimental design to reduce error and bias; and detached use of the instrument of universal context-free generalizations (McMillan & Schumacher, 2006). Qualitative research embodies semi-structured design techniques that are discovered and analyzed in accordance with what the participants believe, think, know, and do. The study generates and contributes practical problem-solving to the real world with decision-making to improve training programs and answer concrete questions (McMillan & Schumacher, 2006; Patton, 2002). Qualitative research is not appropriate for all research; however, this type was most fitted for this study. The qualitative research was holistic and person-centered developing an understanding of the participants' ideas and perspectives. The population of interest was individuals that conformed to the specific criteria of police personnel. They were eighteen or older; current employees, contractual individuals, or volunteers for the agency; had cybercrime preparedness [via Instructor, Trainer, Google, Video, DVD, CD, ZOOM, YouTube, Internet, Experience, or Self-taught]; and had the opportunity to apply the cybercrime skills, knowledge, and abilities at the workplace or other locations.

McMillan & Schumacher (2006) asserted that the frame for the basis of a qualitative study was the type of experiences that happened or was still happening in the naturalistic settings. The frame utilized the description of what transpired and experiences of the prior cybercrime preparedness phenomenon. The researcher's role worked efficiently to collect the core of the phenomenon using semi-structured data inquiries.

Role of the Researcher

I, as the instrument of the study, developed and analyzed the perceptions from the data inquiries focusing on the phenomenon of cybercrime preparedness and the lived experiences of the police personnel. In-depth data was gathered from their perceptions and reflections. I adopted a stance of neutrality and did not attempt to prove any perspectives. The researcher does not attempt to steer inquiries or manipulate the data to skew or align predetermined results (Patton, 2002, p. 51). All data were collected via email or other electronic devices due to the COVID-19 pandemic with no face-to-face inquiries. Trustworthiness, integrity, and honesty were imperative and of the utmost concern. Neutrality was not an easy or attainable component; avoiding biases were incorporated in the process of bracketing that assisted during the data collection. Bracketing was important in the study to record any potential biases (Dawidowicz, 2018).

The research reported any potential sources of error and bias due to the human element of the researcher concerning the data collection. The study required careful detail, a systematic process, and an analytical assessment of the data to ensure credibility, trustworthiness, authenticity, fairness, and integrity (Patton, 2002). The researcher's inquiries demanded an array of elements. It entailed interest, passion, and rapport necessary during the interview inquiries (Jasper, 1994). Essential inquiry techniques exacted a positive demeanor of the researcher to ensure honest and non-judgmental understanding with flexibility. If the face-to-face inquiries had transpired, the researcher might have verbally evoked reiteration, which means to restate or rephrase the inquiries for clarity to collect the unclear statements. There were no verbal interactions with the

participants (except two) during the data collection. The researcher's primary objective was to obtain the data (Patton, 2002). The quintessential data inquiry feedback from the police personnel focused on cybercrime preparedness. Neutrality and credibility were mandatory for the data collection. I had to remain neutral and not attempt to coerce or skew the data. I emailed the open-ended data inquiries enabling the participants to engage in personal thoughts and self-reflections explaining their lived experiences. Moustakas (1994, p. 101) asserted that applying and minimizing biases were important.

> Understanding the nature, meanings, and essences of Epoche, Phenomenological Reduction, Imaginative Variation, and Synthesis is necessary in order to conduct phenomenological research. Through phenomenology a significant methodology is developed for investigating human experience and for deriving knowledge from a state of pure consciousness.

The researcher did not impose any leading inquiries during the informal electronic sessions. Throughout the empirical phenomenology study, I refrained from making any assumptions or preconceived ideas. Moustakas (1994) expressed that excellent data is obtained from the collected inquiries. The research data inquiries were developed and aligned to answer the three research questions. Often, in phenomenology qualitative research, the researcher does not develop the final inquiries until a significant number of data collection and analysis has been performed (Weiss, 1994). The proper words and terms were necessary to collect the data during the one-time informal open-ended inquiry, rather than contrived questions designed to steer or lead the police personnel.

The informed consent explained the purpose, inquiries, and approximate time. The police personnel had to acknowledge "I Accept" prior to the research. The researcher's role required certain principles and regulations. Table 1 illustrated the role of the researcher in conducting the data collection with the required applications.

Table 1

Role of the Researcher in Conducting Research Inquiries

Exploration Search –The researcher needs to explore, investigate, and examine while gathering the reality of the cybercrime phenomenon encouraging the participant to provide constructive data. Should be neutral to avoid bias and steering.
Open-ended Inquiries – Provide proficient time and opportunities for participants to express their ideas, thoughts, perceptions, opinions, and feelings as they respond in their own words.
Tracking – Maintain contact with sequential order. Display the dedicated interest, sensitivity, and openness following the semi-structured open-ended inquiry format and garner verbatim written comments and documented conversations.
Comprehension – Ensure participants clearly understand the questions. All inquiries are written in clear, concise, complete, and correct descriptive terms. If the data collection is face-to-face, repeat or reiterate the inquiry, words, or phrases expressed. All words must be comprehensive and understandable, if necessary explain with examples. Distribute informed consent forms, demographic sheets, and data collection inquiries with other handout material.

Note. From "The Evolving Process of Cybercrime." by L.Y. Martin, 2015, Unpublished Master Plan B Thesis, University of Detroit Mercy. Reprinted with Permission

My role consisted of depicting professionalism while obtaining feedback from open-ended inquiries. Proficient time and opportunities were necessary for participants to complete the data instruments. The police personnel with their cybercrime reflective thinking expressed their thoughts in sequential tracking. Tracking depicted an alignment of order and openness as they responded to the semi-structured inquiries. Clarification assured participants understood the inquiries and to contact me immediately if there were any difficulties. Moustakas (1994, p. 84) cited the importance of descriptive inquiries,

"descriptions that make possible an understanding of the meanings and essences of experience." All participants were police personnel meeting the required qualifications.

I collected the general data, such as gender, approximate age, education, length of employment, title, position, and type of cybercrime preparedness. This assisted in contextualizing answers as data were obtained for the analysis. Byrne (2009) emphasized that empirical qualitative research was focused to understand the phenomenon of addressing challenges and issues. The research study was analogous to the real-world lived experiences of the participants and their prior cybercrime preparedness phenomenon with training and pragmatic applications. The strength of the qualitative research study required collecting the data, confirming, and analytically assessing the emerging patterns and categories with an inductive approach. The personnel provided rich data resulting in constructive social change augmented with the experiential learning that embodied the systemic research design and transparency.

I thanked the participants and employed a debriefing session, which was essential to express appreciation for the collected data. The written comments prepared the narrative. I expressed my openness to the participants in how the inquiries flowed. The process of collecting the data was engaged in the epoche, aligning categories, and themes, and clarifying structural descriptions. The components were incorporated in the qualitative phenomenological research and theoretical underpinnings of Moustakas and others, including the challenges and experiences in the data collection. Experience played a vital role in understanding and grasping the newfound cybercrime preparedness and

training information. Moustakas (1994, p. 13) expressed the importance of what an experience means.

> The aim is to determine what an experience means for the persons who have had the experience and are able to provide a comprehensive description of it. From the individual descriptions general or universal meaning are derived, in other words the essences or structures of the experience.

The volunteer police personnel received no paid compensation for the study. The participants had the right to exit prior to completing the inquiries. If an emergency or difficulty arose and the participant could not complete the inquiry, data could be collected later by e-mail or another electronic device (if the participant was willing). The data inquiry included documented concerns, actions, and written responses submitted via emails and other electronic devices. The study allowed police personnel to express their perspectives and opinions with recommendations. My background, professional skills, education, and experience were shared with the police personnel to ensure credibility and that no biases were impacted by the researcher. The process of bracketing was essential in the research. I "bracketed" my own biases and experiences to allow the police personnel to express their comments and ideas with no influence from the researcher.

Background and Professional Skills of Researcher

I provided my police experience background, service as a college-university professor, and other training information. Integrity and trustworthiness were essential. Patton (2002) cited that qualitative inquiry entails that "the human being is the instrument of data collection, requiring careful reflection, dealing with, and reporting potential

sources of bias and error" (p. 51). The researcher must exemplify integrity, honesty, and neutrality. I remained objective, not subjective, and neutral eradicating any biases regarding the phenomenon. McMillan & Schumacher (2006) mentioned the basis of the researcher's knowledge of a population provides the best data information.

Purposeful Sampling Strategies and Recruitment

Purposeful sampling entails studying information-rich cases that yield in-depth understanding (Patton, 2002). Table 2 depicts and explains purposeful sampling.

Table 2

Purposeful Sampling

Samplings	Descriptions
Site Selection	Site selected where police events are expected to occur.
Comprehensive Sampling	Choose the entire police personnel group by qualifications.
Maximum Variation Sampling	Request law enforcement personnel to obtain differently perceptions regarding the cybercrime preparedness among the information-rich qualified volunteers.
Unique Case	Search for qualified cybercrime voluntary police personnel.
ELT Theory-Based	Invite volunteers with information-rich cybercrime credentials and experience to explain the learned process/Elaborate & recommend.
Sampling Strategies	Cybercrime Purpose, especially for the small-scale study.

Note. From "The evolving process of cybercrime." by L.Y. Martin, 2015, Unpublished Master Plan B Thesis, University of Detroit Mercy. Reprinted by Permission

The police personnel's cybercrime preparedness research incorporated purposeful sampling. Patton (2002, p. 230) argued regarding the weaknesses, strengths, and logic in purposeful sampling. I focused on the size and the selection of information-rich cases.

What would be considered a “bias” in statistical sampling, and therefore weakness; becomes the intended focus in qualitative sampling, and therefore strength. The logic and power of purposeful sampling lie in selecting information-rich cases for the study that is equipped with the phenomena of the theory-based in qualitative research.

Purposeful sampling was at times referred to as judgment sampling. The sampling included site selection, comprehensive, and maximum variation sampling with voluntary ELT-based police personnel cases (Martin, 2015). The police personnel volunteered for the qualitative research. The purposeful sampling was performed in the utility of cybercrime preparedness data obtained from the small sample. The researcher collected data from the information-rich participants who were knowledgeable in the designated field (McMillan & Schumacher, 2006; Forst & Dempsey, 2013). Purposeful sampling focused on the small number of cases that elucidated the research under study. It worked to address the purpose of the cybercrime research by aligning the purposeful sampling strategies and personnel selection. The logic and power of the sampling and recruitment worked in the selection of participants possessing the required qualifications. The volunteer samples were qualified personnel with prior cybercrime preparedness who described experiences providing rich in-depth perspectives regarding the phenomenon.

Purposeful Sampling

The population was the entire segment of Michigan police personnel; whereas the sampling was the subset selected for the research study. The sample size for the research focused on collecting data with the numbers between 8 and 12, and it was not meant

for generalizations (Dawidowicz, 2018). The logic of the purposeful sampling established a few participants studied in-depth to yield rich data and insight regarding the cybercrime preparedness topic. Purposeful sampling types included segments of the site selection, comprehensive sampling, maximum variation sampling, typical cases, unique cases, theory-based, and a combination of purposeful sampling strategies (McMillan & Schumacher, 2006). The qualitative study referred only to Michigan personnel with prior cybercrime preparedness and other qualifications. The study was a purposeful size and the "sampling" employed participants of interest; the goal was to obtain sufficient data appropriate for the study (Dawidowicz, 2018; Dempsey & Forst, 2013; Maxwell, 2013).

Purposeful sampling is sometimes referred to as purposive, judgmental, or judgmental sampling due to the researcher identifying elements from the representative population or possessing the information regarding the topic of interest (McMillan & Schumacher, 2001). The researcher selected the police personnel. The phenomenological studies with small samples often provide suggestive answers to the questions (Martin, 2015). The logic and power of purposeful sampling consisted of only a few participants studied in-depth to yield considerable insights regarding the topic. According to Patton (2002), the value of the phenomenological study is in transferability, which is the ability to apply the learning to similar situations. The personnel described their perceptions and lived experiences with experiential learning. They focused on how cybercrime preparedness was learned and applied in practical ways in the workplace with recommendations to mitigate cyber-attacks and uproot cyber terrorism.

McMillan & Schumacher (1997) expressed that probability sampling procedures, such as simple random or stratified samples were inappropriate due to generalizations. It was impossible to generalize, and this was not the purpose. Statistical sampling is precluded due to logistics and ethical reasons. The strength of purposeful sampling is not as costly and time-consuming. The four major weaknesses were: (1) greater opportunity for error due to researcher's bias; (2) results dependent on the sample's characteristics; (3) less representation of the identified population of interest; and (4) impossible ways to generalize to other police personnel (Martin, 2015). Purposeful sampling was selected to provide an "information-rich" manifestation of the personnel's prior cybercrime preparedness phenomenon and to combat, mitigate, and eliminate cybercrime. The study collected rich data with substantive descriptions regarding the phenomenon in question (Moustakas, 1994, p. 116). The sample size was appropriate and the data was collected by emails and other electronic devices from qualified personnel. Purposeful sampling was selected for the study's purpose and resources (Patton, 2002, p. 243).

The state of Michigan was the population. The police personnel sampling was gathered throughout the state from police agencies with cybercrime preparedness and experiential learning. However, the participant selections were changed due to the corona COVID-19 virus. The initially selected police personnel included a diversity of law enforcement personnel, such as college-university police, medical law enforcement, police civilians, police reserves, police assistants, and state, county, and city police personnel. The full selected gamete did not become a reality due to the COVID pandemic. There were different strategies for purposive sampling in the selection of

the information-rich cases. Guba and Lincoln (1989, p. 25) were accredited for the term and action of purposeful sampling.

The personnel were selected with volunteerism in accordance with their prior cybercrime preparedness, training, and ELT. All police participants were working or volunteering in the agencies. The recruited law enforcement personnel were required to be computer savvy with the required qualifications. Each had to be equipped and willing to share their experiences and perceptions regarding the prior cybercrime preparedness evoking rich in-depth data for the empirical qualitative phenomenological research.

Recruitment and Site Selection

Letters were mailed via US Postal Services and submitted to police administrators requesting Letters of Cooperation and personal emails to begin the study. Copies of the cooperation letters would then be submitted to Walden University's Institutional Review Board (IRB) to garner final approval to initiate the study, and then request volunteers to collect the research. The police personnel had to be willing to actively participate; understand the basic parameters of the study, and be comfortable expressing their ideas, feelings, and perceptions. Participants had to meet the basic criteria. They must be eighteen years or older, employee or contractual individual for the agency, currently working or active in the agency (employed, volunteer, or an active intern or resident), had prior cybercrime preparedness or training, and had the opportunity to utilize the cybercrime preparedness skills, knowledge, or abilities (SKA), and available for at least one open-ended inquiry. All law enforcement personnel understood they could exit at any

time, without any negative repercussions.

The initial inquiry site selections were physical police sites designated by the law enforcement administrator; however, this changed with the COVID-19 pandemic, and no face-to-face interactions were allowed. The collected data was gathered electronically, and no personal contacts were held at the brick-and-mortar sites between the researcher and police personnel due to COVID-19. All data was electronically transmitted. The chiefs and administrators received copies of all research documents (informed consent, data collection, demographic form, and debriefing paperwork) that would be distributed to personnel after the approval of the Walden Institutional Review Board (IRB).

Site Visits, Settings, and Participants

The site visits and settings for the empirical phenomenological qualitative study were changed due to the Corona Virus 19 pandemic with no face-to-face inquiries. Data collection required an extreme amount of time due to the COVID-19 pandemic as multiple law enforcement personnel tested positive requiring quarantine with many deaths of family members. The Corona Virus 19 pandemic sickness escalated as protest marches against police increased with allegations to defund police agencies. My letters submitted to the law enforcement agencies clearly indicated that the police departments and the participants would remain anonymous and not be identified in any way in the research study. I assured the utmost ethical confidentiality and integrity regarding the data collection (understanding that no research would begin until approval by the IRB). The final research resulted in rich empirical qualitative phenomenological information bringing about positive change with transferability to other facilities. The sample size

played an important factor in the research study.

Sample Size

The sample size was represented by the letter "N" determined by the researcher. Dawidowicz (2018) asserted that the goal should be sufficient to gather the appropriate data for the study. The sample size provided pertinent responses to the opened-ended semi-structured data inquiries from the police personnel's lived experiences. Patton (2002, pp. 242-244) argued there are no rules for sample size in a qualitative study; the size depends upon what the researcher is searching for and wants to know.

- What is the purpose of the inquiry?
- What is at stake?
- What would be useful?
- What would have credibility?
- What can be performed and achieved with time and resources?

The sample size was orchestrated to fit the research study's purpose. Dawidowicz (2018, p. 207) argued that "Most often, participant numbers are between 5 and 15." The empirical phenomenology research sample size was determined by the principle of saturation. The term saturation is equated to the point that collected data themes are repeated and where no new information from the participants surfaced (McMillan & Schumacher, 2006). There were no mandated specified numbers for the data collection of the police personnel. The unit of analysis was the law enforcement personnel who were the primary focus of the study. Understanding the challenges of a small qualitative sample was judged in the context and principles that undergirded the analysis of the

qualitative data (Patton, 2002). The size was dependent upon the quality of the analysis, dignity, and time to analyze the data inquiries, in opposition to the number of participants. Building a convincing analytical narrative was based on richness, complexity, and detail; preferably than on statistical logic (Baker & Edwards, 2008). The number of participants for a qualitative study varies depending upon the need.

Baker and Edwards (2008) affirmed that one should strive for a sample of 12; whereas Brannen (1982) cited that there was no rule of thumb in identifying how many participants were enough. A very small sample can result in a study with rich, in-depth significance, depending on the research inquiries; how the study was conducted; and how the data was analyzed. Giorgi (2009) recommended at least eight participants are necessary for a qualitative study. The approximate number of participants must perform saturation, as sufficient data is gathered from the inquiries.

The police personnel provided dense and rich descriptive data. Every expression relevant to the experience was written verbatim. The first step required clear documentation referred to as “horizonalization” (van Kaam, 1966). The complete transaction and transcript were acquired from each police personnel. The second step was reduction and elimination which required testing each expression for two components referred to as invariant constituents. It was a moment of analytically assessing the experience and responding to the question-is it capable of being conceptualized? The results evoked tremendous data that resulted in a high-quality rich study. The three research questions were the foundation for the empirical qualitative study.

Research Questions and Inquiries

The three research questions established the basic query for the research. It was constructively investigated and procured the rationale, purpose, and need for the study. The open-ended research questions were analytically broken down into 10 semi-structured inquiries collecting the data from the law enforcement personnel. The informal inquiries garnered the police personnel's thoughts, lived experiences, and ideas. I concentrated on prior cybercrime preparedness and experiential learning; the effectiveness of cybercrime preparedness; police personnel's learning styles; and cybercrime applications in the workplace and community with workable preventive cyber-attack recommendations. The data evolved exponentially. The study was a rudiment of increased understanding with rich recommendations to combat, mitigate, and uproot cybercrime and cyber-terrorism. The three research questions were answered by employing the 10 data inquiry instrument presented to the police personnel. Reflective perceptions and opinions were articulated relating to the prior cybercrime preparedness, training, and pragmatic applications. The three basic research questions are listed.

Q1. What are the law enforcement personnel's perceptions, lived experiences, thoughts, and ideas regarding the prior cybercrime preparedness, training, and learning, and in what ways was it meaningful, relevant, and interesting?

Q2. Where did the law enforcement personnel acquire the prior cybercrime preparedness, training, and experiential learning and how was the cybercrime preparedness training applied in a practical manner in the workplace and communities?

Q3. In what ways have cybercrime professionals applied the preparedness and list workable recommended strategies and techniques to combat (fight), mitigate (reduce), and uproot (eliminate) cybercrime, cyber-attacks, and cyber terrorism?

The three research questions and semi-structured inquiries were developed after much thought, critical thinking, and an exhaustive review of the literature. I established the concerted efforts needed to fill the literary gap. The research conducted the human science inquiry to discover and explore, which resulted in the inductive analysis. The inquiries were developed after aligning the three research questions to procure the data.

Initially, I constructed one research question. After much examination and suggestions from my committee with reconsiderations, three research questions were developed. The rich data inquiries were systematically aligned to obtain the in-depth meanings of the police personnel's prior cybercrime preparedness. The study aligned each of the 10 data inquiries to build one upon the other. I assured them there were no biases in the data collection. The concentration was focused on collecting procedures and techniques in prior cybercrime preparedness. The research results provided detailed data from the police personnel's cybercrime preparedness contributing much insight that assisted in closing the literary gap. It further provided and sustained rich detailed comprehensive information with recommendations to mitigate cyber-attacks.

The basic core of the human science questions remained interesting, powerful, and alive throughout the study; seeking to reveal the essence and meanings to uncover the qualitative rather than a quantitative study. The empirical qualitative phenomenology

research aligned the scientific meanings established in the principles of the police personnel and their meanings in cybercrime preparedness. The study engaged open-ended semi-structured inquiries for participants to express their thoughts and beliefs with conscious perceptions of their cybercrime preparedness. The participants recommended workable ways to combat cybercrime, mitigate cyber-attacks, and uproot cyber terrorism. The inquiries captured the structure and the meanings of the police personnel's experiences as they elaborated on prior cybercrime preparedness and learning styles. Patton (2002) affirmed the quality of an empirical qualitative phenomenology directly depends on the methodological skills, integrity, and sensitivity of the researcher.

No manipulations or coercions were utilized to shape or influence the police personnel at any time during the inquiries. A tremendous amount of data was gathered through the inquiries with a bridge in understanding the participants. The open-ended inquiries collected the verbatim statements of the police personnel from the documented responses written in relation to the cybercrime phenomena. The informal systematic inquiries consisted of quasi-structured questions that allowed thoughtful ideas and remarks. The inquiries procreated a wealth of valued data-producing knowledge to fill the gap in the empirical literature. The continuity of insight and constructive thinking procured much cybercrime preparedness knowledge explaining ways to enhance preparedness training. The immediate interaction research feedback for additional clarity was obtained from only two of the eight police personnel. The inquiries evoked in-depth data contributing to the interpretation of the cybercrime phenomenon. The expansive data collected responses and intellectual cybercrime intelligence from the police personnel.

Rich feedback with great meanings was provided by the participants (Martin, 2015).

Data Collection and Analysis

The methodological procedures and process for data collection were based on the phenomenology of Moustakas (1994). It was imperative that the inquiries were clear, concise, complete, and understandable. Table 3 illustrates the initial step-by-step data collection inquiry preparation and procedural process I utilized for the research study.

Table 3

*Data Collection Inquiry Preparation (*Martin, 2021)

(1) Request is mailed to the police chief or administrator requesting a personal email address and "Letter of Cooperation" from the law enforcement agency to initiate research. Responses will be emailed, telephoned, or submitted by other electronic devices to Researcher. Additional information is submitted if an agency is interested. The added details could lead to an Approval Letter from the chief. That will be immediately sent to the IRB for approval. Research can only begin after the IRB's approval

(2) Provide any clarity needed regarding research and data inquiry details. Chiefs (Administrators) receive Informed Consent, Demographic Form, and Data Collection Inquiries encompassing 10 data inquiries assuring anonymity and confidentiality. Overview and introduction are provided with the researcher's professional background. Any unclear details are submitted regarding the empirical qualitative research. Articulate any need for clarity and integrity in answering the semi-structured open-ended inquiries.

(3) Distribute the Informed Consent Form to police personnel after receiving the IRB approval. Receive the list of qualified police personnel from the Chief or identified designee. Request volunteers to participate in the cybercrime preparedness study. If personnel decide to participate and meets all essential criteria, an email is submitted to the researcher's email stating "I Consent"

(4) Provide an overview of the material and administer the same process to each law enforcement personnel. Electronic digital divide messages are generated via emails and other electronic devices. Submit the data inquiry instrument with clear explanations of all material (Informed Consent Form, Demographics Form, and Data Collection Inquiries encompassing the 10 data inquiries)

(5) Specific Refreshed Clarifications-Utilize the same method for each participant. Allow police personnel to take ample time to write all ideas, thoughts perceptions, perspectives, reflections, and comments on the open-ended semi-structured data inquiry instrument. Emphasize the need to totally complete the cybercrime preparedness indicating the workplace and community practical applications. Identify proactive and preventive recommendations to combat cybercrime, reduce cyber-attacks, and eliminate cyber terrorism

(6) Researcher responds immediately to any needed request or clarifications. Participants submit all documents. A Personal Thanks and Appreciation is given to each Chief and police personnel for their volunteerism and input in the research with a Debriefing Form

(7) Obtain, collect, record, and analyze all statements with the recommendations. Ensure all research is placed in a secure safe

---

There were seven initial data collection inquiry steps; understanding that the open-ended inquiries did not presuppose what dimension, experience, or feelings were

salient. The police personnel's inquiries were received electronically with open-ended inquiries procuring the data collection and the cybercrime preparedness. The way an inquiry was worded affected how the participant responded and was considered an art and a science. The data collection inquiries' wording makes a significant difference.

To begin the research, I mailed the United States Postal Service (USPS) letters to police administrators requesting letters of cooperation, personal email addresses, and telephone numbers. I submitted the research details to the chiefs, providing attachments with the utmost assurance of confidentiality and anonymity. The research would begin when I received the cooperation letters and the IRB approvals. I requested volunteers to then send the Informed Consent Forms. The demographic forms and data inquiries would be submitted later. The volunteers must agree to participate in the research by emailing "I Consent." I would then immediately address any unclear or vague areas. The police personnel would have quality time to intellectually reflect upon their responses to the data inquiries and request any additional clarifications. I, as the researcher, would collect, record, and analyze all statements utilizing the seven steps of van Kaam's (1966) Modified data analyses. I would cite verbatim statements for clear examples. The data collection would be further examined with the theoretical underpinnings of Moustakas (1994). The study assisted in closing the literary gap and to better-equipping cybercrime preparedness with strategic tactics to mitigate cyber-attacks and cyber-terrorism.

The data collection provided the phenomenon of the police personnel and their cybercrime preparedness with in-depth critical thinking. It worked to express the lived experiences of law enforcement personnel with in-depth consciousness of data.

The data described and determined the underlying behaviors and experiences in the prior cybercrime preparedness. The empirical qualitative study investigated and explained the cybercrime phenomenon, which yielded valuable data from police personnel. The participants expressed their personal ideas and perceptions regarding the phenomenon resulting in rich research information (Dempsey & Forst, 2013; Moustakas, 1994).

Features and Characteristics of the Data Inquiries

The collected data evoked the perceptions of the personnel, their experiences, and the conscious structure of the prior cybercrime preparedness. Consciousness is more than a feature; it is a way of being that occurs with the experience (Zahiva, 2003). The raw data inquiries were written and returned by email and other electronic devices with many verbatim statements and quotations expressed by the participants. Nothing substitutes for the actual written words of the data inquiries feedback (Martin, 2015). This was a plus for the qualitative research. The number of quotations demanded that I incorporate the interpretations to ensure coding, categories, patterns, and segments with the analysis integrated into the written experiences. The comments and details were in-depth, critical, and unique.

The qualitative research inquiries consisted of five basic phenomenological features and characteristics (Martin, 2015; Patton, 2002). They are listed accordingly.

- Seeks to reveal the meanings of the participants' lived experiences aligned with the experiential learning theory (ELT)

- Reveals qualitative, rather than quantitative factors in the police personnel's lived experiences regarding cybercrime preparedness
- Engages participants' self-ideas and maintains involvement (personal-passionate) in the experiential learning and the recommendations to mitigate cyber-attacks
- Does not seek to determine or predict any causal relationships
- Intense and accurate with comprehensive descriptions in the life's experiences of the police personnel's comments, rather than ratings, measuring or scoring

The data when examined and analyzed provided the originally lived experiences of the police personnel, which evoked comprehensive descriptions regarding the prior preparedness for the cybercrime phenomenon. Moustakas (1994, p. 33) argued that things performed through the intuition and self-reflection of the participants include "whatever presents itself, whatever is actually given" in combination with "the presence to (the) consciousness of the essence." The study encompassed open-ended informal semi-structured data inquiries. The inquiries were stated in concise and concrete terms that were defined and discussed for the intended purpose of collecting the cybercrime data. In accordance with Moustakas (1994) and others, the expressed features of the inquiries sought to reveal the essence and meanings of the participants' lived experiences. It uncovered the qualitative, rather than quantitative and engaged the personnel in explaining the experiences in cybercrime learning, as well as the learning process and styles. The study did not seek to determine or predict any causal relationships and was illuminated through accurate experiences, comprehensive coding, and narrative descriptions.

Designing and Structuring Phenomenological Inquiries

The position of each word in the inquiry was important. In accordance with McMillan & Schumacher (1997) and Patton (2002), one must determine the priority in pursuing the topic and the data collected. The placement of words was essential when writing the data inquiries. The inquiries emanated from the police personnel's research preparedness and training questions and assisted in collecting tactics to mitigate cyber-attacks. I focused on understanding the experiences and perceptions of the participants and their viable preparedness with workable recommendations. The qualitative research did not result in generalizations. The study served emanating valued rich transferability. Opportunities procreated abilities to apply the research learning to other situations and circumstances. It enhanced experiential learning with problem-solving preparedness.

The theoretical underpinnings of Moustakas (1994) provided an in-depth understanding and insight into the themes and meanings of the lived experiences of police personnel and cybercrime preparedness. The study resulted in providing worth and significance with rich data as the personnel articulated their experiences. The design and structure of the phenomenological inquiries worked to probe and understand the truth of things through intuitive learning and personal thinking. The direct perceptions resulted in intellectual meanings through awareness, reflections, and acute philosophical phenomenology (Moustakas, 1994; Patton, 2002; Martin 2015). The informal data inquiries were not exact and did not ensure total accountability. However, the illuminated discernment brought great meanings regarding the aim and determination of what

cybercrime preparedness entailed and what the individual cyber-attack perceptions meant to the law enforcement personnel.

The participants articulated reality with comprehensive descriptions in the reflective structural analysis of their experiences. Moustakas (1994, p. 41) asserted.

> My natural bent was to avoid people who tried to instruct me with their facts and knowings, and to approach things for the first time alone. I have always wanted to encounter life freshly, to allow myself to be immersed in situations in such a way that I could see, really see and know from my own visions and from the images and voices within. When I have been alone I have been free to view openly whatever is before me. I have been able to discern for myself what I am encountering, to explore, to think, to learn, and to know.

Perceptions can be quite diverse depending on personal perspectives. The personnel's insight, intuitive learning, and suggestions were collected. Moustakas (1994) asserted in-depth introspectively is obtained during the opportunities of solitude and isolation.

Moustakas (1994) affirmed that what appears in the consciousness is an absolute reality; what appears in the world is a product of learning. The consciousness may be illuminated or elucidated by key figures addressing the consciousness, which was analogous to Moustakas and others. The deep conscious reflections were the development of the phenomenological perspectives, analysis, and its contributions (Moustakas, 1994). The theoretical underpinnings of Moustakas (1994) established and aligned the entire phenomenology approach. The study incorporated the method of reflection and provided

systematic logic and the science of personal reasoning. Coherent resources were carried out utilizing the Modifications of van Kaam's (1966) data analyses.

Modification of van Kaam's Data Analyses

The data analyses of van Kaam (1966) listed every expression, the reduced, and eliminated the determined invariant constituents. They were clustered, placed into themes, and finalized with identification by applications and validity. The emergent relevant themes with verbatim examples were utilized to construct structural descriptions in the systematic passages and imaginative variations (Martin, 2015). Each structure included textual-structural meanings with the essence of the lived experiences. The data analyses evidenced rich information from the cybercrime phenomenon in question. The phenomenological results produced transferable information to assist others with similar backgrounds or in quasi-comparable circumstances to advance positive social change.

The Modified van Kaam's (1966) method of data analyses girded the complete transcript of each law enforcement personnel. Accordingly, the general meanings articulated understandings of the philosophical viewpoints, valuable data, and verbatim statements (Martin, 2015). The study supplied rich data to better equip cybercrime preparedness, as well as mitigate cyber-attacks and uproot cyber-terrorism. The results can be utilized in transferability to other entities. Moustakas (1994) supported the Modification of van Kaam's (1966) method of data analyses with the steps that examined, categorized, and evaluated the participants' transcribed feedback.

The qualitative phenomenological narrative included all transcripts of each police

personnel. The study included seven components (Moustakas, 1994, pp. 120-121). (1) Every expression that was relevant to the experience was horizonalization. (2) The invariant constituents were determined through reduction and elimination and each expression was tested for two requirements. (3) It clustered and positioned the invariant constituents of the related experiences into themes. (4) It checked and finalized the identification of the invariant constituents and themes by the application referred to as validation. (5) The relevant validated invariant constituents and themes were established to construct an Individual Textual Description of the experiences, including all verbatim assertions. (6) The constructed Individual Structural Descriptions of the experiences were aligned for each participant. (7) A Textual-Structural Description of the meanings of the phenomenon ensured the inclusion of invariant constituents and themes.

The meanings and essences of the phenomenon of preparedness were derived from the composite description of the developed experiences. It represented the group as a synergistic whole. The research methods, sample size, data collection, and analysis were systematically processed utilizing the theoretical underpinnings and framework of Moustakas (1994), the concepts of Husserl (1931), and the principles of Giorgi (1997). The police personnel described and interpreted the essence of their experiences. Van Manen (1990, p. 10) affirmed that “the essence or nature of an experience has been adequately described in language if the description reawakens or shows us the lived quality and significance of the experience in a fuller and deeper manner.”

The object appeared in the law enforcement personnel’s consciousness blended

and mixed with the object in nature and meanings were created. The participants expressed their thoughts, feelings, and experiences of the prior cybercrime preparedness phenomenon. Data were systematically compiled into codes, categories, patterns, themes, and segments to obtain well-supplied meanings. The understanding procreated the experiences through extended knowledge, blended learning, and synergistic mingling (Moustakas, 1994). The synergistic mingling was the relationship of the perceptions and preparedness that existed between what occurred in conscious awareness and what exists in the world. Intentionality, Noema, and Noesis must be understood to determine the meanings, concepts, and judgment of the opinions and arrive at the results.

Intentionality, Noema, and Noesis

Intentionality, Noema, and Noesis are of the essence when attempting to procure the meanings of the perceptions and judgment of the police personnel regarding cybercrime preparedness with experiential learning. Moustakas postulated three questions regarding perceptual experiences, meaning, and reflections (1994, p. 68).

- Does language precede meaning or does meaning precede language?
- Does a perceptual experience determine the meaning or is meaning the outcome of the concepts and judgments?
- Is meaning embedded in the experience itself or is it an outgrowth of the reflection and afterthought?

Answering the three questions provided the foundation to analyze the perceptions. It provided thinking, reflecting, perceiving, and understanding of something, whether it

was real or not (Martin, 2015). It was guided by the consciousness that worked in the reality of the study (Moustakas, 1994). The police personnel expounded upon the prior cybercrime preparedness, training, and experiential learning that assisted in the phenomenology of the data collection and van Kaam's (1966) data analyses.

The consciousness was directed by Intentionality and the Noema directed the consciousness towards a particular object. The Noema then ascribed a meaning to what one observed, thought, heard, felt, or touched (Moustakas, 1994). The five senses played a critical role in the personnel's reflections on cybercrime preparedness, as well as the techniques to mitigate cyber-attacks and eliminate cyber-terrorism. Husserl (1931, p. 249) initially introduced the concepts of noeses and noema; whereas noeses constituted the spirit and the mind and stimulated the thinking, memory, feelings, perception, and judgment. Noesis or the noetic side referred to the sensory side or the physical aspect. Intentionality is the experiences encompassing a component and has an ideal side or a noetic side. Intentionality, noema, and noesis were essential to obtain the true experiences and perceptions of the police personnel cybercrime preparedness phenomenon.

It was a possibility to reflect upon the external and not utilize the intuitive to reflect inwardly. The noesis was external; whereas the noema was inward and allowed police personnel to reflect internally. The noesis and the noema were mutually correlated. The noesis was that part of the act that provided a character or special sense in the perceptions or judgments that something was transpiring in the consciousness. Considering, noema was a complex ideal structure that established the meanings of the

acts. Moustakas (1994) asserted that the noema directed a person to experience an intuitive explanation of the phenomenon in a pre-reflective manner (p. 73). Initially, the police personnel might have first reflected on the noesis. However, with stimulating questions during the data inquiries, there were perhaps other fresh awakenings with advanced perceptions inculcated with the noema, which assisted in the responses. Dawidowicz (2018) affirmed that phenomenology considers how and why people do what they do and how they experience their feelings regarding the phenomenon.

The interweaving and intertwining of the noesis and noema allowed a higher level of critical thinking and perception that embraced the whole as a synergistic entity and subjective phenomenon. The study's rich results were a product of the data that aligned cybercrime preparedness and experiential learning. The data produced inductive expressions and significance in the meanings, which were referred to as noesis and noema (Moustakas, 1994). It was oriented as an extension of the lived experiences of the police personnel. Understanding epoche was essential. A workable summary of the phenomenological model was delineated in understanding epoche, phenomenological reduction, imaginative variation, and the synthesis of meanings (Martin, 2015). Epoche provided a unique and original point in clearing the mind, embracing life's situations, and with time transparency that allows the understanding of data without judging.

Epoche, Reduction, Imaginative Variation, and Meanings Synthesis

It was important to understand the meaning, nature, and essence of Epoche, Phenomenological Reduction, Imaginative Variation, and Synthesis of the Meanings and

Essences were critical to conducting the phenomenological qualitative study (Moustakas, 1994). Understanding the essence of epoche and the most intuitive thinking was derived from the authoritarian Moustakas (1994) and not received from books or others. Critical thinking and understanding catapulted and served as a catalyst from the preparedness of listening and insightful intuitions (Martin, 2015). It entertained intimate relationships, which entailed confronting things with self-dialogues.

The need was great to fulfill the research literary gap in the phenomenon of cybercrime preparedness and law enforcement personnel. It was essential to understand the perspectives of training and learning as described in the cybercrime preparedness, which derived from the research results augmented with transferability. The theoretical concept was based on human science guided by epoche, phenomenological reduction, imaginative variation, and synthesis of meanings. The basic essence involved the natural processes of awareness and understanding (Moustakas, 1994). A phenomenon has many parameters depending upon what views are perceived, investigated, and evaluated.

Phenomenology

What is Phenomenology? Dawidowicz (2018) asserted that phenomenology is the collection, analysis, and perception of individuals and their lived experiences related to a definable and specific phenomenon. Phenomenology has its roots in philosophy and is interested in human experiences to provide an in-depth understanding. It is the first method of knowledge because it begins with “things themselves” and is the final court of appeals (Moustakas, 1994, p. 41). The cybercrime phenomenological philosophy

incorporated the study of general principles with underlying ideas and actions. The qualitative research presented the unparalleled prospect into the experiences of the cybercrime phenomenon, which was scientifically described by the police personnel. Moustakas (1994, p. 47) argued concerning qualitative phenomenology.

> The method of reflection that occurs throughout the phenomenological approach provides a logical, systematic, and coherent resource for carrying out the analysis and synthesis needed to arrive at essential descriptions of experience.

The phenomenological theoretical underpinnings of Moustakas (1994) established the designed methodological approach adopted for the study that required the Modified data analyses of van Kaam (1966). The design worked to analytically understand the experiences of the police personnel's preparedness in describing the prior cybercrime phenomenon. Streubert & Carpenter (1999, p. 48) affirmed that "phenomenology is a rigorous, critical, systematic investigation of phenomena." Generalizations were not the results; however, they supported the transferability that is applied to other situations and circumstances. Husserl (1931) asserted that phenomenology involved the examination of consciousness or the way one experiences the world. The phenomenological approach focused on prior preparedness, training, and learning experienced by the police personnel.

Phenomenological Approach

The phenomenological approach is a rich understanding of the phenomenon of prior cybercrime preparedness that collected the perceptions of police personnel, their prior training, and the experiential learning theory (ELT). Van Manen (1990, pp. 9-10)

argued that “a person cannot reflect on the experience while living through the experience; it is a reflection on experience that is already passed or lived through.” The police personnel’s experiences reflected on their thoughts and conscious perceptions of cybercrime preparedness. The phenomenological focused on obtaining a deeper understanding of the meanings and nature of the experiences. The research study and the police personnel’s experiences were important due to the daily increase of cybercrime and cyber-attacks on many critical infrastructures. Police personnel is challenged with the uptick of illegal technological complexities of cyber-attacks and cyber-terrorism.

It was imperative to understand the advantages and disadvantages of the empirical phenomenology of police personnel cybercrime research. It assisted in understanding human science research and human experiences that expanded innovative knowledge and assisted in closing the literary gap. The phenomenological qualitative approach determined the underlying structure by interpreting the personnel’s lived experiences that worked to disclose and elucidate the cybercrime preparedness phenomenon (Dempsey & Forst, 2013: Martin, 2015; Moustakas, 1994; van Kaam, 1966).

Steps and Strategies of Phenomenology

There were special and unique strategies in the phenomenology. In accordance with Streubert & Carpenter (1999), descriptive phenomenology entails four strategies, which are intuiting, bracketing, analyzing, and describing. Whereas Moustakas (1994) cited four steps: epoche, phenomenological reduction, variation, and synthesis. The strategies of Streubert & Carpenter asserted three coordinated comparative correlations.

- Intuiting is the thinking process of the data for comprehension or interpretation.
- Bracketing requires neutrality in analyzing identified phenomena based on data.
- Communicating requires efficiently aligning and describing the critical elements.

The three components allow opportunities to identify the interrelations as a comparative analysis in the phenomenology process.

The four steps of Moustakas (1994) addressed the phenomenological process as a comparative analogy to the four strategies of Streubert & Carpenter (1999). The first step was epoche which eradicated biases and stopped the researcher's personal everyday bias, knowledge, and understanding. The second step was a phenomenological reduction that was self-awareness, self-knowledge, and the ways of listening. The third step was an imaginative variation that was the utilization of the imagination aimed to collect the essence of the structural lived experiences. The fourth step was the synthesis of meanings and essences that were unified as structured descriptions. The four steps were necessary to conduct the study. The comparative analogy aligned similarities and dissimilarities in the four steps compared to the three strategies of phenomenology. Streubert & Carpenter (1999) asserted that phenomenology probes through the data and searches for common themes; and then establishes patterns shared by the phenomenon.

The attempt to define a philosophical method was different from natural sciences. Husserl (1931) established phenomenology as a process providing insight into the conscious objects and focused to gain truth as it manifested itself in the consciousness. Husserl (1931) was a determined self-presence pioneer with a dynasty of science and the

philosophy was developed as a system rooted in subjective openness, a radical approach that remains strong with outstanding contributions. The theoretical underpinnings of Moustakas (1994) supported van Kaam's (1966) Modification data analyses. The investigated experiences of the police personnel's reflections and thoughts focused on cybercrime preparedness and ELT. The interactive metaphorical process created analytical insight. Moustakas (1994) expressed the underpinnings to know the truth of things through discernment, distinct meanings, and philosophical phenomenology.

Underpinnings of Moustakas

The underpinnings affirmed by Moustakas (1994) were established upon the philosophical phenomenologist of Husserl who was considered the founder of modern phenomenology. Husserl (1931, p. 43) cited that knowledge was produced by setting aside all previous thoughts, seeing through, and breaking down mental barriers that are habits set along the horizons in thinking. The comments reinforced how thoughts appeared in the consciousness and meanings that were extensions of experiences. Husserl desired to develop a schema describing and classifying subjective experiences where the implied structure and meanings of human experiences were clearly explained.

Empirical phenomenology was the first method of knowledge for it began with things themselves. Moustakas (1994, p. 41) articulated that as far as one "could remember it worked to seek and know the truth of things." The truth is derived from one's own intuition and perception; learning from one's own direct experiences, and from the awareness and reflections that bring true meanings to light. At times, phenomenology

was alluded to as a movement. It was due to the constant energetic philosophy comprised of related descriptions that were intertwined (Moustakas, 1994).

Moustakas and the Reflection Process

The utilization of the phenomenological approach provided the systematic, logical, and coherent resources aligning data collection and the synthesis essential to arrive at the essence of the phenomenological experiences (Husserl, 1931; Moustakas, 1994). The reflection process has diverse meanings. Reflections consist of pondering retrospective components and presuppositions that underlie basic thoughts and ideas. Following the reflection process, police personnel constructed full comprehensive perceptions of their beliefs, opinions, and situations that portrayed their prior cybercrime preparedness. It was evidenced as experience. Moustakas (1994, p. 47) affirmed that

> Evidence is viewed as something that shows itself—something that is there before one. The very act of seeing, just what is there, just as it is, points to further seeing, again and yet again, and the possibility of confirmation.

The significance and importance of this study were structurally designed as a qualitative study to garner the initial construct of knowledge through the experiences of police personnel and cybercrime preparedness. Moustakas (1994) asserted that any phenomenon represented a starting point for reflections. The appearance was something that created a phenomenon with the challenge to explain the meanings and their constituents. The phenomenological perspective is derived from whether a thing exists or not. The

cybercrime phenomenon represented a starting point for reflections collected from the personnel's thoughts, skills, and understanding. Reflections played critical roles in thinking about experiences of cybercrime preparedness and experiential learning. The final analysis worked with transferability, as the personnel shared proactive ways to enhance preparedness and recommendations to mitigate and eradicate cyber-attacks.

Evidence from the phenomenological study emanated wisdom from the police personnel arranging interpretations that were referenced by Husserl (1931) as the epoche. The word epoche is a Greek word that means to refrain from judgment and bias. The personnel's cybercrime preparedness evoked rich data and new insight that developed from the transcribed responses. Emergent themes and categories embarked on the complex cybercrime phenomenon. Moustakas' (1994) underpinnings worked to eliminate things that represented presuppositions or prejudgments of observed things openly, not disturbed by habits within the natural world. The nature of the study described things as they were when cybercrime preparedness and experiential learning were received by police personnel. Retrospective reflections of the conscious brought additional ideas, meanings, intuition, and self-reflection. The act of consciousness and the object of consciousness are interrelated. Moustakas (1994) affirmed that intuition was essential. The scientific inquiry emerged with comprehensive cybercrime information.

The qualitative research design was instrumental in understanding the phenomenon and useful for a qualitative researcher who might not be aware of variables associated with inductive research (Hoepfl, 1997). I collected the data, documented it,

and analyzed the remarkable comments. The inductive data analysis formed certain patterns and paradigms. In addition, the study evoked a narrative with a wealth of descriptive responses and evidence. Moustakas (1994) argued the phenomenological approach works to enrich the research questions. In essence, how did the experience of the phenomenon come to be what it is? The study engaged and focused on the described meanings of the participants regarding the phenomena with scholarly explanations and timely thoughts obtained from the collected data inquiries.

The data provided rich holistic detailed results. Moustakas (1994, p. 65) asserted that "No experience is ever finished or exhausted. New and fresh meanings are forever in the world and in us." The solid all-encompassing cybercrime research data inquiries were essential to discover responses and emit the flow of the process and procedures. The police personnel answered and described their thoughts and personal interpretations that expressed a vast amount of cybercrime evidenced components with stated actions and ways. Moustakas (1994) argued that there were no limits to comprehension or sense of fulfillment without the insight of a person, place, or thing. The police personnel had rich scholarly comprehension that occurred in their perceptions concerning all aspects of the cybercrime phenomenon.

The traditions of Husserl (1913) and Moustakas (1994) offered the step-by-step process and procedures for conducting the empirical phenomenological qualitative study. The study was contextualized with a philosophical foundation. Husserl (1889-1976) furnished an experimental method based on the conscience of the phenomenal scientific

knowledge. He discovered the essence of meanings, whereas Moustakas focused on the theoretical underpinnings of the phenomenon. The essence was prevalent in the content of the police personnel's consciousness. The focus was on the object that first appeared in the conscious mingled with the object in nature. It created the meaning and then there was an extrapolation of knowledge (Husserl, 1931; Moustakas, 1994). Most qualitative studies have certain philosophical components due to their main characteristics. These qualities play an important role in investigations and evaluations. Investigations emphasize content in human complexities (Denzin & Lincoln, 1998).

The empirical phenomenological study methods of Moustakas (1994, p. 101) established the nature, epoche, phenomenological reduction, imaginative variations, synthesis, and essences that were essential to conducting the study. The methods of the phenomenological data analyses assessed full transcripts from each participant. The clarity of the meanings and the structure further explained the approach. It worked making it consistent with the overall phenomenological and methodological design with strategic parameters in the human science qualities. There were seven listed requirements for expert human science qualitative research (Moustakas, 1994; Martin, 2021).

- Recognize the value of qualitative methodologies and designs in the studies of law enforcement personnel and the lived experiences in cybercrime preparedness that are not approachable through quantitative approaches and methodologies.
- Focus on the experiences of wholeness, which is a holistic analogy and approach, instead of concentrating on the parts.

- Search for cybercrime preparedness meanings and the essences of the police personnel's experiences, rather than explanations and measurements.
- Obtain the descriptions of the experiences and perceptions using first-person accounts in semi-structured informal inquiries and conversations.
- Regard the data of the police personnel experiences as imperative in understanding human behavior and as evidence for scientific investigations.
- Formulate the questions and problems that reflect the interest, involvement, and the researcher's personal commitment assisting to close the literary gap.
- View the experiences and the behaviors as an integrated and inseparable relationship of the subjects and objects, as well as the parts as a united whole.

Moustakas (1994, p. 21) asserted there were common bonds in the human science phenomenon of qualitative research. The common features distinguished the qualitative research model from the traditional natural science quantitative methodologies with aligned theories. Integrating the qualitative research in the common bonds of the orchestrated practical approach and application was utilized in this empirical qualitative phenomenological study. The empirical sound research provided an invaluable tool that incorporated the police personnel's prior cybercrime preparedness, training, and experiential learning. Ideas and critical thinking were garnered with the lived experiences that provided the essence of the cybercrime phenomenon. It entailed a comprehensive description revealing cybercrime preparedness, applications, and the engaged pragmatic operations as an integrated whole. The participants reflected and integrated the great

a plethora of prior cybercrime preparedness as a systematic scientific approach.

Moustakas' Life

Moustakas (1994, p. 41) aligned the human scientific empirical phenomenological research. It was guided by epoche, phenomenological reduction, imaginative variation, and synthesis of meanings. The philosophy positioned the ultimate knowledge in the regions and powers of self. It provided a foundation for significant research. Moustakas' wisdom was not obtained from written text or people; it was garnered from the introspection of observing, perceiving, and understanding within conscious reasoning. Moustakas (1994) expressed being alone with critical thinking from self-dialogues and the immersions of transcendental places. The self-dialogue provided intuitive thinking. It illustrated the constant search for Moustakas to know the truth of things through alertness, intuitive learning, and wise perceptions. The enigmatic intelligence worked in unity with detailed thoughts, individual reflections, and philosophical phenomenology. The illuminated discernment of Moustakas was obtained by avoiding people who attempted to educate and coach with their personal phenomenon and knowledge.

The research underpinnings of Moustakas (1994) expressed the challenge to describe things as they are and understanding the essence and meanings in the light of intuition and self-reflection. The meanings were created when the object appearing in the consciousness mingles with the object in nature, "what appears in consciousness is an absolute reality while what appears to the world is a product of learning" (p. 27). Minimizing biases is referred to as epoche or bracketing imperative in the empirical qualitative phenomenological study. Epoche is mandatory and critically refrained from

any judgment, eliminating biases and prejudices.

The theoretical underpinnings of Moustakas (1994), the data analysis of van Kaam (1966), and the foundational theory of Kolb's (1984) experiential learning theory (ELT) developed the synergistic foundation and outcome of the study. The underpinnings affirmed by Moustakas (1994) were built upon by the philosophical phenomenologist of Husserl (1977). Perspectives that appear in the consciousness have meanings of the police personnel's lived experiences. Husserl (1965, p. 23) articulated the following.

> It is a "science" because "it affords knowledge that has effectively disposed of all elements that could render its grasp 'continent' . . . phenomenology is the 'science of science' since it alone investigates that which all other sciences simply take for granted (or ignore), the very essence of their own objects.

Husserl cited reflections that occurred in the phenomenological approach and systematic logic. The resources carried out the analysis to arrive at descriptions of the experiences.

Moustakas' Phenomenology

The belief of Moustakas (1994) was the desire to approach first things first in seclusion, with the ability to encounter fresh life. It allowed the saturation of the circumstance to critically assess and become aware of the true reality of the person's own vision. This resulted in becoming real from introspection. When Moustakas (1994) was alone, open freedom allowed the visibility of intelligent discernment to critically think, intuitively learn, and encounter great knowledge. The reality of the belief was

that a person's own personal interpretations and understandings resulted in a higher level of knowledge. The proverbial premise 'as a man thinks in his heart, so is he' was the foundational theoretical underpinnings and reality of Moustakas (1994). Husserl (1970) and others based much work on the data analyses of van Kaam (1966). The enlightened thoughts and wisdom of Moustakas (1994, p. 41) were garnered by taking quality time with retrospective reflections and pondering introspections. Moustakas provided rich significant conscious understandings of the truth of the teachings and involvement. The presence and critical thinking evolve when the individual is alone. Deliberate consideration and introspection are essential. Moustakas (1994, p. 41) stated

> The most crucial learnings have come from lonely separation from the natural world, from immersions and self dialogues and from transcendental places of imagination and reflection.

It was my pleasure to experience the honor and privilege setting under the tutelage of Professor Dr. Clark Moustakas at Merrill Palmer Institute on the campus of Wayne State University (WSU) in Detroit, Michigan for 12 training sessions. My initial encounter with Dr. Moustakas was when I was completing a Post-Master Degree [an Education Specialist Degree (Ed.S)] at the University of Detroit (U of D) in Counseling Psychology. The lead professor was Dr. Helen Kean (Executive Dean of U of D's Counseling Psychology Program) and a close friend of Dr. Moustakas. Dr. Kean selected five students to attend the Child Play Therapy Counseling of Dr. Moustakas consisting of three (3) sessions. In the 2nd encounter, Dr. Moustakas served as my professor in a four-week accelerated course at Merrill Palmer Institute. I was completing another Education

Specialist Degree (Ed.S) in Gerontology [Psychology of the Aged] held at WSU with Dr. & Dr. Kahana, the husband-and-wife visiting professors from the University of Michigan. In the final encounter, Dr. Moustakas taught a five-week 'Phenomenology Philosophy' course. Moustakas provided enlightened knowledge and understanding as a professor.

Moustakas (1994) established a step-by-step process when a person conducts a phenomenological study. It was reinforced by the fact that in-depth perceptions were obtained through internal observations and intuition. Moustakas affirmed the majority of learning was derived from quiet time. Thinking deeply is paramount to understanding as one is alone and essential to strategic thinking skills. Conscious intuitive reflections are necessary to separate from the natural world. I learned much listening to Dr. Moustakas and reaping rich golden nuggets of knowledge and understanding. The elucidation of great analytical thinking intermingled with Husserl's teaching philosophies.

Philosophical Perspectives of Husserl

The roots of Edmund Husserl (1859-1938) were in philosophical perspectives and articulated the reality that a study was best suited for qualitative phenomenon experience by understanding the essence of participants and the 'moments of matter.' It was further verified by the empirical phenomenology description. Common or shared experiences evoke reflection-based introspective analysis (Husserl, 1931). It intertwined both, the linguistic expressions, and modes of intuition in the lived experiences. Husserl (1900), a mathematician (articulate in the science of numbers, symbols, and calculations), introduced the term bracketing as an analogy for the actions in suspending beliefs. The term bracketing works to eradicate assumptions, biases, or preconceived notions to

improve the research. Bracketing was essential during the data analyses. Holloway & Wheeler (1996) asserted that the researcher explores and identifies any preconceived notions in order not to allow them to interfere with the feedback from participants. The essence or nature of experiences in phenomenological findings requires bracketing which the method that searches out commonalities. The human experiences require bracketing to search for commonalities that might be related to other phenomenologists' research studying the same phenomenon or experiences (Patton, 2002, p. 107). The qualitative study required focusing on descriptions of what the police personnel experienced and understanding how they actually experienced what they experienced. Streubert & Carpenter (1999) affirmed that bracketing required the researcher to remain neutral with respect to beliefs or disbeliefs in the existence of the phenomenon. Neutrality was of the essence in this phenomenological research, which means that the researcher does not prove or set out to establish a particular perspective or manipulate the data to arrive at predisposed truths (Patton, 2002, p. 51). As the researcher, I acknowledged my own biases, and judgments, and bracketed the components. I applied epoche to the study to ensure neutrality. Neutrality requires that the researcher is not concerned with proving a point and does not have a predetermined theory to prove anything. The four components of Husserl (1970) and Moustakas (1994) ensured bracketing prevention. Bracketing established processes and procedures to eliminate biases with preconceived personal rationale. There were essential requirements to bracket and ensure biases are eradicated and all steering is eliminated. Moustakas (1994) cited one should not speak of the

phenomenological methods as if they were an entire group of equal methods. It is imperative with the summation of the four segments that align and distinguish bracketing that eliminates the beliefs and disbeliefs. Husserl (1970) and Moustakas (1994) described bracketing in regulating the descriptive data including the four segments.

- Epoche required the researcher to set aside prejudgments and address any biased prejudgments and preconceptions to enter the conscious and exit freely.
- Phenomenological Reduction involves bracketing with reflection and reduction, to think, perceive, judge, describe features, and reconsider. Horizonalization requires that all initial comments are treated as equal value.
- Imaginative Variation includes systematic variations with possible structural meanings. Search for examples to illustrate the invariant structural themes and facilitate the development of a structural description of the phenomenon.
- Synthesis of Meanings is the final step in the intuitive integration of the basic textual and structural descriptions into a synergistic oneness for the essence of the experience. Illustrate the invariant structural themes and activate the development of the structural description.

The descriptive data provided clarity with understanding, and it efficiently aligned the foundation of bracketing.

Descriptive Data

Many descriptive data transpired evoking rich valuable experiences in verbatim statements of participants (Dempsey & Forst, 2013; McMillan & Schumacher, 2001).

The police personnel shared cybercrime preparedness, prior training, and experiential learning of the phenomenon. Insight was garnered from the descriptive data to mitigate cyber-attacks. The analytical data provided opportunities to obtain a rich understanding of human and social perspectives experienced by police personnel. The more poignant discernment was evoked by the phenomenological evidence and scholarly investigation of the cybercrime recommendations. The authoritarian, Moustakas (1994), explained the theoretical underpinnings in the study, which provided the human science perspective and the research design resulting in the inductive analysis development.

Inductive Analysis Development

The inductive analysis development began and allowed categories with dimensions to build and interpret general patterns of the participants' prior cybercrime phenomenon data inquiries feedback (Dempsey & Forst, 2013; Martin, 2019; Patton, 2002). The qualitative inductive development and strategies contrasted with the quantitative deductive approach, where the data is analyzed in accordance with the framework of the experimental designs that require variables, measurements, and hypotheses. The inductive development has at least two implications for an empirical qualitative phenomenology study. First, what is the most significant phenomenon that needs to be scientifically described and researched? Second, what research methods, design, and analysis are necessary to gather from the data (Maxwell, 2013; Patton, 2002)?

The inductive analysis emerged from the data and allowed descriptions of the police personnel's prior preparedness, experiences, and learning to analytically

evoke the phenomenon of cybercrime with rich transferable results. The police personnel described their individual reflections and acute perspectives focused on prior cybercrime preparedness. The phenomenology collected and analyzed the participants' perceptions finding a way to synthesize and present the findings. The inductive analysis discovered codes, categories, patterns, and aligned themes as it explored and confirmed creative synthesis (Martin, 2015; Patton, 1990). The informal semi-structured inquiries were open-ended, and not rigidly structured, and the fluidity allowed the three research questions to be answered utilizing the 10 data inquiry instrument. The data collection inquiries were logical and systematic providing opportunities for the police personnel to express themselves without interference. The inquiries were flexible and collected data from open-ended well-designed data inquiries. The inductive reasoning and analysis moved from the specific to the general. The progression emanated from a set of thoughts and perceptions to the patterns or designs that represented a degree of the order under research. It revealed a spectrum of data resulting in high-level rich information.

The analytical and inductive development focused on the method and research design. Miles and Huberman (1994) asserted that pre-structuring the methods tended to reduce the amount of data and simplify the data analysis (p. 16). The design allowed the inductive analysis development to list the beliefs, thoughts, and values of the personnel. Moustakas (1994) expressed that individual textural-structural descriptions provide underlying dynamics in experiences possessing meanings developed from a composite

description, representing the group (pp 120-121). The Modified van Kaam's data analyses (1966) examined responses from the data inquiries, which were gathered in the police personnel's natural settings via electronic devices with the assurance of confidentiality for the police agencies and law enforcement personnel.

Confidentiality

The police personnel and agencies were afforded total confidentiality with the name of the agencies and participants not revealed in the study. The personnel could exit the data inquiries at any time without any negative repercussions. The phenomenological design of Moustakas (1994) obtained rich perspectives regarding cybercrime preparedness and Kolb's (2015) experiential learning theory. The agencies and participants were cognizant that the researcher, Walden University, and publishers would review the data; however, no names, cities, or agencies would ever be revealed. Each willing voluntary police personnel knew the purpose of the study and understood the individuals would view the data and how it would never be divulged. All were aware of the benefits or risks and how the data would be handled and destroyed at the designated time after the study's completion. The participants knew research results could benefit others in the field of criminal justice and other disciplines with the study's transferability.

The research required establishing a workable plan, identifying the methodology, aligning the style, and substantiating a cohesive agreement with the law enforcement agencies to perform the inquiries. It further required identifying the settings, obtaining informed consent or wet signature, and ensuring confidentiality with the established

relationships of the law enforcement commander, chiefs, or designees. All mandates required by Walden University had to be fulfilled. Debriefing was the final pinnacle that evoked tremendous thanks to the administrators and law enforcement personnel with expressed appreciation at the completion of the data inquiry sessions.

Debriefing

Debriefing was important. It entailed thanking the police personnel for their willingness and dedication to actively participate in the study. The debriefing session entailed approximately five to 10 minutes, depending upon questions or comments law enforcement personnel might ask or articulate. Debriefing transpired after the inquiries and all data was collected. I expressed gratitude and appreciation to the administrators emphasizing the study could not have been performed without their participation.

The debriefing session reinforced the high regard for candid responses of the law enforcement personnel, their willingness to participate, and once again the reiteration of thankfulness. Each participant received a debriefing thank you statement emphasizing appreciation while reinforcing the need for any further comments or additional feedback. I provided my name, telephone number, and e-mail address once again to each participant for inquisitions, comments, and if they desired to receive the final research results. The feedback aligned and rendered rich transferable information from the original data gathered from the personnel. Assumptions were not eliminated, and they emerged in the phenomenological qualitative study.

Assumptions

Assumptions can be facts or myths. Patton (2002) asserted that there were both benefits and risks in the deep engagement in the complexity and assumed content encompassing the phenomenology qualitative naturalistic inquiry research. Assumptions can allow the consideration of researcher to regard diverse relationships to the phenomenon under inquiry. I understood that it was imperative to challenge all assumptions, especially the assumptions of the researcher. It was necessary to allow skilled and professional experts to critically assess and evaluate my data research inquiries to assure there were no underlying biases, hidden agendas, or assumptions steering the 10 data inquisitions. I further assumed that the findings of the participants were genuine, honest, truthful, and with the utmost integrity. I listed assumptions regarding the conjecture that the raw data was factual and properly interpreted.

The qualitative study incorporated assumptions that the police personnel demonstrated with confidentiality, availability, and intellectual knowledge. I was cognizant of the limitations due to the small size and the search for participants during the COVID-19 pandemic. The personnel was aware of no compensation. Each was cognizant of their ability to exit at any time. The reality of quality time to complete the data inquiries and email is not a light assumption (Martin, 2015). The assumptions were listed from collecting data to finalizing the open-ended data inquiries performed voluntarily by the personnel. Workable data arose with clarity to provide rich in-depth information promulgating and contributing to the data analyses. The literary gap was filled and brought positive constructive social change with enriched transferability.

Further assumptions predicated that police personnel had to be available, willing to participate, and aware of the data inquiries. Each had to be cognizant of their prior cybercrime preparedness experience and learning. They had to comprehend the nature and content of the research and efficiently answer the data inquiries. The assumptions reinforced the fact that participants provide personal thoughts and reflections of integrity concerning cybercrime preparedness with workable recommendations.

The assumptions of the research were methodologically designed. The data carefully captured and thoroughly described how the law enforcement personnel elucidated, described, and accurately remembered their preparedness. The participants experienced, critically assessed, and evaluated their prior cybercrime preparedness with recommendations. The assumptions of McMillan & Schumacher (2006) and Patton (2002) were aligned with overall qualitative empirical phenomenological research assumptions. Patton (2002) expressed that as a researcher, one should not fail to challenge all assumptions, especially the researcher's biases, and perceptions; and should not assume all inquiries have been addressed (p. 337). Assumptions can be influenced by an impetus of various driving forces that arise during the process; while responding to open-ended data inquiries. The police personnel were cognizant of understanding the scope and limitations of the research. I determined the fundamental atmosphere, ethos, and orchestration of the study. I assumed that the police personnel would honestly express their thoughts, interjections, and interpretations. Further assumptions procreated that the police personnel would follow through and complete the data inquiries as promised. The scope and limitations of the study were aligned accordingly.

Scope and Limitations

The scope and limitations employed in the qualitative phenomenological inquiry study method collected rich data from police personnel. The focus was on the law enforcement personnel in the state of Michigan with the scope of cybercrime preparedness and recommendations for mitigating cyber-attacks and cyber-terrorism. Some police personnel might have been apprehensive in answering and responding truthfully due to their ideal work assignments or excellent positions in the law enforcement agency. Hence, if the participant expressed the truth on the data instrument it could place them in jeopardy or in a precarious position. If the comments were negative regarding cybercrime preparedness, the participants might experience difficulty in providing accurate feedback. Added limitations could include altered or distorted responses due to the police personnel's frustrations, biases, and tiredness. Stress, work overload, and sicknesses were other challenging issues. The target population was requested from diverse Michigan police agencies throughout the state. The administrators made the decision whether their agency would participate in the research.

The small sample was a limitation. However, the empirical qualitative phenomenological approach collected great and rich data from the small purposeful sampling. The study obtained valuable comprehensive data with descriptors. Patton (2002) argued that studying small information-rich participants yield in-depth insight. The small group disclosed and elucidated great cybercrime preparedness data. Comprehensive recommendations were expressed to eliminate cybercrime and cyber-terrorism. Giorgi (2011) affirmed phenomenology can be relevant beyond the formal

research. Anything experiential can be addressed if one can experience it and describe it. It is essential to work at understanding. When a recognized phenomenon reveals a literary gap, it is imperative that someone initiates the research to fulfill the gap.

Retrospective reflections and interpretations established a time of hindsight and elaboration. The police personnel continually make decisions with problem-solving entities. Perceptions and reflections are the main sources of knowledge in phenomenology. The intentions with sensations encompass the entire concrete act of perceptions (Husserl, 1977). There were challenges that existed in the phenomenological research study. At times police personnel had cases or classified information they are unable to divulge. It might be an open case or extreme internal covert information. Many investigative areas are protected and preclude personnel from revealing internal information (Inciardi, 2010). The study was small (N=8) with no generalizations. The high-level informative data resulted in transferable information that can be conveyed to other disciplines. I abstained from making any biased opinions. The scope and challenges were viewed early on prior to developing the empirical phenomenological qualitative design. The scope explained the study's significance and the critical need for trustworthiness.

Trustworthiness

Trustworthiness is essential consisting of integrity, fairness, and reliability. Impartiality and accuracy with honesty intertwined the vital thread of truth throughout the research. It established authenticity and credibility in a systematic manner during the

qualitative phenomenological study. Patton (2002, p. 546) assured trustworthiness was the "reflexive consciousness about one's own perspective, appreciation for the perspective of others, and fairness in depicting constructions in the values that undergird them." Understandable terms are essential when addressing trustworthiness. The important criteria of trustworthiness were credibility and dependability (Devault, 2018).

Trustworthiness provided integrity in the study's foundation. Seales (1999) affirmed that trustworthiness lies at the heart of issues conventionally discussed as validity and reliability (p. 266). Empirical phenomenological qualitative studies require internal validity and transferability as analog to external validity. According to Lincoln and Guba (1985), it was argued trustworthiness is an extension of the person who is collecting and analyzing the data. The researcher's bias cannot be eliminated and can often threaten validity. The biases must be handled with epoche and sound reasoning. I selected the subject matter, data, and techniques for the phenomenological qualitative study. I identified and critically assessed the empirical techniques that could threaten or challenge the data collection and analyses by employing the Modifications of van Kaam (1966). The biases and assumptions were addressed with applied knowledge and precautionary proactive measures. Knowledge alone is not power; however, the application of knowledge with trustworthiness is power if utilized with wisdom and discernment. The police personnel received open-ended data inquiries via electronic devices due to the COVID-19 pandemic. It allowed sufficient availabilities and opportunities for participants to answer and verify trustworthiness during the responses.

The concepts of validity and reliability are utilized in quantitative research. However, it was not an ideal selection for qualitative research. Devault (2018) assured that reliability and validity are not a good fit; instead, researchers must substitute them with trustworthiness. Systematic trustworthiness critically assesses and evaluates intellectual rigor, creativity, and insight with intangible components (Patton, 2002). The phenomenology qualitative study produced findings that could not be obtained through the quantitative statistical methods that focus on cause, effect, prediction, and generalization. The qualitative phenomenology research sought a different segment of knowledge with illumination and understanding. Interpretations were utilized in the collection of data inquiries with a small number of subjects providing rich data. The dominant factors of credibility in quantitative research are derived from surveys and instruments, whereas, in qualitative research "the researcher is the instrument" (Patton, 2002, p. 14). Qualitative research refers to reliability as consistency and consistency as the results, findings, and outcomes (Patton, 2002). Ethical considerations are imperative.

Ethical Considerations

There were ethical considerations and challenges in the qualitative data collection. Patton (2002, p. 406) affirmed that the researcher needs to have an ethical framework when dealing with ethics. Ethics requires sharing all aspects of the study with the police chiefs and personnel. The purpose and the basics of the study must ensure there are no hidden agendas or deceptions. The option to exit at any time and the ability to obtain the final study results were imperative. The ethical considerations entailed moral judgment and professional standards written in the informed consent. It provided in advance to the

law enforcement administrators and police personnel the assurance of confidentiality and limited anonymity. The name of police agencies was known to the researcher and the IRB. The Informed Consent answered the following questions submitted first to the law enforcement administrators and then the police personnel.

- What is the purpose of collecting the empirical qualitative phenomenology research with data collection procedures and processes?
- How will the data be collected, utilized, and what are the required criteria for the police personnel to voluntarily participate?
- What are the data inquiry mandates and the required qualifications that must be submitted by the law enforcement personnel?
- How will the identity of police agencies and police personnel be assured privacy with confidentiality before, during, and after the study?
- How will the data responses be handled and where will the data be securely stored (locked in a private safe) until the five-year Walden University mandatory requirements are fulfilled?
- What risks and/or benefits are involved for police personnel, and will they receive any money or compensation for participation in the study?

All segments of the research were submitted to the police chiefs and directors for approval with data inquiries and stipulations generated in the Informed Consent Forms. Walden University's Institutional Review Board (IRB) provided conditional approval after several assessments and changes. The IRB's full approval could not be provided until the confirmed written notifications were received from the administrators or

designees acknowledging willing agreement for the police agencies to participate.

I was sensitive to the ethical principles throughout the research as the evolving design was procreated. According to McMillan and Schumacher (2001, p. 420), ethical principles are key components in the planning, designing, and data collection ensuring trust and acceptance are implemented. The police administrators received copies of the material that would be distributed to the personnel. After approval by the Institutional Review Board (IRB), the informed consent and description of the study were submitted to the police agencies searching for volunteers. Ethical procedures were imperative throughout the entire research study. Mandatory ethics was essential, clearly established, and applied, which was analogous to the Code of Ethics utilized by police-fire agencies, educational facilities, hospitals, real estate state corporations, and other institutions.

The ethical issues and guidelines were inclusive of the requirements. Ethics required that the personnel expressed honesty, integrity, and veracity. Derrickson (1997) identified 10 basic ethical informed consent components: the purpose of the study; promises and reciprocity; risk assessment; confidentiality and data storage; informed consent and IRB requirements; data access and ownership; researcher's vita and professional background; researcher's confidant or contact person when confronted with challenges; data collection boundaries; and the ethical framework. Basic considerations and standards were essential and efficaciously addressed in the research (Patton, 2002, pp. 408-409). Derrickson (1997) and Patton (2002) provided professional components regarding the ethical checklist provided with skills, words, and ethical considerations.

My confidant for the research was my Chair, Dr. David P. Milen. I emailed the letter of cooperation from the police administrators immediately to the IRB. The research began after full approval.

Informed Consent and Significance

The Informed Consent was provided to the police personnel after the IRB's approval. The consent was clear, concise, and straightforward with an emphasis on the importance and an invitation to take part in the research. The ethical issues were aligned as valuable and workable tools that were applied throughout the study. The police chiefs initially received the Informed Consent Form. Then the police personnel had to make the decision to participate with the required email of "I Consent." The email sufficed any necessary waiver form or wet signature. It further ensured the ethical processes protected the agencies, participants, and educational facility.

The significance of this study worked efficiently in filling the literary gap. The research focused on police personnel, cybercrime preparedness, and experiential learning. The recommendations presented ways to mitigate cyber-attacks and cyber-terrorism. The lived experiences provided a rich narrative with in-depth descriptions of the cybercrime phenomenon. The study brought about critical thinking skills, positive social change, and valuable information emphasizing the need for further research. The participants encompassed Kolb's (2015) experiential learning theory (ELT) with Moustakas' (1994) design and van Kaam's (1966) data analyses. The collected data rendered rich narratives. The data expressed the police personnel's verbatim statements and perceptions with scientific procedures, processes, and data analyses. The inductive

analysis established meanings from the data. It developed findings and themes. The explanations of the findings provided the utilization of practices, theories, and the point of convergence of the former literature research. The qualitative research interactively combined science, data, and evidence to develop the inductive developmental analysis.

I had to systematically search the literature focusing on police personnel and cybercrime preparedness. There was no literature research on law enforcement personnel and cybercrime preparedness training utilizing a blueprint of experiential learning theory. The empirical qualitative phenomenological research added and dispersed a rich in-depth study with the investigation of scientific critical thinking. The research provided well-sourced rich data collected from the personnel. The results emanated opportunities for positive social change with enriched transferability to other entities.

Summary

The empirical phenomenological qualitative study focused on law enforcement personnel in Michigan and their prior cybercrime preparedness, training, and the experiential learning theory (Kolb, 2014). Moustakas (1994) provided the theoretical underpinnings with the concepts of Husserl (1931), principles of Giorgi (1997), and others. The study procured the phenomenon of prior cybercrime preparedness with van Kaam's data analyses. The research procreated rich recommendations to combat, mitigate, and uproot cybercrime. Chapter 1 addressed the evolving cybercrime, problem statement, purpose, and research questions. The definitions were articulated with the significance of the empirical qualitative study. Chapter 2 focused on the literary review with the wide range of diverse undertakings in the complicity of cybercrime,

cyber-attacks, and cyber terrorism. It addressed the gap in the literature encompassing Kolb's (1984) experiential learning theory (ELT), social media, and cyber security. Chapter 3 provided the phenomenon of the qualitative research methodology, design, research questions, purposeful sampling, and the role of the researcher. The study further aligned the data collection, inquiries, and data analysis with ethical considerations. It explored how the study would be conducted. Chapter 4 discusses the findings, research questions, and data inquiries. The data analyses explain the challenges and results, as they articulate the inductive analysis design and verbatim statements. The research expresses the proactive measures to combat cybercrimes, mitigate cyber-attacks, and eradicate cyber terrorism. Chapter 5 provides a detailed summation of all previous chapters. The study explains the significance of the evidence, the key qualitative findings, conclusions, and positive social change. The research provides meanings and results for transferability with rich recommendations for future studies.

Chapter 4: Results

Introduction

The purpose of this empirical phenomenological qualitative study examined and analyzed the lived experiences and perspectives of Michigan's law enforcement personnel with great results from prior cybercrime training preparedness. Moustakas (1994) was the authoritarian who expounded on the theoretical underpinnings of phenomenology. The human science perceptions provided the research design with data inquiries resulting in the inductive analysis. The literary search did not locate any prior cybercrime preparedness focusing on police personnel. The scientific exploration evoked the phenomenological evidence and scholarly investigation collected from the qualitative data analyses. The cybercrime preparedness and experiential learning research presented meaningful results with detailed thoughts and strategies to combat cybercrime and mitigate cyber-attacks.

The literary gap indicated the need to research law enforcement personnel's prior cybercrime preparedness and lived experiences. Kolb's (1984) Experiential Learning Theory (ELT) served as a blueprint and tool to ascertain the participants' experiences. In addition, it gathered the cybercrime learning styles and workplace achievements. The focus was to systematically investigate and enhance the police personnel's cybercrime preparedness. The experiential learning theory (ELT) was utilized as a principle, format, and blueprint. The study procured the experiences and learning styles receiving workable recommendations from personnel as van Kaam's (1966) data analyses were employed.

The theoretical process allowed the cybercrime preparedness to be analytically assessed and evaluated resulting in rich cyber-attack social change with transferable information.

The Theoretical Process

The phenomenological theoretical process engaged the empirical and systematic qualitative theories of Kolb (1984), Moustakas (1994), van Kaam (1966), and others for the overall scholarly foundation and approach. The methods consisted of eliciting and analyzing the evidence of cybercrime preparedness and proactive cyber-attack strategies. The police personnel expressed their perspectives and critical thinking with meanings and implications that fulfilled the goals and objectives of the research.

Goals and Objectives of the Study

The empirical qualitative phenomenological approach depicted the goals and objectives of the study. Opportunities were allowed for open-ended semi-structured inquiries to explore the perceptions with recommendations from the participants' lived experiences (Byrne, 2009). The research was established with scholarly concerns and scientific critical thinking. The systematic understanding provided the analytic cybercrime preparedness phenomenon and experiential learning styles with viable recommendations. The objectives were established to collect the following components.

1. Identify and examine prior cybercrime preparedness and the lived experiences of police personnel.
2. Garner the reflective cybercrime learning techniques and experiences that occurred during the cybercrime preparedness with retrospective perceptual challenges and controversial issues.

3. Assess and evaluate the comments of the participants.
4. Procure the abstract thoughts, ideas, and experiences in the preparedness and what worked or did not work.
5. Obtain the participants' ideas, details, plans, and how the applied skills and knowledge were implemented in the workplace.
6. Share the cybercrime training taught in the communities and other facilities.
7. Express proactive strategies and techniques to combat cyber-attacks and eliminate cyber terrorism.

The data was aligned to evoke empirical qualitative phenomenological research with practices bringing about systematic and coherent cybercrime preparedness with positive social change and transferability. The feedback was analytically assessed in a step-by-step process incorporating the written verbatim statements. The police personnel shared cybercrime preparedness that procreated insight. The descriptive data provided many components to combat cyber-attacks and cyber terrorism. The research rendered rich analytical cybercrime learning to understand the human-social perspectives experienced by police personnel. The goals and objectives provided opportunities to grasp the structure of the research study and its significance.

Significance of the Research

The significance of the study explored and examined the poignant cybercrime challenges, comprehension, and critical thinking of the police personnel and their prior cybercrime preparedness and learning. The feedback provided viable research to fill the literary gap. It elicited a better understanding of the challenges, issues, and results of

the police personnel's preparedness with possibilities to enhance the process. Added recommendations produced provisions and strategies to mitigate cybercrime and cyber-attacks. The study focused on perspectives and preconceived notions of participants with significant rich feedback. The research added to the literary gap with shared valuable data containing significant contributions to cybercrime preparedness. The findings systematically revealed the inductive analytical design from planning to synergism. The indicated strategies and tactics contributed scholarly ways to combat cybercrime. There were eight significant scholarly indications provided in the scientific law enforcement personnel cybercrime research.

- Added to the literary gap that police personnel experienced in cybercrime preparedness and experiential learning (What worked and what did not work?)
- Depicted diverse cybercrime modalities and styles in the learning process
- Demonstrated pragmatic cybercrime applications in the workplace
- Engaged in cybercrime training and supplemental informed requisites in the workplace, community, and educational facilities
- Presented ways and procedures cybercrime preparedness can be further enhanced
- Identified techniques and tactics to better equip law enforcement personnel with workable measures to combat and deter cybercrime
- Recommended preventive strategies and techniques to mitigate cyber-attacks and eliminate cyber terrorism focusing on infrastructures
- Increased the rich preventive cybercrime information to bring about positive and productive social change with transferability to other entities

Kolb's (1984) Experiential Learning Theory (ELT) assisted in providing a schematic paradigm with rich data from open-ended data inquiries. Proactive components emerged aligning techniques to efficiently combat cyber-attacks and cyber-terrorism. The significance of the study produced opportunities to learn from the police personnel's philosophies and interpretations. The initial segment of the learning experiences was developed by Kolb's (1984) theory with principles established as an extension of three theorists: John Dewey (1938), Kurt Lewin (1939), and Jean Piaget (1952). Kolb's experiential learning theory did not totally encompass Dewey's (1938) continuity and interaction ideas; however, they were somewhat interconnected in the reflective thoughts with learning styles and experiences. The comparative analysis of Dewey (1938) was the foundation of learning heightened by expressions in detailed observations oriented towards learning and human scientific experiences. The aspects added that an organic connection exists between learning and experience; it could also result in an error.

Jean Piaget (1952) believed that intelligence was shaped by the interactions of persons and their environmental entities. Piaget defined an action as a sequence possessing components integrated and governed by basic core meanings, which was a way of learning and orchestrating abstract concepts. Whereas, Kurt Lewin (1939) contributed greatly to the experiential learning theory including the data collected from a person's concrete experiences: emphasizing that the analytically assessed and evaluated resulted in conclusions and inferences. Lewin (1939) examined patterns of interaction between the individual and the total field or environment with concepts initially implemented in the integrated systems rather than the parts. Feedback was provided

by individuals with results modifying behaviors and in selected innovative experiences (Kolb, 1984). Kolb utilized these aspects to build upon and incorporate the foundation of the experiential learning theory. The goals and objectives of the study procreated the significance of providing opportunities to learn from the participants' interpretations, opinions, and reflections. There were many challenges and issues during the law enforcement personnel's cybercrime preparedness qualitative research study.

Challenges and Issues

The challenges and issues of cybercrime preparedness in the empirical phenomenological qualitative study included attempting to collect a small purposeful sample to understand and perpetuate the comprehension of the police personnel's prior cybercrime preparedness. The study addressed a gap in the literature on law enforcement personnel and cybercrime preparedness with experiences to enhance preparedness and training. It further extended a proclivity to efficiently establish tactics and strategies to combat, mitigate, and uproot cybercrime. The major challenges were the difficulties in obtaining police agencies to agree and participate in the research. The issues were mainly due to COVID-19 and other confrontations. The obstacles are explained later how they were surpassed in conjunction with other controversial issues and challenges.

Challenges with Corona Virus (COVID-19) Pandemic

The coronavirus (COVID-19) pandemic resulted in major changes in the research study. When I was preparing for the data collection, Michigan became the 3rd highest USA COVID-19 state. Michigan was rated number one in the nation with positive pandemic cases during the latter weeks of the research. The state was highly congested

with the variant strands and international Delphi strains. The COVID-19 pandemic resulted in great sickness, multiple deaths, societal incapacitations, and egregious economic havoc in police agencies and communities. Many segments of the study had to be reworked due to the unknown factors of the pandemic and the escalating inconsistencies. The face-to-face data collection was eliminated at the law enforcement site locations. Many police personnel were hospitalized with positive coronavirus cases that required multiple quarantines. Hospitals were filled and over-taxed with COVID-19 patients. Horrendous havoc was placed on police departments and agencies were greatly overburdened with limited staff. The police personnel were reduced tremendously, and police stations opened only several hours a day. Police personnel were laid-off and hours were restricted to part-time status. Staff was assigned to their home residence with designated virtual-remote limitations. Colleges and universities closed their brick-and-mortar police educational campus units transitioning to virtual remote sites.

Unexpected challenges evolved with multiple protest marches and controversial anger amidst issues against law enforcement departments. Citizens' anger resulted in police incidents, up-ticked arrests, police brutality, controversial accusations of racism, and a potential decrease in police agencies' funds. The extensive sickness, limited staff, the possibility of defunding police agencies, and adverse entities changed the entire parameters of the personnel cybercrime preparedness research study. The restricted hours and skeleton crew of police personnel eliminated active participation in the study for a segment of time. The COVID-19 pandemic continued to rage throughout the state, nationally, as well as internationally with horrendous devastation and unexpected deaths.

Issues with the COVID-19 Pandemic

The police agencies had their hands full with challenging obstacles requiring "shut-downs" in law enforcement units and sections that postponed the research data collection. The police agencies were operating by "appointments only" and restricted hours. Multiple police personnel were affected in unfortunate ways due to COVID-19. Many police chiefs and directors contacted the researcher to apologize for the atrocious conditions and limitations during the controversial incidents and critical COVID-19 situations. The state of Michigan mandated face masks to enter stores; limited numbers in social gatherings; required 6-foot spacing; and mandatory hand sanitizing. Restaurants, bowling alleys, and other facilities were locked down. The police department executives, who had previously agreed to participate in the research, were no longer available.

Mandatory Need to Progress

The crux and fluidity of time were of the essence due to the critical need to complete my dissertation. I received the conditional agreement on August 31st from Walden's IRB [Date: 2020.08.31/09:17:27-05'00']. It was imperative I receive letters of cooperation and notifications from law enforcement agencies. The agreed-upon approval letters were mandatory to garner from all police administrators. I had to submit copies to Walden's IRB and receive full approval to begin the research. Due to the COVID-19 pandemic, the research progression totally restricted the study. I could not request volunteers with the necessary credentials without administrators' approved notifications for IRB approval. I constantly reached out. I mailed United States Postal Services (USPS)

letters to law enforcement chiefs, commissioners, and directors to procure their unlisted telephone numbers, email addresses, or designees. I utilized my networking system of family, friends, associates, and affiliates with an overabundance of telephone calls, texting, and other electronic devices. It was a long taxing and tedious journey.

It was a difficult and challenging issue with insurmountable obstacles. I submitted multiple requests to police agencies throughout Michigan without fruition. After eight months of consistent requests, I finally received approval notifications from law enforcement administrators willing to participate. I submitted copies to Walden's IRB and received affirmations for full approval to begin the research. The potential qualified volunteers received the informed consent forms, demographics, and data collection instruments consisting of the ten data inquiries. The research data inquiry instrument was systematically developed to answer the three basic research questions. The questions collected the scientific data for the empirical qualitative phenomenological study that produced rich workable research results. The 10-part question inquisition instrument was designed to completely answer the qualitative study's three research questions**.** The inquiries were detailed, orderly structured, and understandable with critical assessed evaluations for systematic scholarly processing. There were no esoteric terms or words to confuse the participants. The results were analytically processed utilizing the seven step-by-step Modified data analyses of van Kaam (1966). A complete data transcript of each law enforcement personnel was analyzed. The three research questions were the foundation questions orchestrated and aligned for the research.

Research Questions

Q1.What are the law enforcement personnel's perceptions, lived experiences, thoughts, and ideas regarding the prior cybercrime preparedness, training, and experiential learning, and in what ways was it meaningful, relevant, and interesting?

Q2.Where did the law enforcement personnel acquire the cybercrime preparedness, training, and experiential learning and how was the cybercrime training applied in a practical way in the workplace and communities?

Q3.In what ways have personnel applied preparedness with recommendations to combat, mitigate, and uproot cybercrime, cyber-attacks, and cyber terrorism?

The data collection produced rich feedback from the police personnel. It incorporated much insight into the architecturally designed data inquiries. It provided a wide range of rich police-cybercrime information and a solid foundation for future research studies.

Data Collection Process

The data collection for the empirical research progressed after many challenges, conflicts, difficulties, and setbacks. Copies of the letters of cooperation with confirmed approval notifications were finally received from the police agencies' administrators. I submitted copies to the IRB and full approval was granted. I now had to concentrate on recruiting qualified police personnel volunteers with cybercrime preparedness. The required criteria for police personnel were (1) eighteen or older, (2) current employee, contractual individual, or volunteer for a police agency, and (3) had prior cybercrime preparedness training (via Instructor, Trainer, Professor, Google, Video, DVD, CD, ZOOM, YouTube, Internet, Experience, or Self-taught), and (4) had the opportunity to

apply the cybercrime (fraud, cyber-bullying, theft, cyber-attacks) skills at police agencies or other establishments. I initially submitted the Informed Consent including the other material to the police CEOs to critically assess and evaluate.

Informed Consent

I previously emailed the Informed Consent to the many police CEOs and administrators. It was prior to attempting to obtain any potential police personnel volunteers. The Informed Consent explained the purpose of the cybercrime preparedness study, data collection procedures, sample research inquiries, and the nature of the study. The document ensured confidentiality, and anonymity, and listed any risks or benefits. It affirmed that the research did not personally offer direct benefits to the police personnel; however, the study would provide rich data benefitting other agencies. The outcome would depict cybercrime preparedness and learning styles with techniques to mitigate cybercrime and cyber-attacks. The law enforcement CEOs submitted affirmations as willing agencies to participate in the research. The affirmed agreements were submitted to the IRB with confirmed decisions. I then received lists of qualified police personnel. I contacted and electronically submitted the documents to the potential volunteers. Willing volunteers emailed “I Accept” to my email address. The data did not identify or divulge any police department or participant via the shared demographics. To further ensure anonymity the participants set up free temporary emails (yahoo, hot mail, g-mail, AOL, or net) with coded names or pseudo-initials. The police personnel anonymously submitted the demographics and data inquiry research responses. The process ensured additional confidentiality and anonymity for all police agencies and personnel.

Data Inquiries

I submitted the data inquiry instruments to the police personnel with assurance the words and terms in the data collection tools were understandable, clear, concise, complete, and with precision. I emphasized the importance of integrity and truthfulness when responding to data inquiries. The research requested each participant to respond to the 10 questions by providing examples and workable strategies. The police personnel provided much cybercrime preparedness data with a preponderance of scholarly suggestions to mitigate cybercrime, cyber-attacks, and cyber terrorism. The participants were encouraged to immediately email, telephone, or electronically contact me if there were any areas needing clarity. The data inquiries consisted of 10 open-ended semi-structured questions prepared to collect the experiences and perceptions of the police personnel. The responses and explanations produced extensive intellectual data.

I contacted only two participants to ensure the expressed comments presented were correctly detailed in the inductive inquiry analyses. Accurate data clarifications were affirmed via email, telephone, or other electronic devices. My desire was to assure the interpretations were accurate concerning the inductive inquiry analysis design. I contacted and emailed two participants, and I assured them of neutrality. I did not interject any biased ideas or attempt to steer them in any way. The two expressed their personal opinions and diverse learning with critical thinking. They both agreed that the inductive inquiry analysis interpretation was accurate and closely aligned with their personal interpretations and analogies. The data inquiries provided clear elaboration. The personnel emanated rich intellectual insight. The wealth of professional knowledge of the

police personnel was astronomical. The participants presented responses to the data inquiries with a great range of cybercrime discernment and scholarly intelligence.

Collection of Data

The data collection process required extensive time due to COVID-19. I received many verbal promises from the chief administrators with no further responses or departmental feedback. The collection process required locating police agencies with qualified cybercrime personnel. It was amazing how many police organizations did not have cybercrime units, sections, or personnel who had participated in any cybercrime training. Many police administrators stated that their police personnel had never had a cybercrime class or written any cybercrime reports. Finally, 10 law enforcement administrators verbally agreed to participate. However, the promises were short-lived. Within the process of two weeks, all ten directors and chiefs were unable to abide by the verbal telephone affirmations; and not one police administrator could follow through with the commitment. Two administrators were transferred; three chiefs moved into other positions (outside the state); two police directors became ill with COVID-19; one retired and two died from the COVID-19 pandemic. Many months passed prior to finally obtaining a written approval notification from a law enforcement administrator. It was an extremely difficult and long taxing journey.

Finally, after months of requests, I received written notification approvals from police administrators. I immediately submitted the letters to the IRB and received full approval. Research began. As participants were recruited, preparations for the data were established to systematically align on spreadsheets and to ensure the data was accurately

recorded. The comments and details were coded and appropriately documented. The spreadsheets recorded data responses in designated areas. Documented were the hieroglyphic contact dates, times, comments, and diverse learning with workable cybercrime entries. The data was examined utilizing the theoretical underpinnings of Moustakas (1994) and van Kaam's (1966) step-by-step Modified data analyses. The data collection provided the extensive phenomenon of cybercrime with in-depth critical thinking. The transcripts emitted comments supported by verbatim statements. The sample was small (N=8); however, it provided an immense plethora of data.

Description of Sample

The targeted participants in the qualitative phenomenological study were initially projected at approximately 10 to 12 skilled personnel with cybercrime preparedness. Eight volunteered and provided the essentials with the demographics (job title, position, employment, volunteerism, gender, approximate age, education, agency, and experiential learning). I was unable to document much of the demographic data due to the privacy, protection, and anonymity of the police personnel. The participants were well-versed with extensive scholarly cybercrime intellect and high-level perceptions. The purposeful sampling aligned responses from the few participants (N=8). The personnel data was studied in-depth and yielded rich insight focusing on the cybercrime phenomenon.

Patton (2002) affirmed that the principles of purposeful sampling were utilized in qualitative research for identification, selection of information-rich research, and more efficient use of limited resources. The sampling included willing law enforcement

agencies with site selections in Michigan and qualified volunteer personnel. The study required police personnel willing to participate with cybercrime knowledge, availability, and experience. The sampling consisted of eight voluntary participants with in-depth cybercrime insight. The scholarly intellectual cybercrime wisdom procreated much data with a rich impartation of technological information for future studies and transferability. The police personnel described their experiences: understanding that the ability to efficiently describe cybercrime knowledge and experiential learning skills was a complex process. The study provided comprehensive data analytically assessed by van Kaam's (1966) data analyses. The computerized data spreadsheets systematically documented inclusive segments for comprehensive data analysis.

Data Analysis

The collected data was analyzed by the Modified data analyses of van Kaam (1966). The spreadsheets and charts initially aligned diverse sections of concepts, codes, and categories with insight developed from the police personnel's cybercrime preparedness and training perspectives. The empirical design and organizational strata aligned data that were systematically and strategically analyzed. The prolific documented spreadsheets allowed data to be constructively entered and analytically processed into contents, codes, categories, patterns, themes, and segments. The results produced in-depth comparative analysis data related to the phenomenon under study. Van Kaam's (1966) data analyses approach served as an intense tool. The participant's cybercrime data was orchestrated and processed utilizing van Kaam's procedures taken under critical

advisement. The recorded transcripts required organizing the data in accordance with the principles evidenced in the integrity of scholarly professional research.

All data inquiry transcripts were recorded to ensure the full dimensions emerged with details and in-depth insight. The process of epoche, phenomenological reduction, imaginative variation, synthesis of composite textual, and composite structural descriptions was employed in the research. Experiential learning was embraced and the ways we learn, what is learned, and why it is learned. The data was guided by the evidence and with bracketing. The process assured that my own perceptions did not engage as part of the participants' reflections or perspectives. The data inquiries were critically assessed, promulgating intensive far-reaching comprehensive components. A detailed examination and a systematic investigation produced information inculcating the approach of van Kaam's data analyses. The procedure required collecting, recording, reading, re-reading, and re-reading each segment of the data. The system aligned the data and identified categories designated as codes, categories, patterns, and segments.

I had to step aside from any personal biases with bracketing. I assessed and evaluated the documented data by examining, categorizing, and thematizing. The data analyses were leveraged in accordance with van Kaam's data analyses with accentuated support of Moustakas (1994). The principles were based on scientific law to explain the natural operations of the research. The meanings and essences of the cybercrime preparedness phenomenon were derived from the conjecture of the composite descriptions and developed experiences in the data analyses. The law enforcement personnel's feedback was aligned as individuals, as well as a coordinated collaborative

diverse group. The entire process was articulated as an analytical assessment progressing into a synergistic whole.

Analytical Assessment

The extensive analytical data assessment ensured neutrality and bracketing utilizing van Kaam (1966) with the support of Moustakas (1994). Bracketing required locating key phrases and statements. There were interpreted meanings of the phrases from the police personnel's interpretation. Meanings were revealed after an intense investigation that evolved and offered a tentative statement or definition of the phenomenon. The data inquiries were assessed by applying the seven steps of van Kaam's (1966) data analyses with vital comprehension. The detailed examination and systematic investigation produced rich cybercrime information from the data analyses.

The collected data inquiry contents were recorded, contextualized, and entered on spreadsheets. The responses were all documented and evaluated by examining the explanations, nomenclature, and comments. The detailed data was sectioned into segments to determine distinct qualities and essential features. The distinct qualities were then characterized, grouped, and ranked. The features were elements with defined words, terms, and phrases positioned on the spreadsheets.

Five distinct features emerged, were examined, and investigated in detail to equip the alignment in sequential order. The features were identified as concepts and listed as codes, categories, patterns, segments, and strategic themes. Codes were defined as words, terms, and phrases expressed as a set of principles and a system of symbols in the arrangement of things. Codes were diverse, unique, and developed into categories.

The categories were classified as divisions in the orderly combination of things. The classificationswere coordinated as systematic levels transitioning into patterns. Patterns were plans or models designed to make things predictable, and achievable, and what could happen with workable segments. The segments were defined as emerging points, recurring issues, identification purposes or objects moving into higher levels referred to as strategic themes. The strategic themes consisted of skilled management, organization, and planned approaches with a variant of diverse procedures. Many terms overlapped or were in close proximity. Figure 7 was entitled the *Cybercrime Preparedness and Training Matrix Paradigm*. It was created and designed from the research responses.

Figure 7

Cybercrime Preparedness and Training Matrix Paradigm

FEATURES	**DEFINITIONS**
Features were formulated from the police personnel's documented concepts, ideas, and abstract notions.	
Codes	Set of principles, symbols, words, terms, and phrases in the arrangement of things.
Categories	Divisions in the scheme of classifications with coordinated systematic levels.
Patterns	Plans or models designed to make things predictable, achievable, and can happen.
Segments	Sections or points, recurring issues, identifiable purposes, or objects.
Strategic Themes	Insight and understandings in mgt and planning with approaches and procedures.

The context of Figure 7 labeled as the *Cybercrime Preparedness and Training Matrix Paradigm* were examples collected from the research data responses. The training matrix paradigm was developed to analytically assess the data inquiries. Five basic features were defined and sequentially aligned with meanings coded and categorized. The cybercrime matrix paradigm was developed as patterns evolved. They then expanded into segments and extended into the strategic themes procreated as an evolutionary process.

The strategic themes included detailed data that allowed a creative synthesis to become a reality. The naturalistic design allowed police personnel to respond to the data inquiries in their natural settings via emails and other electronic devices. The design was flexible with participants utilizing the necessary time to complete the data inquiries that developed into codes, categories, patterns, segments, and then strategic themes.

Moustakas (1995, pp. 82-83) described data as the non-judgmental stance in listening deeply and entering the other person's perception and experiences "to encourage and support the other person's expression, what and how it is, how it came to be, and where it is going." The acquisition of the comprehension and the facets of 'inner understanding' and 'perceptual listening' demands in-depth listening with empathic neutrality to critically assess and evaluate the strategic themes. The strategic themes were gathered from the police personnel's written formulated perceptions with diverse applications. The strategic themes expanded taking on the quality of intellectual depth as the law enforcement personnel reflected and evolved while answering the 10 data inquiries.

The perceptions and vigilant crafty thoughts emanated keen senses of discernment and judgment. It resulted in feasible, operational, and quintessential engineered thoughts, ideas, and analytical perspectives. The magnitude of innovative ideas perpetuated creative thinking as the police personnel actively employed organized undertakings. The wise judgment and projective thoughts and discernment articulated foresight to implement functional ways to mitigate cybercrime and cyber terrorism.

I initially collected a vast amount of data, which began to emanate a

collaborative cycle-like contextual continuum. I then reworked the strategic themes and noticed many were in close correlation to Bloom's seven *Taxonomy of Educational Objectives* (1956**),** as well as Kolb's (1984) basic experiential learning theory. I decided I would orchestrate the alignment of Kolb's experiential learning encompassed as an acquisition to the four integrated components. The four components entailed Kolb's concrete experience, reflective observation, abstract conceptualization, and active experimentation. They were flexible depending on the police personnel's specific cybercrime preparedness, training, and experiential learning.

Due to the vast array of segments, I incorporated several similar terms to evoke coordinated collaboration. I utilized the term "strategic themes" to explain and encompass the similar concepts of the codes, categories, patterns, and segments. Workable segments emerged with the identified components that emanated into strategic themes. They extended from the contextual contents of the data inquiries. They were not exact; however, they were in close proximity. There were mutual relationships aligned into a collaborative comparative analysis. The documented comments and responses by the police personnel were brought into an agreement and aligned as analogies. There were several components that were tantamount to corresponding similar identities. They illustrated Kolb's (1984) experiential learning theory (ELT) and the current research data.

Table 4 entitled the strategic themes by police personnel and cybercrime preparedness aligned the themes. It illustrated the indicated number of law enforcement personnel articulating the experiential learning theory of Kolb and its' four scientific processes.

Table 4

Strategic Themes by Police Personnel and Cybercrime Preparedness

Themes	Number [N=8]	Process
Strategic Themes-Cybercrime Preparedness Law Enforcement Personnel	**Police Personnel**	**Kolb's Comparative Analysis Data Inquiry Questions**
1. Concrete Living (Real-Actual World) Foundation of the cybercrime preparedness/Problem-oriented	8	**Concrete Experience (CE)**
2. Retrospective Reflection (Looking back on learning)/Introspection	7	**Reflective Observation (RO}**
3. Authenticity-Credible & Reliable (In-depth Expanded Learning)	8	**Reflective Observation/Abstract Conceptualization (RO/AC)**
4. **Abstract Thinking and Conceptualizing** Building on the Foundation by Reflecting	7	**Abstract Conceptualization (AC)**
5. **Inquisition-Inquiry Oriented** *Meaningful*-(At the beginning it did not seem important. I understood it as time passed.) *Relevant*-(consistent/pertinent). *Interesting*-(It was somewhat pleasurable . . . not exciting until . . . investigating cybercrime and attacks)	8	**Abstract Conceptualization (AC)**
6. **Collaboration & Experimentation-Experiential** Investigation; Integrated thinking and applying the "taught and caught" cybercrime preparedness.	8	**Active Experimentation (AE)**
7. **Pragmatic–Practical Application/Applied** Expanded - Learning Problem Solving /Decision Making-Invention -Creative Thoughts, Innovation with Critical thinking	8	**Active Experimentation (AE) Reassessing the basic Concrete Experience (CE)**

The strategic themes of the research study extended and were an extrapolation of the data analyses classified by the participant's responses. The strategic themes were also incorporated as scientific approaches with procedures in the principles, knowledge, and understanding. Workable organization skills and practical applications were employed. The strategic themes encompassed skilled management, planning, and the scientific approach. It further explained the experiential learning of the law enforcement personnel,

cybercrime preparedness and training gathered from the data inquiries. The matrix entailed the collaborative coordination of codes, themes, categories, and patterns that evolved into strategic themes. These were then aligned in a cyclic fashion. The cybercrime preparedness, ideas, and thoughts promulgated an array of strategic themes. Experiential learning was employed as a comparative analysis moving from the theoretical to the pragmatic. The theory was a speculative plan formulated from the data inquiry codes, categories, patterns, and segments, and then emerged into strategic themes. The pragmatic components were techniques that were applied and incorporated into the police personnel's real world of critical thinking.

The seven key strategic themes emerged and were summarized in connection with the phenomenon as challenges of intentionality. The challenge of intentionality emanated achieved an understanding of the purpose of conveying the content of perspectives. The **s**trategic themes flowed from the police personnel's prior cybercrime preparedness contained in Kolb's (2014) foundation employing the seven sequential procedures.

- Concrete Living (Real World) -what do I know & what is needed (individual)?
- Retrospective Reflection-Looking back-what do I need to learn (conceptual)?
- Authenticity-Credible/Reliable - how well do I need to understand (relational)?
- Abstract Conceptualization-how much do I need to know (conceptual)?
- Inquisition Inquiry/Relevant-how will I understand and enhance it (relational)?
- Collaboration and Experimentation-how can I further apply it (developmental)?
- Pragmatic–Problem Solving/Decisions-how can I use/apply it (developmental)?

The experiential learning expressed by Kolb (2014) was built on concrete living as the principle with the emphatic way of learning, enhanced by experience. It was formulated and utilized as a foundational component to answer the three research questions established and aligned into the 10 data inquiry instrument. The compiled data inquiries were analytically processed via the Modified step-by-step process of van Kaam (1966) that developed into the seven strategic themes with inductive inquiries. Kolb's (1984) four basic words were incorporated resulting in codes, categories, patterns, and segments. They were aligned and then affirmed the quality of the strategic themes.

Strategic Themes

The strategic themes were analytically viewed, investigated, and examined. I remained neutral and unbiased as the instrument of the study. I eliminated any preconceived notions I had concerning police personnel and the cybercrime preparedness phenomenon. I discerned essential consciousness features (Noema) and eradicated any beliefs regarding the experiences (Noesis) that I might entertain. I integrated the essences and meanings of the experiences. Epoche was the first essential process of eliminating any biases, preconceived notions, or assumptions that I had regarding the police personnel and the phenomenon under study. After the epoche, the phenomenological reduction was employed. I "bracketed out" and held up the phenomenon for in-depth inspection-examined, analyzed, and dissected it. Bracketing required identifying any personal experiences related to the cybercrime phenomenon. It was encapsulated and interpreted into the meanings of the words, terms, and phrases obtained from the police

personnel's interpretations. I further examined the data inquiry meanings by contacting two participants who concurred concerning the inductive inquiry explanations.

The data inquiries were aligned as strategic themes critically assessed by van Kaam's (1966) comprehensive Modified data analyses. The application of the seven indispensable requisites was required. Van Kaam asserted that an experiential design imposed on participants might distort the full meanings and richness of human behavior. The procedure elucidated the underlying structure of the participants' experiences interpreting the original phenomena in which the experience occurred. Each step was critically analyzed from the transcribed data collection inquiry of each participant using van Kaam's extensive step-by-step design (Moustakas, 1994, p. 120-121). Van Kaam's data analyses were assessed requiring each step to acclimate in sequential order.

1. List every expression that is relevant to the experience, which is horizonalization.
2. Determine the invariant constituents through reduction and elimination and then test each expression for two requirements.
3. Cluster and position the invariant constituents of related experiences into themes.
4. Check and finalize the identification of the invariant constituents and themes by application referred to as validation.
5. Utilize relevant validated invariant constituents and themes to construct an Individual Textual Description of the experience; this includes all verbatim statements from interviewees.
6. Construct Individual Structural Descriptions of the experiences.

7. Align and construct for each research participant a Textual-Structural Description of the meanings and essences of the experiences of the phenomenon [cybercrime preparedness and training].

It was necessary to employ and ensure all invariant constituents and themes were appropriately utilized and in sequential order. The Individual Textual-Structural Description developed into the Composite Descriptions of the meanings with essentials representing the personnel that resulted in the inductive inquiry analyses.

Inductive Inquiry Analyses

Multiple themes evolved from the data inquiries that were critically assessed and analyzed employing van Kaam's (1966) data analyses. Deep consideration was required in the examination and investigation to perform the in-depth comparative analysis. The results were in the inductive inquiry analyses design integrated with Kolb's (1984) experiential learning. The inductive inquiry analyses listed and aligned the functional-operational design inclusive of the eight procedures and processes. The eight consisted of a plan to organize, comprehend, apply, analyze, synthesize, evaluate, and apply synergism. The Inductive Inquiry Analyses Design and Learning Experiences were articulated by the police personnel. The proximity was aligned with Kolb's ELT and the responses in the data analysis collected from the participants in the research. Table 5 described the inductive inquiry analyses design. It encapsulated a wide range of evolving cybercrime comprehension and learning experiences with critical composite data. It began with a plan and ended with the final component of synergism. The culmination of synergism reinforced the fact that the sum is greater than the individual parts.

Table 5

Inductive Inquiry Analyses Design

PLAN-Architecture, Sc Design, Foundation, Concrete Workable Real-World Analogy-Goals, Objectives, Forecasting, Knowledge (CE)

ORGANIZE-Style, Establish, Align Orderly Structure-Personnel (Coach, Inspire, Regulate), Methods, Money, Machinery, Material CE)

COMPREHEND-Retrospective Reflections, Abstract Thinking, Introspection, Understanding, w/Experiential Learning (RO/AC)

APPLICATION-Authentic Practicality, Experiment, Employ, Diligent Effort, Relevant, Sc Engineering, Conceptualization (RO/AC)

ANALYZE-Investigate, Inquisitions, Examination Patterns, Discover Hidden Meanings, Good Judgment, Analytical Strategies (RO/AC)

SYNTHESIS-Collaboration, Compound Combination, Formulate Values, Integrating Elements, Combining Design and Predict (AC/AE)

EVALUATE-Assess, Estimate Value, Judge Worth, Comp Analysis, Problem Solving & Decision Making, Verify, Invent (RO/AC/AE)

SYNERGISM-Interaction of Things, Advanced Critical Thinking, Innovation, Great Effect than Sum,/Evidence-Based (RO/AC/AE/CE)

The inductive inquiry analyses were collected from the police personnel's data inquiries. It produced a detailed alignment articulated as an inductive inquiry analyses design. The alignment was constructed as a non-judgmental, empathic, and creative synthesis rendering significant evidence, data, and transferable components. The details evoked concepts, codes, and categories that assisted in guiding principles with creative evidence to form a synergistic whole. The synthesis promulgated categories into patterns and segments as the inductive inquiry analyses emerged into strategic themes. The inductive inquiry analyses were built on the system of the personnel's detailed comments written in the cybercrime inquiry instrument. I examined the data inquiry transcripts to ensure accuracy. Two police persons were contacted to ensure the veracity of inductive

inquiry analyses with the agreed-upon congruence. It was essential to examine and re-read thoroughly. The inductive inquiry analyses focused first on police-cybercrime preparedness and what were the most significant components or elements to know. Second, what designs were necessary to gather data (Maxwell, 2013; Patton, 2002)?

Emergent Inductive Inquiry Analyses and Research

The inductive inquiry analyses emerged with the collected data providing rich information from the police personnel. It gathered their preparedness, training, experiential learning, and applications. Learning is never passive and dependent upon what we know from prior experiences (Martin, 2015). It involved previous knowledge, skills, and cognitive abilities, just to name a few. The data produced workable and transferable information. There were learning approaches, distinctions, and styles that can assist others in diverse scholarly learning and training. The inductive inquiry analyses were designed from the evolving responses derived from emerging detailed patterns.

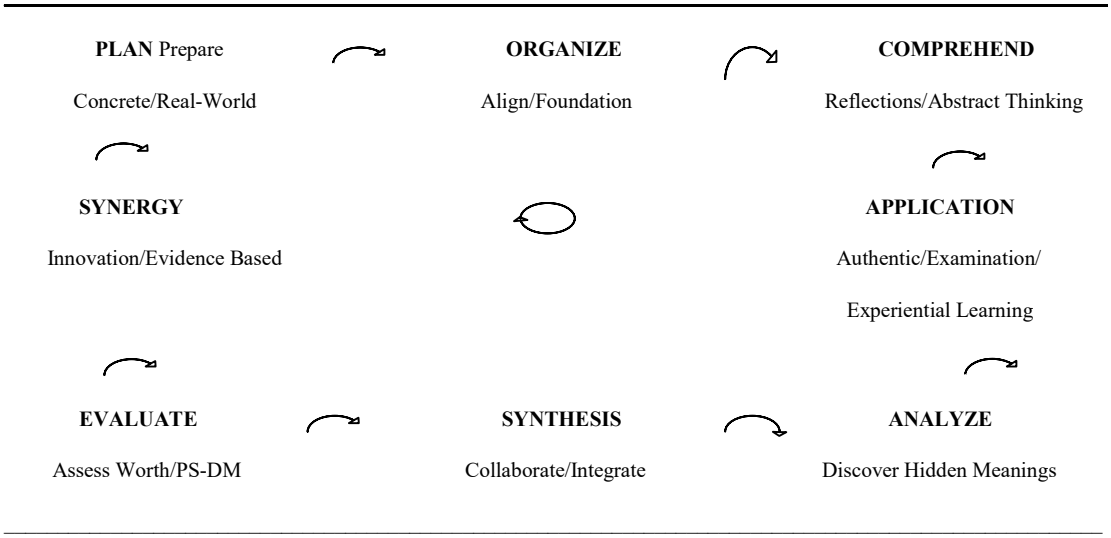
Most inductive research studies often express a paradigm between three to eight categories (Patton, 2002). The informal semi-structured inquiries collected open-ended (not rigidly structured) data. The aligned fluidity allowed the 10 inquiries to be answered in a flexible manner. The explanations provided understanding in developing and producing rich cybercrime data. The data collection inquiries were logical and systematic. They provided opportunities for law enforcement personnel to express themselves without a documented time slot or any interference. The data collection was pliant with the participants' ideas and thoughts expressed in the data collection. The inductive reasoning and analyses moved from the specific to the general. The progression

was from the police personnel's cybercrime preparedness reflections to the discovery of a systematic design with strategic themes. The alignment represented a degree of orchestrated organizational order. The results of the analytical inductive development emerged with a thematic structure. The orderly procedures focused on the processes and methods. The inductive analyses involved locating and discovering the categories, patterns, and themes from the data (Patton, 2002, p. 453). The findings in the inductive analyses evolved from the generated qualitative data. Whereas, deductive analysis is in accordance with an existing framework applied in quantitative research. The analytical inductive development from the study can be utilized as a foundation for future research.

Multiple strategic themes arose from the data analyses of van Kaam (1966) produced by the inductive inquiry analyses. Figure 8 entitled the *Cyclic Police Personnel Cybercrime Learning & Preparedness Process* exhibits examples of the data results collected from the cybercrime instruments.

Figure 8

Cyclic Police Personnel Cybercrime Preparedness Process



The inductive inquiry analysis produced eight categories that were designed in a cycle-like process. An efficient way was provided to analyze the data and procreate a design for future research. Huberman (1994) asserted that the pre-structuring methods tend to reduce the amount of data and simplify the data analysis (p. 16). The design allowed the inductive development to gather perspectives and values from the police personnel. The cyclic sequence consisted of eight entities beginning as a plan and concluding with synergy. The progressive circle can be applied in an evidence-based system. It originated as a plan and resulted in a foundation. The organized plan was comprehended via reflections. The application became a reality as it was analyzed. The synthesis emanated through collaboration with the assessment. The evaluated evolved arriving at synergy. The whole is greater than the parts for enhanced cybercrime preparedness. The suggestions in the cyclic process aligned a progressive movement with precision. The process can be repeated as a recaptured extended double-cyclic circle.

The Cyclic Process

The cyclic process of police personnel's cybercrime learning, and preparedness revealed pragmatic strategies in the information processing as the data was encoded, stored, and retrieved. The process design initially began with a plan and culminated in synergy. The focus was on prior cybercrime preparedness with proactive measures. It presented a workable plan in the real world, organized with principles that worked to comprehend the collected data. The police personnel emanated abstract thinking as they applied and examined the prior cybercrime preparedness. The approach ended in cyclic learning experiences. It encompassed the investigation of scientific conceptualization.

The analyzed process procreated the proclivity of inquisitions of codes, categories, and patterns with hidden meanings. It was synthesized by employing the integrated cybercrime investigation evaluated by assessing the value of problem-solving and decision-making. The pinnacle of synergy was an innovative coordinated collaboration. It resulted in the whole being greater than the parts. The results produced the culmination of data analyzed by the step-by-step process of van Kaam's (1966) Modified data analyses.

Modified Data Analyses of van Kaam

The application of van Kaam's (1966) data analyses assessed and evaluated the details concerning the police personnel's prior cybercrime preparedness. It reflected perceptive thoughts with ethical credence and integrity. The Modified van Kaam's (1966) process of data analyses elucidated and revealed the emic focus. It shared the police personnel's collected data inquiry responses. The relations and interactive segments provided clarity with understanding. The analytical assessment of each participant emitted transcribed data. Police personnel described the perspectives during cybercrime preparedness with experiential learning, and pragmatic applications in the workplace, community, and educational facilities. They expressed projected strategies and techniques to combat, mitigate, and uproot cybercrime bringing positive social change. Patton (2002) argued ways to inductively analyze qualitative data inquiries. (1) Identify and describe the meanings, (2) Clarify and explain the participants' focus. (3) Recognize categories or patterns not specifically labeled. (4) Develop terms to articulate and describe the inductively by generated categories. The outcome addressed and filled the literary gap between police personnel and cybercrime preparedness.

Addressing the Literary Gap

The police personnel and prior cybercrime preparedness assisted in closing a gap in the literary research. The study addressed the police personnel as a group (not only patrol officers) and identified police personnel's prior cybercrime preparedness with experiential learning. The focus was on the diversity of learning styles and pragmatic applications in the agencies and communities. Rich techniques emanated from preventive skills to combat cybercrime, cyber-attacks, and cyber-terrorism. Each participant's data inquiry was analytically assessed utilizing van Kaam's (1966) extensive data analyses. The research data and key components were orchestrated and evaluated after collecting the inquiries electronically by virtual-remote devices. The results ascribed in-depth perceptual data from the police personnel rendering rich pertinent information and demographics.

Demographic Results

The research demographics consisted of many important components. The police personnel volunteers stipulated the mandated required credentials. The criteria were eighteen or older; current employee, contractual individual, or volunteer for a police agency; had prior cybercrime preparedness or training (via an Instructor, Trainer, Google, Video, DVD, CD, ZOOM, YouTube, Internet, Experience, or Self-taught); and had the opportunity to utilize the cybercrime skills at the agencies and in communities. Documented in Figure 9 is the general compiled data entitled *Demographics of Police Personnel Positions and Job Title.* The percentages were collected from the police personnel's positions, the number of participants, educational degrees, and titles.

Figure 9

Demographics of Police Personnel Positions and Job Titles

Positions [N=8}	Number of Participants/Education		Job Titles	Percentage
Sworn Officer	1	AAS	1 Captain	12.5%
Sworn Officer	1	MBA	1 Lieutenant	12.5%
Sworn Officer	1	PhD Candidate	1 Sergeant Investigator	12.5%
Sworn Officer	1	CJS-MA	1 Sergeant	12.5%
Law Enforcement	1	AA	1 Officer-'Reserve'	12.5%
Police Civilian	1	BA	1 City	12.5%
Police Assistant	1	MCS	1 Patrol Officer	12.5%
Police Volunteer	1	BS/MA/EdS	1 College Intern	12.5%

Due to the agreed-upon confidentiality and anonymity, I could not list all of the specific demographics provided by the police personnel. I abided by the ethically secured confidentiality and anonymity agreement. The law enforcement agencies and police personnel were assured there would be no identifiable demographic leakage. The demographics consisted of varied positions, job titles, and data inquiry percentages. The police personnel (N=8) consisted of one captain, one lieutenant, two sergeants, one officer, one civilian, one police assistant patrol officer, and one volunteer police college intern. The demographics were diverse emerging from the participant's data in the evidence of integrity and trustworthiness. Multiple segments of the identifiable demographic were not revealed to ensure privacy, confidentiality, and anonymity. All agencies and participants have assured the evidence of trustworthiness.

Evidence of Trustworthiness

The empirical phenomenological qualitative research included evidence of trustworthiness. It examined and investigated the lived experiences of the police personnel's cybercrime preparedness with experiential learning and pragmatically applied

achievements. Patton (2002) asserted that trustworthiness entails honesty with authenticity and confident expectations. It further includes factual qualitative rigor and genuine systematic truth with quality and fairness. The participants provided a wealth of knowledge filling the literature gap. The engaged experiential learning provided enhanced cybercrime preparedness, as well as strategies to mitigate the cybercrime phenomenon with evidence of trustworthiness. The 10 data inquiries were designed as the "first-time utilization" to answer the three research questions. The items were critically assessed and evaluated by three college friends and associates of the researcher. Two were college professors and one was a professional university research dean. The high-quality empirical qualitative data was greatly valued in the evidence of trustworthiness. The prior preparedness balanced perspectives of evidential learning in the phenomenon.

The trustworthiness evidenced the depiction of core concepts in the real world with authenticity, concreteness, and reliability of the police personnel and cybercrime preparedness. The scholarly perspectives of the law enforcement personnel evoked rich data with evidence of trustworthiness judging the integrity of the qualitative research. The focus was on the police personnel's preparedness to handle the ever-increasing cybercrime with proactive truth, honesty, and credibility.

Moustakas (1994) emphasized the four core concepts, which are conscious acts, perceptions, intentional experience, and inter-subjective validity. These were the primary sources of the data inquiry collections utilizing real-world knowledge for the systematically structured empirical qualitative phenomenological research. I returned to the collected data multiple times to ensure the integrity of the codes, categories, patterns,

segments, and strategic themes. I wanted to reaffirm that I was not biased and utilized systematic accuracy with integrity and trustworthiness.

Trustworthiness as a Science and an Art

Husserl's (1965, p. 45) phenomenology afforded knowledge as a science that was logical in the affirmation that the only thing, we know for certain is that which appears before us in consciousness. The study captured the direct quotations as the source of raw data from the participants' data inquiries, rather than the interpretations of experiences often formulated by a researcher (Patton, 2002). Trustworthiness as a science entails the systematic study of the knowledge derived from the research integrity, principles, and methods. Trustworthiness is an art that involves human creativity and reliable pragmatic applications of the study. The captured data inquiries provided opportunities to analytically assess and evaluate the perceptions of the police personnel's cybercrime preparedness. Ethical trustworthiness and integrity were critical components in the three research questions that were developed into 10 data inquiries. They were analyzed by van Kaam's (1966) data analyses encompassing the experiential learning theory.

Research Questions and Data Inquiry Results

The three research questions in the empirical phenomenological qualitative study were answered by law enforcement personnel. The data inquiries were developed and orchestrated to collect the participant's prior cybercrime preparedness. The data expressed the submitted thoughts and perceptions. Figure 10 entitled *Research Questions and Ten Data Collection Inquiries* explained how the three research questions were analytically divided into 10 data inquiries to capture the essence of the research study.

Figure 10

Research Questions and Ten Data Inquiries

Q1. What are the law enforcement personnel's perceptions, lived experiences, thoughts, and ideas regarding the prior cybercrime preparedness, training, and experiential learning, and in what ways was it meaningful, relevant, and interesting?

a.. What are your perceptions and thoughts regarding your previous cybercrime training and preparedness?

b. In what ways was the cybercrime training and preparation meaningful, relevant, and interesting?

c. How did other cyber-training experiences assist you in the cybercrime law enforcement learning?

Q2. Where did the law enforcement personnel acquire the prior cybercrime preparedness, training, and experiential learning and how was the cybercrime preparedness training applied in a pragmatic manner in the law enforcement workplace?

d.. What geographical location or site did you receive your prior cybercrime training and preparedness?

e.. How did you apply your cybercrime preparedness and learning in a practical manner at the workplace?

f. List several ways you believe the evolving cybercrime training and preparedness could be enhanced?

Q3. In what ways have cybercrime professionals applied cybercrime preparedness and list workable recommendations to combat, mitigate, and uproot cybercrime?

g.. In what ways have you applied the cybercrime training, learning, and preparedness in positive ways?

h. What are your recommendations to equip police, combat (fight), and mitigate (reduce) cybercrime?

i..What methods and/or strategies do you believe can assist in uprooting (eliminating) cyber-attacks, cybercrime, and cyber terrorism?

The final compiled inquiry collected any additional enriched cybercrime data.

j.. List any other Cybercrime Law Enforcement Preparedness and Training Procedures you believe will help to fight, reduce, and eliminate cybercrime, cyber-attacks, and cyber terrorism?

The three research questions were analytically developed into 10 data inquiries to secure the qualitative phenomenological research answers. The aligned step-by-step process answered the three research questions. Figure 10 aligned the process to ensure the three research questions were adequately answered. The personnel had sufficient time to experience their inner thoughts and perspicacity as they answered the data inquiries.

Rich suggestions and recommendations emanated from the inquiries to enhance cybercrime preparedness, as well as measures to combat and eliminate cyber-attacks and cyber-terrorism. The three research questions were answered utilizing the systematically designed data inquiry instrument. The data collected the law enforcement personnel's experiences with insight addressing the prior cybercrime preparedness and pragmatic applications. The methods of abstract and logical thinking allowed the police personnel's reflections and orchestrate the alignment of inductive reasoning.

The full constructs of cybercrime preparedness and experiential learning evidenced descriptive thoughts to radiate the overwhelming comprehensive-textual data responses. The qualitative approach combined with experiential learning provided police personnel to establish scholarly coherent systematic data. The data collected procreated the participants' comprehensive detailed problem-solving and decision-making comments, whereas the rich information resulted in workable outcomes and proverbial conclusions. Additional explanations are located in the narrative.

The three research core questions were articulated in clear concise terms that remained viable throughout the human science research. The inquisitions collected the five listed phenomenological characteristics of Moustakas (1994, p.105) that (1) revealed the full essence and meaning of the human experiences; (2) uncovered the qualitative experiences rather than the quantitative; (3) engaged the total-self of the participants' sustaining personal and passionate involvement; (4) did not predict or determine causal relationships; and (5) was illuminated with intensity throughout the comprehensive

cybercrime preparedness rendering real-world experiences. The 10 analytical data inquiries presented responses with great results and resolutions.

Data Inquiry 1

Q.1. What are your perceptions and thoughts regarding your previous cybercrime training and preparedness? Seven of the eight respondents (87.5%) emphasized positive statements that they enjoyed, were encouraged, comfortable, well-pleased, and felt quite confident. The one adverse participant (12.5%) affirmed, “I did not understand cybercrime enough to grasp much of the material.” Two of the positive verbatim statements articulated: “It was good and I was trained by an expert on the Department with Q & A time.” “I always had a love for anything dealing with computers.” One participant made two mediocre statements articulated accordingly. “It was not pleasurable or interesting because I am not good on computers; however it was exciting when I began investigating the actual cybercrimes and attacks.” “At the beginning, it did not seem important. I then begin to understand it as time passed.”

There was extensive feedback from the data inquiries explaining the learning process and appreciation as the cybercrime procedures were explained. One verbatim explanation expressed “The cybercrime training provided an excellent foundation for creative investigation measures with practical knowledge.” The constructive thoughts, ideas, and perceptions were further clarified in the narrative. Two persons (25%) expressed unique learning styles and techniques during the cybercrime investigation preparedness; however, the styles and techniques were not specifically clarified.

Seventy-five percent (75%) of the law enforcement personnel expressed (although, not clearly explained), that they enjoyed the prior cybercrime training, and it was something they wanted to learn. The data inquiry responses described the multiple opportunities that were presented in learning the innovative technological cyber-components and the vast array of cybercrime anonymity. Three (37.5%) police personnel discussed the perceptions of prior and current cybercrime preparedness that focused on goals, objectives, and architectural real-world training with the design. Additional written comments expressed data that tended to prepare the participants for further cybercrime training. Three components were quite prevalent and assisted in the learning process that consisted of the following: (1) expressions of orderly planning, (2) structured organization of new cybercrime preparedness material, and (3) forecasting of things to come. The police personnel described the diligence of the trainers and facilitators with positive comments in their coaching, encouraging remarks, and employing practical real-world examples during the initial cybercrime preparedness training. It tended to establish greater learning, comprehension, and understanding.

The knowledge and learning styles evoked comments predicting the approximate projected cost of the personnel, training, computers, and software. The police personnel addressed their thoughts of preparedness aligned with their own beliefs regarding systematic cyber-principles and training methods. The specific set of data was evident in the existing knowledge and skills of the police personnel's prior cognition of cybercrime preparedness, training, and learning. The cybercrime preparedness yielded the solid (concrete) foundation, suggested in retrospectively reflecting, examining, and

discovering the hidden meanings in critical thinking and authentic practicality.

Data Inquiry 2

Q.2. In what ways was the cybercrime training and preparation meaningful, relevant, and interesting? There were diverse answers with six (75%) expressing productive comments to the inquiry. One positive verbatim statement affirmed, “I had a class taught by the FBI agent that stirred my thoughts and interest in cybercrime (identity theft), cyber-attacks, and cyber-terrorism.” The one comment (12.5%) expressed mediocrity, “I was not experienced in computers and it was new to me. I know it was organized well, but it took awhile to comprehend and understand.” The one adverse participant (12.5%) stated “it was too much too soon and I was just learning to understand computers.”

The described ways were meaningful, relevant, and interesting emphasizing prior cybercrime preparedness that was diverse, uniquely aligned, organized, and semi-structured with various cybercrime training strategies. It had a wide range of step-by-step procedures and processes, whether taught by a tutor, instructor, coach, Internet, iPod, or self-taught. Participants tended to focus on proactive measures regarding cyber-attacks with problem-solving and decision-making policies and procedures. One (12.5%) person expressed “The training was meaningful and provided a constructive way to investigate and analyze cybercrime.” The meaningful learning and training components provided identity theft and cyber-terrorism dimensions with emphasis on the need for further detailed investigative tools. Expressions are inferred by analyzing and discovering hidden meanings in weak passwords and evidence-based encrypted synthesis. Words articulated cybercrime comprehension and real-world concrete reflections with abstract thinking

and understanding. The police personnel expressed relevant and interesting cybercrime material that allowed them to interact and share preventive cyber-terrorism with others.

It was quite obvious that many participants were professional and well-read in cybercrime. The synergistic cybercrime applications evoked high-tech intelligence that was incredible and reliable (authentic) training information. One participant (12.5%) found cybercrime training and preparedness quite interesting; explaining that comprehensive cyber-attacks and cyber-terrorism work to embrace high-tech tools in cyberspace. One police personnel (12.5%) expressed that "innovative opportunities for the prevention of cyber-attacks served as a part of the target attacks of 911; and it now serves to be instrumental in the damage to pipelines, dams, electric grids, aviation, law enforcement, airlines, air-traffic, and other critical systems." The data feedback alluded to "vulnerable cyber-attacks that could alter the pressure on gas lines, might change the nutrients in the cereal plants, and de-value other critical controlled computer systems." The cybercrime preparedness inquiry responses evoked multiple meaningful and interesting needs in working effectively with the new computer-integrated systems. One individual (12.5%) emitted, "The training was interesting and established creative skills to design, plan, examine and understand hidden agendas behind cybercrime." Comments evoked a variety of high-technical architectural designs, scientific methods, machinery, and material necessary to prevent future cybercrime devastation. I, as the instrument of the study, learned a great amount concerning cybercrime techniques while reading and analyzing the data inquiry responses. The majority of the eight participants had a storehouse of cybercrime credentials, cyber engineering, and knowledge.

Data Inquiry 3

Q.3. How did other cyber training experiences assist you in the cybercrime law enforcement learning? This question resulted in tremendous data. It stirred seven participants (87.5%) contributing multiple factors to the inductive analysis that emanated a great number of inquiry responses. It provided rich cyber training with organized statements. Personnel expressed the contents of the patterns, themes, and principles with creative encrypted synthesis. Verbatim statements were expressed in real-world learning components, such as "Other cyber-training experiences assisted me tremendously" and "The cyber training made it interesting from my previous computer training." Apparently, other segments of cyber training experiences provided a foundation for the experimentation and the acknowledgment of certain patterns and themes in cybercrime preparedness. It could have been a strength or weakness depending upon what challenges and events transpired in the first cyber-training (Martin, 2015).

There were emerging flexible convenient strategic themes, such as the goals, objectives, designs, and plans that tended to tell a story of cyber training experiences that assisted in learning objectives with rich descriptive qualitative data. It detailed the process of understanding with encouragement via coaching, training, and instruction. It further enhanced the methods regarding computers, technology, cyber-material, and comprehension that activated many retrospective reflections and abstract thinking. The other cyber training experiences assisted and provided a foundation with the principles of cybercrime scientific thought-provoking processing. Diverse and unique learning ideas, strategies, and cybercrime conceptualization of cyber training played major roles.

The cybercrime delivery further perpetuated locating the proper learning patterns. Discovering the innovative meanings to address the personal experiences was oriented toward the new innovative cybercrime training. Prior computer training stimulated good judgment intertwined with integrative and coordinated cyber-activities. The real-world expressions established a vision with beliefs and values to think, receive, act, do, and improve. The philosophy aligned the underlying thoughts and conduct in the prediction of the workable cybercrime problem-solving and decision-making tactics.

The collaboration of cyber-training experiences procreated critical thinking and innovation. The experiences assisted in shaping a paradigm to assist in experiential learning. Lushbaugh & Weston (2016) affirmed that the reality in the advancement of silicone technology along with the Internet further established three systematic aspects: all computers are virtually interconnected; individuals have become more computer literate; the security threat is now a global open advantage with cybercriminals.

Data Inquiry 4

Q.4. What geographical locations or sites did you receive your prior cybercrime training and preparedness? The prior cybercrime geographical locations, training, and preparedness were limited. Eight police personnel (100%) affirmed they received the initial cybercrime preparedness and training in the state of Michigan, whether instructor-led or self-taught. However, three (37.5%) police personnel experienced additional training outside the state in Ohio, New York, Georgia, Illinois, and California. The four verbatim responses addressed the geographical cybercrime preparedness locations:

"I learned on the college campus in Lansing."

"I learned with a cyber-terrorism training expert in the Police Academy."

"My bedroom was the geographic cybercrime/identity theft learning site."

"I was further trained in Ohio at a CA/CT workshop that was very good."

The conjectures of the geographical cybercrime preparedness locations were not specific. It was not known if the written out-of-state sites inferred were indicative of virtual-remote or physical locations. In essence, it was not clear if the listed secondary cybercrime preparedness training sites were actual physical brick-and-mortar locales or Internet student-centered teaching and learning. The locations that the police personnel cited extended from the preparedness consisting of class sessions, self-taught, interactive e-books, flashcards, and quizzing. The virtual-reality training was engaged in cyber-simulations with the temporal-spatial continuity presented on the Internet.

Data Inquiry 5

Q.5. How did you apply your cybercrime preparedness and learning in a practical manner at the workplace or in the community? Seven of the eight participants (87.5%) postulated how they applied their cybercrime training in the workplace, as well as in communities and educational facilities. Only one (12.5%) did not apply the cybercrime preparedness training and learning right away, except for assisting in writing one credit card identity theft report prior to the law enforcement departmental transfer two days later. Listed are 15 verbatim statements concerning the applied cybercrime preparedness in the workplaces, as well as training in the communities (Martin, 2021).

"I worked and trained several cybercrime (identity theft) experimentations."

"I wrote some reports and trained other police personnel."

"I now teach ID theft in the agency and at other educational facilities."

"I trained others in how to gather cybercrime evidence for investigation."

"I built upon the basic cybercrime ID-fraud-theft and taught others."

"I have worked as a team member on several cyber-terrorism projects."

"I expanded upon cybercrimes and cyber-attacks training & taught others."

"I have designed and presented many cybercrime oral presentations."

"I shared cybercrime and cyber-attacks investigations for the agency."

"I taught cybercrime Identity-theft in my unit and several college workshops."

"I worked on a cybercrime, cyber-terrorism and cyber-attack seminar."

"I now teach full cybercrime workshops with simulations in colleges."

"I wrote several preventive cybercrime articles and excerpts for my unit."

"I encouraged three other detectives to become a part of training cyber-attacks."

"I used the training for cyber-attack investigation purposes in the department."

Many police personnel (87.5%) indicated that cybercrime preparedness training and learning were utilized in practical ways, inside and outside of the workplace.

Lyman (2016) asserted that it is imperative that police personnel understand and share training information and resources with the communities, educational facilities, and local, state, and federal to coordinate strong collaborative communications as an integral part among agencies. Several law enforcement personnel asserted they shared the pros and cons of proactive cybercrime measures on iPods, and YouTube with engagement tracking, and other media delivery systems for educational high schools, colleges, neighborhood block clubs, churches, and community police gatherings.

Data Inquiry 6

Q.6. Can you list several ways you believe the evolving cybercrime training and preparedness could be enhanced? Eight of the eight participants (100%) provided valuable ways and techniques to efficiently impart positive cybercrime preparedness training. The police personnel listed many techniques to enhance (heighten and increase) the development of preparedness. There were ways to assist students, such as distributing a list of common cybercrime terms at the beginning of class to better prepare for training. Seven (87.5%) police personnel indicated the importance of receiving handout cybercrime training material to refresh and reflect upon after the classes. Six participants (75%) emphasized that sworn patrol officers have enough on their plates without adding additional weights of cybercrime and cyber security. Five (62.5%) personnel explained that trainers or coaches should check for understanding before progressing to the next session. Four (50%) participants expressed those trainers should allow class time opportunities to practice and retain the cybercrime knowledge and skills.

Three (37.5%) police personnel cited the need to stop a moment during the class to absorb the information, especially when explaining innovative techniques and tactics mitigating cyber-attacks and cyber-terrorism. Two (25%) police personnel asserted the need to utilize civilians, college professors, detectives, cyber security trainers, or FBI instructors for training who directly engage in cybercrime forensic work and computer crime investigations. One (12.5%) individual emphasized “It is important to coordinate the use of websites, Instagrams, and DVDs with the availed opportunities to replay the

freshly learned cyber crime information." One (12.5%) person promulgated the need to ensure the instructor has a sincere passion for teaching cybercrime and is not a novice in the field. "The cybercrime facilitator/instructor should have expert cyber-skills and possess background excellence working for a while in the field of cybercrime." Listed are ten additional written verbatim statements collected from law enforcement personnel to efficiently enhance and enlighten cybercrime preparedness and professional training.

"Set up small cybercrime units in police departments to handle the increase."

"Encourage civilian personnel to work at cybercrime and become self taught."

"Send civilians to cyber-attack and cyber-terrorism training with cyber-experts."

"Work in groups doing cybercrime tasks for others to become more successful."

"Use strategies to strengthen and deepen the cybercrime comprehension."

"Compile a list of cybercrime IPODS and simulations for hands-on training."

"Identify websites with information to strengthen cybercrime training."

"Instructors should have patience due to the enigma in learning cybercrime."

"Professional skilled trainers are essential for cybercrime training."

"Sensitivity is mandatory for cybercrime instructors due to the great amount of new material provided and the need to apply comprehensible applications."

Additional techniques and strategies were presented to enhance cybercrime training preparedness. Police personnel emphasized the importance of allowing time for question and answer (Q & A) opportunities during the cybercrime learning process to provide greater clarity and understanding.

Further expressions emitted the need to encourage cybercrime training with prototype critical thinking, cyber-examinations, and investigation training. Expediently select skilled cybercrime and cyber-attacks peer-trainers with the excellence of cybercrime knowledge. Ensure all police personnel has had a prior introduction to computer training before entering the cybercrime classes. Employ facilitators with exceptional hands-on cybercrime abilities to impart clear, concise, and user-friendly instructions for classroom learners. Strengthen cybercrime knowledge-based classroom participation. Make sure police personnel understand the basic eight Index Crimes [forcible rape, robbery, arson, murder, burglary, larceny, aggravated assault, and auto theft] before the cybercrime preparedness training. Enhance the cybercrime trainer facilitators' role in the management of experiential learning. Identify Train the Trainer individuals to engage in learner-driven techniques. Ensure the instructor-trainer possesses excellent professional hands-on cybercrime abilities and not mediocre cyber-skill sets.

Effectively utilize seasoned detectives and investigators who work daily with cybercrime and can provide cybercrime case history investigation techniques with illustrated examples. Encourage cybercrime trainer facilitators to prepare cyber-interactive videos and iPods that can assist in structured student-tested training. Three-quarters (75%) of the participants cited the need for a chart, list, worksheet, or semi-structured pamphlet with cybercrime websites, references, or recommended links. The distributed hand-outs will strengthen and increase the learning process. In addition, two participants (25%) encouraged the need for teamwork during preparedness to stimulate the proclivity of the learners to share their newfound cybercrime information.

Data Inquiry 7

Q.7. In what ways have participants applied the cybercrime training, learning, and preparedness in positive ways? Amazingly, seven participants (87.5%) affirmed they immediately utilized cybercrime on-the-job and trained others on-site in high schools, colleges, neighborhood block clubs, organizations, synagogues, churches, and local businesses. The personnel was great at using their skills, knowledge, and abilities from the diverse cybercrime training. Many police personnel enlarged their cybercrime preparedness skills exponentially. The small study (N=8) provided much food for thought and strengthened the need for additional research. Three police personnel (37.5%) cited cybercrime skills with the following verbatim statements: "I am now a civilian cybercrime trainer, coach, and consultant for several police agencies, community sites, and colleges." "I have set-up and presented 15 cyber-attacks/cyber-terrorism fliers, seminars, and workshops for small businesses." "I have become more creative and innovative with cybercrime, identity theft, human trafficking and cyber-bullying problem solving after my self-taught training. I served as a facilitator presenting cybercrime information in numerous block-club meetings and police community gatherings."

One comment I found quite interesting was garnered from one (12.5%) police personnel who asserted "I am a civilian and new on the job (one week) and I used my cybercrime training twice. I learned a lot about identity theft, cyber-trafficking, and how to prevent cybercrime problems. I look forward to working in the detective unit." Additional data was depicted by police personnel and their applied cybercrime training, learning, and preparedness. One participant (12.5%) asserted that "I became more

computer literate with skilled proactive innovations after the cybercrime training held at the academy and the college." Further expressions affirmed that police personnel were more astute and quicker on their feet in understanding problem-solving and decision-making techniques after their basic cybercrime training. "I learned to better assess, evaluate, investigate, estimate and judge all cases, including cybercrime cases after the training." One (12.5%) police personnel expressed writing a couple of identity theft, cyber-extortion, and phishing articles and distributing them in workshops, libraries, and community-policing sessions. Lushbaugh &Weston (2016) indicated phishing entails clicking on an official-looking email from a bank and the 'one-click' allows the cyber-thief to retrieve all information from the victim's bank account.

Data Inquiry 8

Q.8. What are your recommendations to better equip police personnel to combat (fight) and mitigate (reduce) cybercrime? Seven (87.5%) participants of the eight cited productive and favorable suggestions. There were diverse and similar comments with extensive recommendations to better combat and mitigate cybercrime, cyber-attacks, and cyber-terrorism. Listed are fifteen verbatim statements with rich ideas, thoughts, and workable actions asserted by law enforcement personnel (Martin, 2021).

1. "Ensure trainer is equipped with the latest proactive and preventive cyber-attacks and cyber terrorism information."
2. "Train leaders as well as personnel in the latest cyber-security tactics with strong passwords and encryptions."
3. "Set up cyber strategic measures with continual backup."

4. "Provide the latest updated investigation tools with documented departmental policies to mitigate cyberthreats and cyber-attacks."

5. "Receive proper cyber information and maintain the latest innovative cybercrime techniques."

6. "Instruct and provide funding to finance current cyber-security and invest in greater firewalls with the latest encrypted data."

7. "Provide additional funds in the budget for expanded Civilian cybercrime, cyber-attacks and cyber-terrorism training."

8. "Establish and train high-level civilian personnel with cyber security."

9. "Reinforce information regarding current strong passwords that are required to be changed often with a clear dialogue of DOJ's cyber laws."

10. "Use Grants and federal funds to set up cybercrime training for sworn and civilian personnel for anti-virus/anti-fraud with encrypted security."

11. "Commands must have funds with plans to train leaders as well as the law enforcement personnel early-on in current cyber security and cybercrime infrastructure techniques."

12. "Use strong passwords, security apps, and encrypt data to combat the many cyber-attacks and cyber-terrorism."

13. "Work to understand cyber-attacks, cyber-security tools, and the cyber-encryption to assist in setting up new policies and politics regarding foreign cyber terrorism."

14. "Set-up cybercrime teams with several other law enforcement agencies to establish cyber crime principles and guidelines for preventive measures to form a synergistic whole."

15. "In order to better equip police personnel in combating and mitigating cybercrime, I recommend that the basic parameters of cybercrime training opportunities are disseminated throughout all police agencies."

The police personnel cited a wide range of recommended perspectives to better equip cybercrime preparedness and training.

Data Inquiry 9

Q.9. What methods and/or strategies do you believe can assist in uprooting (eliminating) cyber-attacks, cybercrime, and cyber terrorism? One hundred percent (100%) agreed that it was necessary to establish plans or viable structures for everyday people to be aware of cybercrime prevention. Other comments were "Since everything is tied into computers, free cybercrime workshops should be set up for the public and taught by civilians, not only sworn officers." Public announcements on television and other social media can assist in cybercrime prevention. Cyber Safety and security will eliminate the many scams and threats. The law enforcement personnel expressed ways and techniques to uproot the ever-increasing cybercrime. Listed are 18 verbatim comments asserted by police personnel emphasizing workable techniques, tactics, and strategies

to reduce and eliminate cybercrime (Martin, 2021).

1. “Document digital evidence and explain port scanning scrutinizing for open computer doors used by attackers.”
2. “Understand how to decipher email headers, doxing, and sniffing (that monitors traveling data) and present info as public service messages.”
3. “Have a cyber plan and make sure there are ways to protect, eliminate, and decipher the ongoing critical cyber-attacks.”
4. “Avoid the cheap cloud services that are vulnerable to cyber attacks.”
5. “Have strong cyber plans, goals, objectives, and strategies to prevent ubiquitous data theft and always check for illegal activity each day.”
6. “Prevent cyber-attacks and computer viruses introduced by infected disk or media; maintain protective security.”
7. “Use investigative teams with different Internet skills to submit and retrieve downloaded surveillance data and make sure it is secure.”
8. “Obtain targeted intelligence and cyber fraud training from IC3.”
9. “Remain current and never let ‘pharming’ catch you off-guard in a hijacked domain (a fake site) such as your bank or credit union.”
10. “Encourage people to understand the sensitivity of the computer evidence and report any cyber theft immediately,”
11. “Recognize that jurisdiction plays a critical role in cyber-attacks and cyber-terrorism; understand federal and state laws.”

12. “Secure and protect the integrity of cybercrime evidence and restrict with a digital search plan and encrypted data security.”
13. “Be aware of the time and the critical aspects when addressing and securing the data on the network during cybercrime investigation.”
14. “The National Institute of Justice explains electronic evidence.”
15. “Digital evidence is of value and may contain data that is perishable; seal and secure returning to the businesses as soon as possible.”
16. “Identify and document any digital electronic devices (scanners, DVDs, CDs, flash drives, or bar coding) and systems.”
17. “Check for the cyber hardware disabler which is a device that has a self-destructing device to eliminate any electronic evidence.”
18. “Understand that the cyber electronic memory hard drive holds an excessive amount of evidence similar to the cell phone’s SIM card. “

Data Inquiry 10

Q.10. The final data inquiry provided the greatest amount of valuable cybercrime law enforcement data. The processes and procedures can assist in reducing and eradicating cybercrime. The data inquiry for #10 questioned-Will you list any other cybercrime law enforcement preparedness procedures you believe will help to fight, reduce, and eliminate cybercrime, cyber-attacks, and cyber-terrorism? The entire eight participants (100%) provided a tremendous number of valuable deep recommendations and proactive measures. Many techniques, tactics, and courses of action were articulated emphasizing strategies to combat, mitigate, and uproot cybercrime.

Many police personnel had the latest scientific technological cybercrime scholarly skills with high-level professional digital cybercrime knowledge that was quite apparent. Amazingly, seven participants (87.5%) addressed the need to invest in critical infrastructure (waterways, electrical grids, pipelines). The infrastructure crisis was current and one of the major issues and concerns of USA President Joe Biden, who affirmed daily the detrimental infrastructure conditions. The focus was to invest trillions of dollars to restore the crumbling antiquated infrastructure throughout the United States.

The data inquiry feedback for Figure 11 was astronomical with a vast array of pertinent and stimulating data. It had the greatest amount of email attachments aligned and listed with rich proactive and preventive recommendations. Figure 11 explained the intensive and moving responses in the techniques and strategies to combat, mitigate, and eradicate cyber-attacks and cyber-terrorism. I could sense the passion that was cited in the cybercrime feedback emanated from the law enforcement personnel as I read each response. I was stirred by the responses. There were multiple areas and terms I was not familiar with and did not quite understand. However, I was empathetic and moved with the high intensity and desire to make positive social change and eliminate the current detrimental status quo of the cybercrime parameters. It was quite prevalent in the written expressions of the police personnel. The information comments affirmed by the law enforcement personnel are aligned in Figure 11 entitled *Ways to Combat, Mitigate, and Eliminate Cybercrime.* It is the illustrated chart-like figure citing the participants' professional cybercrime proactive and preventive recommended comments.

Figure 11

Ways to Combat, Mitigate, and Eliminate Cybercrime

- Economic funds must be deployed into the crumbling cyber-controlled infrastructure
- Focus and invest in preventive cyber technology to correct the antiquated critical infrastructure
- Establish reliable plans providing greater firewalls and encrypting data for cyber-terrorism security
- Plans with actual dollars are imperative for the debilitating infrastructure and pipeline protection
- Use strong passwords, security apps, code, and encrypted data to combat CA/CT
- Prevent foreign countries from infiltrating our cyber-controlled waterways and electrical systems
- Organize and set up anti-virus and anti-fraud networks with encrypted security/Ensure privacy
- Sworn supervision is necessary for civilians and certified cybercrime agents
- Synchronize and work with community leaders for evaluation of the latest cybercrime techniques
- Patrol officers must not be burdened with added cybercrime weights-main concern is safety &security
- Cyber security to prevent foreign cyber-intrusion (political/CA/CT)/Apply current laws
- Use multi-faceted credible cyber-security to prevent Foreign CA/CT/Auto update malware
- Conceptualize high-level cyber security systems and train personnel on cyber security
- Train leadership first to understand need for combating, mitigating, and eliminating cybercrime
- Coordinate and code backup copies; store off-site, encrypt, prevent, control and access
- Collaborate and Set up CC/CA/CT protection with the latest software and security systems
- Integrate problem-solving and decision making; always shut-down public Wi-Fi cyber programs
- Be Aware Cyber-terrorism constantly communicates on the Internet/Understand identity theft
- Train cyber-security strategic maneuvers with constant backup/Set up seminars and PA's
- Think abstractly-Implement strong security breach programs with encrypted tools & measures
- Celebrate by getting Grant funding to hire additional police personnel with cybercrime skills
- Strong Virtual Private Network (VPN) Encrypt Critical Data/Align workable plans & goals
- Employ Strong Encrypted Coded Methods when utilizing Public Wi-Fi/Articulate objectives
- Maintain High-Level Enablers with Innovative Techniques and High-Speed Internet
- Reflect on Social Engineering with Current Anti-Virus Features/maintain coded step-by-step plans
- Set up civilian cybercrime units within police agencies supervised by sworn personnel
- Critically think regarding cybercrime security with encrypted data and proactive strategic tactics
- Teach public, small businesses, and community settings about cyber-attacks and cyber terrorism
- Change PWs often and provide greater cyber digital awareness training in agencies & communities
- Contact Charge Cards and Flag with Fraud Alerts/Maintain evidence for identity theft w/back-up
- Coach & train employees-limit access to critical data/maintain restricted cybercrime areas
- Provide fliers regarding preventive cybercrime/Distribute ID Theft information to communities
- Maintain sworn officers over civilians in cybercrime investigation units/update the latest cyber info
- Train the principles of cyber-attack to employees, citizens, and public/Professional cyber-security
- Limit and isolate critical information with coded and encrypted protection; check often
- Evaluate new innovative CC police preparedness and training procedures /explain ransomware
- Hire additional civilians with professional cybercrime skills to train other police personnel
- Sworn supervision to train Human Trafficking; Certify & teach encrypted coding to cybercrime persons
- Coordinate with the FBI the regional proactive community-policing cybercrime techniques
- Inform others of the potential critical infrastructure and the need for professional cyber file security
- Detail policies to protect staff's personal information; teach coding and prevent internal cyber leakage
- Set up federal and state policies with licensed cybercrime security agents to eradicate foreign entities
- Hire certified cyber-security encryption individuals to train personnel/Provide fed, state, & local laws
- Systematize units combined of police personnel, civilians, and community leader stakeholders
- Set up Wi-Fi with encrypted coded data and cybercrime strategies/Articulate Internet of things (IOI)
- Purchase and use Norton 360 Life Lock cybercrime protection; do not use cheap cyber cloud service

The responses from Figure 11 in *Ways to Combat, Mitigate, and Eliminate Cybercrime* were astronomical. The power and energy of the responses emanated from the old analogy of the "movers and shakers." I learned much from the rich responses. The police personnel provided creative techniques to address ways to mitigate and eliminate cybercrime and cyber-attacks. Emphasis was placed on greater firewalls, coding, and establishing anti-virus/anti-fraud networks with encrypted security to ensure privacy. Information was cited to distribute and protect charge cards with flags for fraud alerts.

Meaningful suggestions referenced the critical need for political cyber-policies to prevent cyber-attacks and cyber-terrorism. Several comments alluded to establishing new national laws: (1) "Implement government policies with intense high-level national cybercrime felony laws to eliminate the constant upheaval of cyber-intrusions by foreign countries;" (2) "Signify concern requires the greater cyber security with federal policies to prevent national cyber-scams and thefts." (3) "The need is horrendous due to the cyber-attacks and cyber terrorism against our country by outside nations."

Others suggested the need to contract bonded and licensed cybercrime security agents to train and troubleshoot for law enforcement agencies. To protect small businesses, "It is essential to train leaders in small businesses and executive staff to maintain limited restricted access to critical cyber data." Proactive dimensions necessitate the need to limit and isolate critical cyber data with encrypted protection and cyber checks daily. Several (37.5%) police personnel stated to encrypt stronger Virtual Private Networks (VPN) with integrated data to protect cyber security in the workplace.

The employment of stronger encrypted and coded data is necessary when utilizing public Wi-Fi and to assure they are closed at the end of the electronic device's session. "In public places, never open critical files for they can be accessed 30-50' feet away in the same room or facility." "Inform the public with fliers, brochures, and pamphlets regarding preventive cybercrime information and make it available in all libraries, resource centers, and public facilities." "Critical cyber data must be restricted and protected with several coded layers before the data can be accessed."

The cybercrime prevention responses were not explained with full clarity and understanding. It would perhaps have been clearer if the data collection had been face-to-face inquiries. There were responses that were somewhat vague and ambiguous without clear concise meanings. Three prime examples were (1) to maintain sworn officers over civilians in all cybercrime investigation units; (2) to engage professional contracted cyber-security (bonded-licensed) cybercrime training agents; and (3) to hire certified cyber-security encryption individuals to train personnel. There were additional rich and pertinent comments proclaimed that identified ways to combat, mitigate, and eradicate cyber-attacks and cyber-terrorism. However, many needed additional information for added fact-finding clarity. Listed are some of the articulated assertions that needed additional data for further detail and comprehension with understanding.

- Provide federal, state, and local cybercrime laws and political cyber-policies
- Set up Wi-Fi with encrypted expansive data; explain digital search plan
- Shape cybercrime technical strategies and identify cheap cloud services
- Explain the Internet of Things (IOI), port scanning, doxing, and sniffing

- Establish several collaborative national, federal, state, and local cybercrime taskforces to work at eliminating cybercrime, both domestic and international
- Supply the economic provisions to purchase Norton 360 Life-Lock cybercrime protection; identify the location of the hardware disabler and the VPN
- Provide the reasons and ramifications of not utilizing cheap cyber cloud services
- State-specific ways to report cybercrime schemes, scams, and intense technological frauds and identify who receives the initial complaint report

There was unanimous agreement by police personnel to require corporations to immediately inform victims of compromised cybercrime incidents and cyber-attacks. Face-to-face inquiries might have had greater accuracy. As an opposing factor, it might have extended into branch-like divisions heightening a storehouse of added data that might work in the opposite direction. The personnel emphasized actions needed for the USA to concentrate on the weak and insecure critical infrastructures with many open to ransomware. Lushbaugh &Weston (2016) indicated that ransomware renders a pop-up message that the computer has been infected with a virus. The victim is directed to a website link that locks down the entire operation and requests ransom funding.

The Learning Process and Procedures

The cybercrime experiential learning process of police personnel was diverse. They extended from the police academy, colleges, Internet, or were self-taught. The architectural real-world study provided the learning procedures of Kolb (1984). They were analytically processed by the extended data analyses of van Kaam (1966). Rich

results were collected from the police personnel. However, there were a few areas that were somewhat vague and needed additional clarity. The study was small (N=8) with an excessive amount of data. The data was significant in closing the literary gap between police personnel and cybercrime preparedness. Many ideas prevailed with abounding data and proactive cybercrime strategies to combat cybercrime. The data was enormous. One law enforcement personnel attached seven full single-spaced pages to the data inquiry instrument. The police personnel's cybercrime preparedness provided a foundation with principles for future research and everyday experiences in the findings.

Experiences in the Findings

The cybercrime preparedness inquiries were received from law enforcement personnel with an extensive amount of data. All were evaluated utilizing van Kaam's (1966) data analyses. The findings revealed concepts with codes, categories, patterns, segments, and strategic themes establishing the inductive analysis. The procedures emerged from the system as van Kaam's step-by-step data analyses were employed. The personnel data inquiries expressed a wide range of cybercrime phenomena.

The participants articulated a vast array of ideas and perceptions focusing on cybercrime preparedness. The quintessential transcripts consisted of valuable training information. The experiences of police personnel promulgated rich ideas and critical thinking. The training techniques to enhance cybercrime preparedness played an important role. The empirical qualitative study expressed written dialogue discussed

from the small number of police personnel (N=8). The array of diverse cybercrime preparedness and experiential learning was rich and highly informative. There was no pilot study and no face-to-face data inquiry collections. It appeared that many participants expanded their cybercrime preparedness horizons by enrolling in additional training. After the basic training, many pursued additional cybercrime instructions. Advanced cybercrime preparedness was sought from different training locations and learning sites: Google, colleges, seminars, videos, or self-taught procedures. The concept of cybercrime vigilance suggested the need for alertness and intelligence supported by additional cybercrime scholarly endeavors. The collected data inquiries were analytically processed using van Kaam's data analyses. The intense step-by-step process procreated in-depth data with rich recommendations. The study revealed a copious flow of information to bring about social change with transferability to other agencies.

Summary

The study garnered much from the law enforcement personnel in the phenomenon of prior cybercrime preparedness. The empirical phenomenological qualitative study collected a plethora of scholarly knowledge. Rich and in-depth suggestions produced overwhelming components to mitigate cyber-attacks and eliminate cyber terrorism. Chapter 1 addressed the cybercrime, problem statement, purpose, and research questions. The theories were addressed with definitions and the significance of the research study. Chapter 2 focused on the literature review with the wide range of diverse undertakings in the complicity of cybercrime. Cybercrime, cyber-attacks, and cyber terrorism research

were discussed. The study articulated the necessity to close the law enforcement personnel and cybercrime gap in the literature. Kolb's (1984) experiential learning theory (ELT) viewed social media and cybersecurity.

Chapter 3 provided the research methodology, design, and purposeful sampling. The research clearly expressed the role of the researcher. The data collection process was articulated and aligned with ethical considerations and data analyses. The study explored and expressed the underpinnings of Moustakas and how the study was conducted. Chapter 4 discussed the challenges regarding cybercrime preparedness research and the findings. The results presented the procured data from the research questions and the critically assessed data analyses. The inductive analysis was addressed with concepts in codes, categories, patterns, segments, and strategic themes. The strategic themes emerged from the data analyses to better equip, integrate, code, and provide transferability to other entities. Chapter 5 provides a conclusion and recommendations with the interpretation of the study addressed with the significance of experiences, findings, and limitations. The rich perceptions and themes provided a wealth of experiential learning and reflections with wide and varied cybercrime dimensions. The research assisted in explanations to bring about positive social change with the narrative expressing suggested results and expressions. The empirical qualitative phenomenological research added richly to opportunities for social change, transferability, and the need for future studies.

Chapter 5: Findings, Conclusions, and Recommendations

Introduction

The purpose of the empirical phenomenological qualitative study was to research and understand cybercrime preparedness and training in the lived experiences of law enforcement personnel and prior preparedness with experiential learning. Many scholars and leaders are informed concerning the innovative knowledge that my cybercrime research contributes to the field of criminal justice and other disciplines. The study illustrates the transferability and why it is meaningful and significant. The research approach required personnel to examine previous cybercrime preparedness and collect comprehensive thoughts and reflections. The study was built on the underpinnings of Moustakas (1994), Kolb's (1984) experiential learning theory (ELT), and van Kaam's (1966) data analyses. The phenomenon entailed what was experienced to make sense of the world and develop a worldwide view (Patton, 2002). Moustakas offered human science inquiry methods including core concepts with designs to collect data and explain the meanings of human experiences. The narrative discusses overwhelming suggestions to mitigate cybercrime with an override of the jurisdictional system.

Experiential learning encompassed the acquisition of Kolb's (2014) four integrated components: concrete experience, conceptual reflections, abstract formulations, and experimentation. The four were flexible depending on the previous and current learning experiences of the law enforcement personnel. The applied Modification of van Kaam's (1966) data analyses required each participant to complete the 10 data

inquiry tool. The data transcripts were analyzed employing van Kaam's seven step-by-step procedural processes. The steps transitioned from the individual textural-structural descriptions and developed a composite description of meanings and the essences of the participants representing the group (van Kaam, 1966). Moustakas (1994) expressed that the individual descriptions provided the underlying foundation and dynamics. The meanings developed from the explanations represented the synergy of the entire group. The personnel described their personal perspectives on the cybercrime phenomenon. The learning styles and experiences with practical applications were presented in the workplace and community. Police personnel elaborated on strategies to combat and uproot cybercrime bringing productive social change with transferability. Kolb's (1984) Experiential Learning Theory (ELT) served as a tool to ascertain the police personnel's learning perspectives. Holt & Bossler (2013) expressed that cybercrime created substantial challenges for police, particularly at local levels.

Police personnel were often not prepared to handle the increased cybercrime transitions due to the advancing complicities of technological operations. Cybercrime continues to increase exponentially. There is a great lag in equipping, training, and preparing law enforcement (Berg, 2007; Siegel & Worrall, 2014). The study addressed a gap in the literature focusing on cybercrime preparedness and police personnel. The study assisted in filling the literary gap with the concentration on police personnel as they expressed their perceptions of prior preparedness. Kolb's (1984) Experiential Learning Theory (ELT) was utilized as a blueprint to assist in preparing the open-ended semi-

structured inquiries; whereas van Kaam's (1966) data analyses concentrated on analyzing the cybercrime preparedness phenomenon. The research provided great contributions that revealed the social constructs of cybercrime. The real-world view of law enforcement personnel and cybercrime preparedness was enhanced. Strategic tactics were also recommended to mitigate cybercrime and eliminate cyber terrorism.

Interpretation of the Study

The interpretation of the study included a naturalistic inquiry. I, the instrument of the study, collected data remotely from the police personnel in their natural settings via emails and other electronic devices. Moustakas' (1994) methodology defined the phenomenon as the common everyday bonds of human and scientific research. The empirical qualitative phenomenology study included recognizing the design and methods. It then focused on the experiences, and not only the parts. Qualitative research concentrated on the procurement of meanings rather than the measurements that quantitative studies produce. The study collected the results from law enforcement personnel's data inquiries. The experiences of cybercrime preparedness, training, and experiential learning data were essential to understanding the scientific investigations and human behavior perspectives. My personal interest and commitment were not to prove anything but to understand the complexities as they unfolded. I focused on the data inquiries, ensuring I remained neutral without biases. Patton (2002) contended that interpretations and experiences were so intertwined that they often become one. The interpretations are essential to understanding an experience; an experience includes the interpretation.

The cybercrime preparedness and experiences served as an integrated connection in the reflections and pragmatic application as a synergistic whole; the ethical data collection worked to procure and discover the cybercrime preparedness perspectives. The diverse learning styles of police personnel provided a vast array in the inductive analysis design.

The experiential learning was activated as the law enforcement personnel moved through Kolb's (1984) four distinct cycles:

- Cybercrime preparedness was procured, examined, explained, and interpreted with built-in concrete experiences.
- Reflections were activated with retrospective actions encapsulated in critical thinking, learning modalities, and styles to better understand cybercrime preparedness.
- Abstract conceptualizations emerged into the reflections established upon varied experiences with innovative ideas and diverse modified exchanges.
- Active experiential learning, preparedness, and actions provided opportunities for added dimensions including practical applications in the workplace and other areas. New experiences and ideas evolved as the police personnel responded to the multiple data questions with workable comments and thoughts.

Kolb (1984) emphasized that knowledge was persistent and shaped by experience, making connections from prior experiences to new experiences. Growth and development were added to the experiential learning theory (ELT) and the data rendered real-world information from the experiences of the police personnel. The articulated languages were

the ontological contingencies with stipulations and conditions of understanding. It was interconnected to previous learnings. Reflections were combined with abstract formulations and innovative processing was applied in practical ways. There was data on a wide range of learning modalities and participants obtained training from FBI agents, professors, facilitators, coaches, instructors, trainers, or were self-taught. The police personnel employed a variety of equipment with technologies of hardware and software material. The research methods, sample size, and purposeful sampling were scientifically aligned. The data collection and analysis were systematically processed. The theoretical underpinnings of Moustakas (1994) provided the foundation for the 10 data inquiry instrument. The data was assessed and evaluated using van Kaam's (1966) data analyses. Both data analyses of van Kaam (1966) and Moustakas (1994) assured neutrality and bracketing during and after the data collection process. The data collection and analyses began to flow together complimenting each during the research study.

The study contributed to the cybercrime literature assisting in filling the gap between police personnel and cybercrime preparedness. Participants had to return and reflect upon their prior preparedness to provide comprehensive cybercrime descriptions and answer the data inquiries. The essence of reflections resulted in an overwhelming number of recommendations and details. The specificities were emitted by the personnel regarding prior cybercrime preparedness. The qualitative study contributed rich information to the field of criminal justice, cybercrime, and other entities that reinforced the additional police personnel preparedness research. In-depth recommendations were rendered to mitigate and deter the trajectory of cyber-attacks and cyber terrorism.

Significance of the Experiences

The significance of the research procured experiences and reflections of police personnel and cybercrime preparedness. It collected the analytical appropriations with enhanced strategies and techniques to combat, and uproot cyber-attacks, and cyber terrorism. The need for the research was due to the extensive increase in cybercrime and police personnel not sufficiently equipped to handle the challenges. It was a highly complex and controversial issue. Lyman (2016) affirmed that law enforcement personnel currently focus on proactive measures, rather than reactive ones. The antiquated reactions conducted in the past are no longer a fact. Investigations are now proactive. Cybercrime forensic investigations procreate the need to analytical assess what transpires before the crime and identify who could be the culprit (Lushbaugh & Weston, 2016). The FBI consistently works with local police agencies understanding their first-hand abilities in the initial contact and observation of cybercrimes.

Cybercrime investigations are dynamic in nature and it requires a great amount of technical expertise with an understanding that the volume of evidence is burdensome (Lyman, 2016). Cybercrime has continued to increase with the largest known cybercrime activated against the USA in 2020. The theft of cyber data targeted billions of Americans with vague evidence and conjectures pointing fingers at countries, such as Russia and China. The anonymous cybercrime accusations escalated while personal data floated in cyberspace and Americans remained victims. Cyber-attacks continue to escalate with political and national conveyed associations that are becoming a worldwide epidemic.

The local law enforcement personnel are often the first responders collecting the initial preliminary reports with ongoing investigations from victims. Lyman (2016) affirmed that the fastest-growing crimes in the country are "those labeled as cybercrime or crimes that take place over the Internet" (p. 258). There is an intensity of need for research on police personnel cybercrime preparedness and experiential learning. The new innovative procedures to mitigate and uproot cyber-attacks are critical. The findings and significance of this study assisted in closing the gap by contributing valuable and significant information integrating Kolb's (1984) experiential learning theory (ELT).

The study produced inductive inquiry data as an extension of the police personnel's perceptions of cybercrime and pragmatic applications. The participants responded in diverse ways with their beliefs, values, and perspective. The cognitive conceptions were reflected in cybercrime preparedness. Significant principles, actions, and systematic paradigms arose as the participants addressed the data inquiries. Constructive ideations and conjectures were presented by participants to mitigate cyber-attacks and eliminate cyber-terrorism. Moustakas (1966) asserted detailed experiences are improved by visions and sounds with natural arousals of memories. Retrospective reflections and discernment result during the process of critical thinking. The empirical phenomenological study added insight and valuable information in understanding basic parameters and dimensions concerning cybercrime preparedness and training. The varied learning modalities emanated rich information with integrity for positive social change with transferability. A productive framework was provided for future research.

The Framework of the Empirical Phenomenological Study

Kolb's (1984) theory provided the framework for the empirical phenomenological study and aligned challenges to select, integrate, and understand cybercrime preparedness. The theoretical underpinning of Moustakas (1994) established the methodological design and sketched the foundation in a systematic way to collect and analyze the data. The design described purposeful sampling, site selections, data collection, and analyses. The procedures aligned how the study was conducted with opportunities for comprehensive reflections from the police personnel. The study captured the perspectives and descriptive data employing rich theoretical support of Moustakas (1994), which was based on the workmanship of others. The data analyses utilized van Kaam's (1966) seven-step process providing interpretations as an extension of the theoretical framework. The inductive inquiry analyses identified comprehensive concepts with analytical discernment. Henceforth, it evolved into codes, categories, patterns, segments, and strategic themes developing an inductive inquiry design. The phenomenological methodology provided the foundation of the design and approach guiding the study (Dawidowicz, 2016). The research promulgated a rich response to the data inquiries from the police personnel utilizing the research of Giorgi (1997).

The empirical phenomenological psychological research of Giorgi (2009) was originally developed at Duquesne University and emitted a structure for the study. Much was provided for the format with principles extended as a framework for the open-ended data inquiry collection. The reflections and interpretations were based on Giorgi's (1997) five-step process that worked to (1) gather the sense of the whole in reading the entire

statement; (2) apply discrimination of meaningful units by reading and re-reading with a focus on the research phenomenon; (3) accommodate transformations of everyday expressions into a focus on the phenomenon as the concrete language transforms into the psychological science language; (4) employ synthesis of transformed meaningful units into experiential structures from the developed statements; and (5) initiate the final synthesis as it is systematically combined with all statements describing and capturing the essence of the experiences and the phenomenon under study.

General Approach

The general approach focused on the concepts of the police personnel and evaluated the phenomenon. The initial facets are cybercrime preparedness, experiential learning, and pragmatic applications. The cybercrime preparedness phenomenon captured the open-ended data inquiries. Answers were collected via emails, electronic apparatuses, and other technological devices. Creswell (2009) asserted the general format of research design included (1) pursue an interest in an idea; (2) conceptualize and examine the process; (3) operate how it will be accomplished; (4) select the method; (5) establish the population and sampling; (6) align the data collection process; and (7) perform the analyses with the conclusion. The research design was clearly stated and addressed.

Research Design

The empirical qualitative research design was the most appropriate design for the phenomenological study. Opportunities were provided to collect the cybercrime preparedness data and conceptual meanings from police personnel and their experiences. The methodology played a critical role in aligning and describing the details of the study.

The framework was arranged to collect the police personnel's prior experiences during the prior cybercrime preparedness utilizing Kolb's ELT. The insiders' views were emic, which is unique and distinctive to the participants. Etic was the outsiders' views. Bartunek & Louis (1996, p. 88) articulated views regarding emic and etic:

> People who are insiders to a setting being studied often have a view of the setting and any findings about it is quite different from that of the outsider researchers who are conducting the study.

Insiders' views and interpretations played critical roles in the perceptions established in the scholarly reading and critical thinking of police personnel. There were individual challenges depending upon the interpretations derived from the different skills and attitudes. Bartunek and Louis (1996) provided a workable process while conducting an emic-etic (insider-outside) research. It was imperative that I addressed the emic and etic processes. It included the goals with ethical integrity aligned as an extension of informed consent and confidentiality. I had to ensure I remained neutral and without bias. I did not comment or state any personal reflections to influence the police personnel. The research design yielded the foundation and the theoretical framework of Moustakas, Giorgi, Husserl, and van Kaam. The lived experiences of the personnel provided data with integrity and reliability for future research. The learning by experiences expressed by Kolb (2014) was built on lived training and personal participation utilizing concrete experiences. The groundwork provided ways to answer the three research questions that were analytically aligned within the 10 data inquiry instrument. The responses were organized on spreadsheets with the results assembled into codes, categories, patterns,

segments, and then strategic themes as an inductive inquiry design. The aspects of a phenomenology research design were cited by Dawidowicz (2018)-(1) work to understand the human conditions involved in the experience bringing about a result; (2) answer the inquiries about the personnel; (3) grasp the phenomenon through their senses; (4) serve to understand the knowledge and insight clearly; and (5) examine how responses can be transferred from one experience to another experience.

Substantive Significance

The empirical qualitative research was produced by fulfilling Patton's (2002) substantive significance requirements that demanded four findings to be achieved by the research (1) strength of the evidence to support the phenomenon; (2) results are increased and deepened by the in-depth understanding of the phenomenon; (3) support the creative innovation significance; and (4) contribute productively to social change with valuable rich problem-solving and decision-making efforts to society. The four elements assisted in determining the substantive significance of the study. The foundation is established for future research. Patton (2002) asserted that readers and users of the analyses are the final judges; their own decisions and judgments concern the substantive significance (p. 467). The findings provided additional substance to the significance of the police personnel's cybercrime preparedness. The social constructs produced workable strategies with tactics to combat, mitigate, and uproot cybercrime and cyber terrorism.

Discussion of the Findings

The findings were diverse with similarities in the police personnel's expressions. The prior preparedness training was gauged with the cybercrime phenomenon. The research

findings offered insight into the study as it described and analytically examined the perspectives of Michigan law enforcement personnel. The literary gap was addressed focusing on the perceptions of police personnel and prior cybercrime preparedness with engaging ideas, experiences, and scholarly learning. The theoretical aspects moved to the pragmatic components. The study examined and investigated the lived experiences of police personnel in cybercrime preparedness and learning styles with confidentiality.

Confidentiality

Confidentiality was assured with the anonymity that the identity of the police personnel and agencies would not be revealed in any way in the research. Confidentiality means I know; however, I will not divulge the information. Whereas anonymity means I do not know for the data inquiry instruments are returned anonymously. During the study, temporary emails were set up with pseudonyms to further protect privacy. No person reading the research can identify the police agencies or personnel. Patton (2002) contended that the norms of confidentiality are changing as tensions emerge between ethics and protecting individual privacy. I had to change several items to protect the privacy, confidentiality, and anonymity of police personnel.

There were demographic data I could not reveal that might be identifiable. I collected rich intellectual cybercrime knowledge and understanding from participants. Knowledge is power; if incorporated and applied with discernment, enlightenment, understanding, and experiential learning (Martin, 2015). I assured each agency of its integrity and dedication to protecting all identities. It was cited that researchers must establish an attitude of concern, confidentiality, and dedication to obtain the necessary

collected data (Patton, 2002).

The informed consent assured confidentiality listing the purpose: who and what the data was for; how it would be utilized; what would be asked; how the responses would be handled; and what were the risks and benefits. The cybercrime preparedness data was implemented with confidentiality as police personnel expressed their distinct and diverse training in cybercrime preparedness with experiential learning. The participants provided a great amount of data with the human scientific inquiry orchestrating the study and providing great wealth with in-depth results. I personally experienced great enlightenment and growth from the rich data of the police personnel regarding preparedness and the extensive proactive cybercrime tactics.

Researcher's Reflections

The empirical qualitative phenomenological research questions explored the police personnel's perceptions and experiences collected from prior cybercrime preparedness. The phenomenological qualitative method entailed the interest, design, and approach guiding the study (Dawidowicz, 2016). Cybercrime is pervasive touching countless individuals and businesses. The research questions utilized the 10 data inquiry collection tool. I had to ensure I remained neutral without bias reporting any potentially biased sources. The inability to observe participants face-to-face might have worked as a positive entity; only further research will reveal if this is a reality. Patton (2002) affirmed that systematic data collection requires credibility, integrity, and neutrality balanced around the selected phenomenon.

I had to ensure the rigor possessed was strict professionalism with competence,

skills, and credibility. I ensured I had integrated and aligned key elements in the data inquiries. This allowed the opportunity to understand the preparedness proficiencies in a practical manner. I designed and developed the data inquiry tool with assistance. I sought the expertise and wisdom of experts in the field from other universities to analytically assess and evaluate the data collection inquiry. The 10-item data inquiry tool had to collect data with the appropriate words and terms without steering personnel in any way.

The police personnel revealed techniques and tactics focusing on prior cybercrime preparedness. In addition, the participants articulated preventive procedures to mitigate cyber-attacks and eliminate cyber terrorism. Much of the outcome and narrative are documented as detailed quoted statements transcribed from the data inquiries. An overwhelming amount of feedback was procreated from cybercrime preparedness, ELT, and scholarly cybercrime knowledge. The police personnel answered without an allocated time slot. They provided much more than I anticipated with professional and informative intellect. The extensive data was significant and interesting with positive productive social change and transferability. Although there were multiple challenges, the study produced a wealth of knowledge and viable information.

Additional Challenges and Reflections

Due to the COVID-19 virus pandemic, there were no face-to-face interactions. I believe it might have worked in positive ways to assist in eliminating biases and maintaining neutrality in the research. All responses were garnered by email, telephone, and other electronic devices. I believe the trustworthiness in confidentially and anonymity evoked great opportunities for integrity, accuracy, and upright comments. The

anonymity allowed police personnel greater comfort zones to express honest answers to inquiries. The participants openly expressed their opinions and perceptions. The findings emanated rich ethical expressions with significant real-world comments and abstract thinking. The participants expressed a great amount of highly informative material. There was an indication that the personnel was educated or certified as cybercrime experts. A large segment of the scholarly cyber terrorism strategies was submitted with recommendations provided as a synergistic unity. The study evoked high-technological components evident in the need for additional phenomenological research. The personnel expressed the need for cybercrime investigation research with an in-depth retrieval process to obtain the forensic digital-divide data.

Limitations

There were quite a few research limitations. The limitations are not listed in sequential order or aligned as priorities. One limitation was the study concentrated only on police personnel in the state of Michigan. Several additional participating states might have allowed the proclivity for greater versatility and more participants. If additional states were involved, my challenges might not have been as difficult attempting to obtain consenting law enforcement agencies. Another limitation was the small sample size (N=8). I initially desired a sample size of at least 12 participants. However, the purposeful sampling data from the eight police personnel produced an excessive amount of rich in-depth data. The small sample size provided valuable data procreating rich and workable information. I was shocked by the great amount of data that resulted from the

small sample size. The qualitative phenomenological study was not meant for generalizations (Dawidowicz, 2018; Martin, 2015). The empirical method described and systematically explained the phenomena as completely and accurately as possible in accordance with the values that undergirded the findings.

The COVID-19 pandemic played a critical role in obtaining the necessary law enforcement agencies and personnel for the research. The requests were submitted to multiple administrators, police chiefs, public safety commissioners, and directors in Michigan to enlist their agencies to participate in the research. The requests were confronted with great challenges due to the coronavirus pandemic. There were reduced staff, sickness, death, and adverse controversial marches throughout Michigan, which limited the research. The Centers for Disease Control (CDC) identified Michigan as the pinnacle of the coronavirus pandemic with the highest affected COVID-19 state in the USA. For 13 months I submitted non-stop over 835 USPS letters, emails, and other electronic transmittals to law enforcement agencies requesting participation.

During the initial five months (prior to the pandemic), I received positive responses, verbal confirmations, and emails from chiefs, and directors expressing the desire to participate. However, when I received conditional approval, I was faced with a quagmire. It was eight months of constant "request-after-request" before I received a solid confirmation. I hit "one brick wall, one after another." Two police executives informed me that police doctoral research had transpired during the last five years that assured anonymity. However, it was evident that the agencies were readily identified in the research. I was further informed by several police executives from large agencies

that they demand all external research must be submitted and approved by the police law departments or legal units. It could require 12 to 18 months for final approval decisions.

Another limitation of the study was the inability to have face-to-face data collection inquiries. Qualitative inquiries are usually in-depth studies utilizing face-to-face techniques to collect data (Patton, 2002). Face-to-face inquiries might have provided additional clarifications to the data. However, it could have negatively impacted the responses and distorted explanations. Face-to-face inquiries allow facial expressions and kinesics (body language) to be displayed with verbal feedback (Hess, 2017). There were no recorded, listening, or visual aids available during my data inquiry collections due to the COVID-19 pandemic. Jasper (1994) cited that data inquiries and interviews require sensitivity, trust, and rapport during data collection. I established a virtual rapport with each participant before they submitted the "I Accept" volunteer agreement. The process was different from face-to-face interactions and it did not allow participants to reiterate (restate or rephrase answers). However, the participants perhaps answered with greater honesty due to the virtual-remote use of emails and other devices. The participants had sufficient time for critical thinking; there were no restricted time limitations. The police personnel had ample time to think, reflect, and respond to the data inquiry instruments.

Moustakas (1994) emphasized that we grow as we reflect on memories and experiences in retrospective processing. The results were deep explorations and greater enhanced details. I believe the police personnel exhibited greater veracity and integrity due to the anonymity. Only two participants (25%) edited the data transcripts and provided affirmations to the inductive inquiry analyses. All eight participants should have

experienced the opportunity to provide feedback on the inductive inquiry analyses. The personal affirmed opinionated interpretations produce greater accountable accuracy. Member-checking in the inductive inquiry analyses feedback presented a higher level of precision and completeness. Qualitative phenomenology provided rich research despite the limitations. The exploring strengths and stability were efficient while working through the many challenges. The police personnel's cybercrime preparedness and experiential learning presented a diversity of scholarly learning. The plethora of data emerged with rich recommendations and opportunities for positive cyber-attack social change providing workable transferability.

Social Change and Implications

Social change can become a reality by the impartation of the many cybercrimes preventive procedures and processes addressed by police personnel. One participant (12.5%) articulated that "Cybercrime is serious and a threat to our livelihood and the entire nation. Stronger counterattacks must be implemented to offset the mass cyber-attacks and cyber-terrorism we face daily, especially with critical infrastructure." I garnered a great need for cybercrime social change in that one statement. The lag in necessities and technological needs in police personnel cybercrime preparedness and cyber security techniques appear as critical needs necessary to mitigate cybercrime.

The participants provided valuable and workable techniques listed for social change to mitigate cyber-attacks and eliminate cyber terrorism. In addition, law enforcement personnel asserted the ineffective critical infrastructure of the computer technology SCADA (Supervisory Control, and Data Acquisition) system and how

it could result in egregious damage and horrendous devastation to USA utilities. The emphasis focused on the inadequacies of the USA's technological computer system that controls water treatment plants, electric power grids, pipelines, medical facilities, gasoline pumps, and many more. The data inquiry feedback correlated with the statements of Holt & Bossler (2013) that affirmed cybercrime has created substantial challenges for law enforcement, particularly at the local level.

Law enforcement personnel are often not prepared to handle the cybercrime transitions due to the evolving cybercrime technological interventions. Berg (2007) and Siegel & Worrall (2014) supported the statement in the analogy that cybercrime with its challenges increased exponentially, along with the difficulties in proficiently equipping, training, and preparing law enforcement. However, it is essential to understand the complexities in grasping the fundamentals of the increased cybercrime technological and pragmatic information that daily confronts law enforcement personnel.

The nature and behavior of police personnel are aligned with the complicated challenges utilized in their daily skills and knowledge. Then, adding another major entity can result in adverse weights and complications. It appears at a higher level than in the past; this is due to the ever-increasing day-by-day technological cybercrime complicities. Cybercrime is growing at an exponential rate without the opportunity for total elimination (Martin, 2015). The data inquiry responses promulgated real-world proactive cybercrime projections with rich preventive practical implications.

Practical Implications

The research procreated practical implications for social change supported by the police personnel's comments and reinforced the critical need to update the anti-virus programs, enhance cyber security, and install more secure with impenetrable firewalls. The findings offered insight necessary to protect the data and prevent increasing cyber-attacks. Local police personnel are the first responders to cybercrime and are cognizant of the great vulnerability of cyber-attacks and cyber-terrorism (IACP, 2005; Siegel & Worrall, 2017). The escalating cybercrime has become apparent in the USA with cyber-attacks focused on the aged critical infrastructure, both public and private components. There are many needs at federal, state, and local levels for cybercrime policy changes, and were cited several times by participants in the feedback. It focused on escalating cybercrime threats with actual cases of ransomware incidents and critical infrastructures.

Ransom of 4.4 Million Paid in 2021

The CEO, Joseph Blount Jr. of Colonial Pipeline, was before the Senate Homeland Security Committee Federal lawmakers on June 7, 2021. He explained how he made the decision to pay a 4.4 million-dollar ransom to the criminal cybercrime hackers who penetrated the corporation's networks in May 2021. He reiterated that he took full responsibility and would perform in an identical manner if confronted with the same set of circumstances. Blount became the CEO of the pipeline in 2017 and expressed the need to pay the 4.4-million dollars ransom for the decryption tool bringing the Colonial Pipeline's network back online as rapidly as possible. Colonial Pipeline shut down the cyber-IT systems to prevent further compromise to the network, understanding that the

pipeline was a critical infrastructure. The CEO was cognizant that he had to immediately restore the flow of more than 100 million gallons of essential fuel. The corporation distributes daily approximately 50% of fuel on the USA East Coast to first responders, airlines, gas stations, and many other major corporations and entities. The horrendous cyber-controlled entities identified the great need to update critical infrastructures and work on eradicating cyber-terrorism. It was inferred the cyber-attack was orchestrated by Russia or China; however, it could not be confirmed. It emphasized the continual growth in the ever-increasing cyber complicities by foreign countries. Lyman (2016) asserted that the online Internet also served as a sort of "virtual jihad university" and played a role in three radicalization components: the Internet grievance, mobilization in developing group dynamics, and ideology for future extremists.

It is imperative that institutions and corporations share and immediately distribute vital cybercrime incidents. When the medical hospital records and other institutions were compromised, the victims were not informed until twelve months later. Siegel & Worrall (2017) asserted that the propensity was to reduce the fear in individuals and to maintain secrecy with covert actions. Sharing illegal cyber-attacks and cyber complicities could assist in stopping adverse cyber-terrorism. Lyman (2016) cited that cybercrime exposure could assist in deterring cyber-attacks. Many might be prevented if the delayed criminal activities were readily exposed. The failure to share immediately provided hackers (possessing high-level expertise) to further test their skills with the continuum of time and space perpetuating extremely insidious Internet crimes. Years ago, ethical hackers (good guys) were recruited by large corporations and governments to identify

cyber weaknesses and potential vulnerabilities (Lushbaugh & Weston, 2016). The data analyses revealed scholarly and well-versed police personnel cybercrime experts.

Data Analyses

The phenomenological study procured perceptions of police personnel presenting cybercrime preparedness with constructive social change and transferability from the data analyses of van Kaam (1966). The data inquiries answered the three research questions and evoked rich insight and overwhelming contributions to the high-level cybercrime technical knowledge with a great understanding of the phenomenon. The focus was on enhancing preparedness with recommendations to combat cybercrime and mitigate cyber-attacks. Each comment was logistically aligned and analytically processed. The feedback expressed the conjectures of honesty with viable thoughts. There was an extensive array of apparently highly intelligent and educated cybercrime police personnel.

The strategic themes were determined by gathering the words, terms, phrases, and concepts from the collected data. I evaluated the data inquiry and systematically arranged key components captured on spreadsheets as an extension of van Kaam's data analyses. I summarized the data into concepts: breaking them into codes, categories, patterns, and segments that evolved into strategic themes. The data analyses were time-consuming; however, they supplied meaningful worthwhile information that emanated into the inductive inquiry design. I concentrated on the words, terms, and phrases as the inductive inquiry design evolved from the data collection. Productive meanings were analytically aligned from the police personnel's data that emerged into significant strategic themes. Pertinent thoughts and logical thinking were combined with Kolb's (1984) experiential

learning that moved from prior cybercrime theoretical preparedness to the pragmatic process. I entered the words, terms, and phrases integrated with indicated concepts on the spreadsheets aligning the matrix into codes. The culmination of components was identified as strategic themes. I reworked the ethical data and reassured the reliability of van Kaam's data analyses for stability. I assessed and reassessed to ensure if the same data was reproduced by another person could it be similarly classified. However, as Patton (2002) cited it was virtually impossible to replicate the exact analytical process in empirical qualitative phenomenological research. Another researcher will incorporate their own individual personal and intellectual thoughts to analytically process the same data in their own precise ways. The data analysis process was extremely time-consuming. It was essential to assess and evaluate the correct meanings. I ensured I was not in error or not disregarding reflections or abstract notions articulated by the police personnel.

Ethical integrity and accuracy were of the essence. I was quite aware of the limitations and disadvantages of the qualitative phenomenological research study. There were five major limitations: (1) only one research state, Michigan; (2) a small sample size; (3) COVID pandemic restrictions hindering police agencies and personnel;(4) no face-to-face interactions; and (5) the failure that all personnel (N=8) did not have the opportunity to critically assess and edit the inductive inquiry design. The data was rich and extensive. The data analyses utilizing van Kaam's step-by-step process were quite stimulating and laborious. However, the data provided a foundation for future research. I initially believed the shared experiences as a retired 30-year urban sergeant would allow me to rapidly gather police agencies and personnel. However, I was greatly mistaken.

Shared Experiences

Patton (2002, p. 106) focused on the assumption that "there is an essence or essence in shared experiences." There is recognition of the intrinsic meanings of shared experiences mutually understood; henceforth, the ability to express commonly shared ideas and experiences. Shared experiences were important; although, they could evoke certain biases and obstacles. I immediately indicated to the police agencies, I was a retired 30-year urban police sergeant and a police consultant for four agencies. However, it did not provide the network efficiency I anticipated. Obtaining police agencies was "more difficult than pulling teeth." As indicated earlier, I mailed many letters attempting to locate agencies and obtain the email addresses of the CEOs, administrative assistants, or secretaries (not available or listed on the Internet). It was an extremely hard and long task to locate the participating police agencies. When I finally received a possible approval, I reflected on the rubrics, benefits, and anonymity listed in the informed consent to ensure all entities were concise and complete. I emphasized the importance of truthfulness and honesty in answering the data inquiries.

I emailed the police CEO three attachments (informed consent, demographics, and data inquiry) to provide to the contact person and expressed the importance of understanding the attachments. An email was requested if there were any areas that were vague or unclear. I indicated to apprise me if there were instances that might challenge or place anyone in a precarious position. There were no comments received regarding needs or clarifications from the agencies or participants. I emphasized added anonymity by instructing participants to establish temporary emails (yahoo, AOL, hot mail, or MSN).

I was sensitive to focus on ethics, confidentially, and anonymity with protected privacy for all law enforcement agencies and police personnel. Ethical processing was the narrow scope of restrictions that limited and prevented exposure to any demographic data. It was critical not to reveal the agencies or participants. Police personnel were confident that their agencies had confidentiality and anonymity. I provided sufficient time for participants to document their answers on the data inquiry instruments. The data collection parameters allowed honesty and truth with integrity and accuracy promulgated throughout the study. The rich phenomenological data analyses provided deep workable and preventive cybercrime techniques, strategies, and tactics.

Phenomenological Research Data Analyses

The modification of van Kaam's (1966) data analyses incorporated the collected inquiry transcripts and produced real-world projected applications. Each verbatim comment or statement relevant to the phenomenon was systematically and analytically processed utilizing the step-by-step format. I listed the expressions relevant to the experience in the preliminary groupings referred to as horizonalization (every statement having equal value). Reduction and elimination were incorporated by determining the invariant constituents and it tested each expression for two requirements. Initially, I checked to ensure-Whether it contained a moment of experience that was essential with a sufficient constituent for understanding it. Secondly, was it possible to abstract and label it? Expressions that did not meet the requirements were eliminated. Any overlapping, vague, or repetitive expressions were eliminated or articulated in more exact descriptive terms. The remaining horizons were constituents of the invariants of the experiences.

Grouping the invariant constituents of the cybercrime preparedness experiences were sequentially aligned as codes, categories, patterns, segments, and strategic themes. The invariant constituents were the core themes of the experiences. Validation required finalizing the identification of the invariant constituents and ideas by application. I rechecked the invariant constituents and issues of each comment focusing on three areas. Were they clearly stated and expressed in the data collection inquiries? If they were not clearly expressed, were they compatible? If they were not compatible or explicit, were they relevant? If not relevant, they were deleted. The written statements were included.

The individual textual description of the experiences was identified in the collected data and incorporated as relevant invariant constituents and themes, including all comments. They were then constructed as individual structural descriptions of the experiences based on individual structural descriptions of the imaginative variations. Each relevant issue and cybercrime preparedness experience was developed into a composite description constructed with a textual-structural description. They were then assigned as relevant invariant constituents. The essence of the phenomenon in cybercrime preparedness and the meanings were derived from the conjecture of the composite description in the developed experiences and represented the diversity of the law enforcement personnel. It was further coordinated as a collaborative synergistic unity greater than its parts. I documented and formulated copious notes as I coded the data.

The findings met my objective to obtain the quintessential perspectives of the police personnel and their lived experiences. The focus was on their prior cybercrime preparedness, training, and experiential learning. Ethical credibility was mandatory with

neutrality and trustworthiness of the cybercrime preparedness phenomenon. I did not attempt to influence the police personnel in any way as they emailed the completed open-ended data inquiry instruments. I contacted only two (25%) participants for further clarification concerning my impressions of the inductive inquiry analyses. Kolb (1984) asserted that knowledge was not in equilibrium, but constantly shaped by experiences, making connections from new experiences to prior experiences. The earlier experiences worked in connecting the new knowledge. Prior learning stimulated abstract conceptualizations with the new pragmatic activities and applications.

The law enforcement personnel employed a wide range of learning modalities in their quest for cybercrime preparedness. The cybercrime skills were assembled from different learning points: trainers, instructors, facilitators, coaches, self-taught, Google, iPod, the Internet, virtual-remote digital divides, and other complex technological entities. The empirical qualitative study enabled law enforcement personnel to personally engage their thoughts, intensive ideas, and ideations as they completed the data inquiries. Amazingly it worked to reveal experiential learning and cybercrime preparedness. The police personnel's lived cybercrime preparedness with experiential learning filled the essential components of the literary gap and provided valued positive social change with transferability. The study presented a gateway for a more intense and powerful investigation to rework the overwhelming knowledge for future empirical research. The study explored and revealed alternative approaches for police personnel assisting in the cybercrime preparedness flexibility to meet future demands. There were components in the modalities of police personnel's cybercrime preparations with experiential learning

promulgating multiple responses in the individual learning styles. The data articulated significant comprehensive real-world concrete reflections with abstract thinking and discernment. The human scientific inquiry aligned the format for future cybercrime research and provided great value in sharing preparedness with experiential learning. An integrated holistic person-centered system expanded from the lives of the participants.

Integrated Holistic and Person-Centered System

The qualitative research was an integrated holistic and person-centered system developed to understand cybercrime preparedness and the lived experiences of police personnel. The population of interest was individuals that conformed to the criteria of police personnel in Michigan; having experienced prior cybercrime training and gainfully employed or actively volunteering within the police agencies. According to McMillan & Schumacher (2006), the frame for the basis of the phenomenological study was the type of experience that happened or was still happening in naturalistic settings. I collected the core of the cybercrime phenomenon with sensitivity and flexibility incorporating the workable skills and techniques that resulted in the findings.

Findings

The empirical qualitative phenomenological study procured rich data from the law enforcement personnel's prior cybercrime preparedness with in-depth strategies to combat cybercrime and mitigate cyber-attacks. In addition, it might eradicate cyber-terrorism. The study was small with an excessive amount of pertinent data. The police personnel described their individual reflections, critical thinking, and acute perspectives focused on prior cybercrime preparedness, training, and experiential learning with

proactive cybercrime recommendations. The research resulted in an inductive analysis from van Kaam's data analyses that revealed contextual codes, categories, patterns, segments, and strategic themes. I delved into the mechanics of each classification critically analyzing to ensure I was not "over-fitting." Over-fitting is where it is tailored too closely to the original data and was not workable with new data. The data were aligned in accordance with the purpose, rationale, and principles that undergirded the analyses of the empirical qualitative phenomenology study. The potential to yield insight and positive social change unfolded encompassing Kolb's experiential learning with transferability. The ability to understand and clearly observe the nature of the police personnel and their prior cybercrime phenomenon established a foundation for future research. It played a critical role in the perspicacity of the entire study.

The findings emanated ethical procedures throughout the study by (1) understanding the human perceptions; (2) focusing on the phenomenon experiences; (3) comprehending why participants perceive and experience the same analogy in diverse ways; (4) examining how research brings about social change; and (5) working to understand how the transferability experiences and results work for others in similar circumstances (Dawidowicz, 2018, p. 203). The study explored the phenomenon of prior cybercrime preparedness and the perceptions of law enforcement personnel. Their lived experiences provided perspectives with critical introspection and retrospective thinking resulting in rich recommendations to combat, mitigate, and uproot cybercrime. It collected the police personnel's learning styles, approaches, and ways to evaluate their accomplished achievements.

The findings suggested that police personnel preparedness was garnered in many ways, through classes, technical training, and learning styles with self-taught tools. The proactive cybercrime tactics varied depending on the experiences and behaviors of the police personnel**.** The epitome of candor transpired from the data inquiries as an extension of the police personnel's perspectives and experiences during, prior to, and after the preparedness with high-level cyber technologies. Values were extended and conducted in accordance with scholarly standards. The cybercrime preparedness and police personnel research emanated an overwhelming amount of value for future studies. The subsequent segment entails a recapitulation of the findings.

Research Question 1 (Data Inquiries 1-3)

The first research question was [**Q1**.].What are the law enforcement personnel's perceptions, lived experiences, thoughts, and ideas regarding the prior cybercrime preparedness, training, and experiential learning, and in what ways was it meaningful, relevant, and interesting? The three data inquiries (1-3) answered the initial research question. The study revealed the ideas, thoughts, and perceptions of police personnel. They were quite diverse with similarities demonstrating variations in the prior cybercrime preparedness and training. The law enforcement personnel presented their perspectives dependent on their personal opinions and needs as they acted and reacted during the prior cybercrime learning. They had similarities; however, they were not exact or did not follow precise cybercrime preparedness processes and procedures.

The following factors transpired in response to the first segment of data inquiries performed. There were diverse training modes, techniques, and classroom management.

There were self-taught instructional experiences and versatile learning styles. The personnel received cybercrime preparedness from academy staff, FBI trainers, college educators, and instructions from other police personnel. Ideas and technological interactions were expressed with underlying diverse training with details. The study allowed the open-ended semi-structured data inquiries to procure ideas from personal perceptions and reflections. Most of the police personnel expressed they learned a lot, received great examples, and were well-pleased, whereas a few had difficulty grasping the material due to inefficient computer literacy and basic technology inadequacies. Lyman (2016) expressed that cybercrime required a great amount of basic cyber training, technical expertise, and investigation skills with the ability to analyze the data.

In addressing the second half of the inquiry segment-was the prior preparedness meaningful, relevant, and interesting? Seventy-five percent (75%) rendered constructive comments. Two (25%) participants attributed “computer inexperience” and “I was just learning computers.” Lyman (2016) contended that the distinguished attributes of computer crime investigation demand the listed concerns-(1) the monitoring of bulletin boards; (2) contacting businesses and schools; (3) detecting Internet perpetrated crimes; and (4) focusing on treacherous computer-enabled crimes. One police personnel (12.5%) emphasized the need to provide greater opportunities to understand the positive implications during the cybercrime training learning process. Participants in the initial cybercrime preparedness alluded to the systematic computer training that was utilized intrinsically with developed digital divides. The advanced high-technological tools were essentially combined with the necessary insight of police forensic investigators that

invest in cutting-edge scientific technologies (Hess, Orthmann, and Cho, 2016)

The third data inquiry evidenced seven participants (87.5%) with positive responses to prior cybercrime training experiences. The results contributed greatly to the details and a wide range of multiple factors, which evolved and provided the foundational components of the inductive analysis design. Law enforcement personnel had to understand the basic hands-on knowledge with cognitive law enforcement knowledge of computers as a target, a tool, and the acknowledgment of basic crimes incidental to an offense (Hess et al., 2016). The naturalistic real-world prior cybercrime learning was built on the experiential learning theory (ELT) and the principles of Kolb (1984). The learning design of Kolb (1984) offered opportunities to understand the diverse learning styles; explain the cycle; build structures with principles; to underpin the learning cybercrime activities using pragmatic applications. Kolb's learning theory was a basic four-cycle learning process referred to as a training cycle. As discussed earlier, Kolb's model was aligned and developed by asking the following four questions.

- What do I know (individual)?
- What do I need to know (conceptual)?
- How much and how well do I need to understand (relational)?
- How can I grow my learning in this area (developmental)?

The responses from the first three data inquiries supplied answers to the initial research question. The law enforcement personnel expressed an enormous number of perceptions, lived experiences, and thoughts with ideas. It referred to the prior cybercrime preparedness and experiential learning in ways that were meaningful, relevant, and

interesting. The participants further indicated that the initial cybercrime preparedness resources should include a variety of learning props, such as review exercises, quality checklists, videos, CDs, DVDs, iPods, flashcards, self-quizzing, hand-outs, and other digital mobile electronic devices for ongoing individual cyber social learning.

Our social cyberlearning is important. Rosenweig (2013) affirmed that cyber-social learning depends on the interconnectivity of the basics in the cyber-system and how one operates from cybercrime to cyber-warfare maintaining safe systems. The first three data inquiries rendered many categories that evolved into inductive inquiry analyses. The data was analyzed by van Kaam's (1966) seven-step process emerging into the contextualization of codes, categories, patterns, segments, and then strategic themes.

Research Question 2 (Data Inquiries 4-6)

The second research question was [**Q2**.].Where did the law enforcement personnel acquire the prior cybercrime preparedness, training, and experiential learning; and how was the cybercrime preparedness training applied in a pragmatic manner in the law enforcement workplace? The second set of data inquiries (4-6) answered research question two. All eight participants (100%) received cybercrime preparedness and training within the geographical location of Michigan. Additional cybercrime training was received by three (37.5%) police personnel outside the state of Ohio, New York, Georgia, Illinois, and California. However, it was not clear and did not indicate if they attended brick-and-mortar classes or virtual-remote via technical transmittals. Kolb (1984) cited the importance of experiential learning as an extension of real-life entities. The initial learning provided a foundation for additional cybercrime information and

learning. Eighty-seven and one-half percent (87.5%) cited they favorably applied their cybercrime training in workplaces, communities, and educational facilities. There was only one (12.5%) that did not apply the cybercrime preparedness training and learning right away. However, the participant utilized cybercrime preparedness assisting in writing one identity theft credit card preliminary report. The document was written prior to a transfer to another unit two days later. The police personnel listed many techniques to enhance cybercrime preparedness training. Seven police personnel (87.5%) indicated the importance of receiving handout cybercrime material to reference after the completion of the cybercrime classes. Collect additional cyber-info from the SOS.FBI.gov website.

One major component was evident. Seventy-five percent (75%) emphasized that sworn patrol officers have enough on their plates without adding the additional weight of cybercrime and cyber security. The data indicated that perhaps civilians or other personnel, not sworn patrol officers, should be responsible for the cybercrime. Patrol officers should make their own decisions if they want to be a part of cybercrime training. There were inferences, however not clearly articulated. The responses did not state if the initial cybercrime reports should be the responsibility of sworn officers. Additional cybercrime research can provide clearer and more concise clarifications in this area.

Other feedback expressed the blending of civilians, investigators, detectives, college professors, cyber security trainers, or instructors (who are directly engaged daily in cybercrime and investigations) to train, facilitate, and instruct cybercrime preparedness. The police personnel indicated that the cybercrime instructors, trainers, and facilitators should not only understand cybercrime preparedness but have a passion for

instructing cybercrime. In addition, the facilitators should have actively worked or possess current cybernetic experiences in cybercrime with the latest in critical thinking and perhaps forensic cybercrime investigative skills.

Research Question 3 (Data Inquiries 7-9)

The third research question was [**Q3**.].In what ways have participants applied the cybercrime training and preparedness and what are your recommendations to combat, mitigate, and uproot cybercrime? The third set answered data inquiries (7-9), which was research question number three. The applied cybercrime training responses addressed recommendations to better equip the police personnel in combating and mitigating cybercrime with strategies to uproot the prevailing cyber-attacks, cybercrime, and cyber terrorism. Seven participants (87.5%) affirmed they taught cybercrime skills and trained others on the job, in high schools, colleges, organizations, and local businesses.

The personnel developed and presented cyber-attack material, as well as cyber-terrorism information fliers, seminars, and workshops for small businesses, block-club meetings, education, and community gatherings. The majority applied their cybercrime training, and experiential learning preparedness in various ways. They presented scholarly considerations to better equip police personnel procreating a wide range of strategic maneuvers. One police personnel cited, “I worked on two different cybercrime consulting teams; one for the city and one for the county training others how to combat and reduce cybercrime. I served as a project manager on one team for three weeks.”

One hundred percent (100%) of the personnel agreed that it was necessary to establish plans or structures for everyday people to become cognizant of cybercrime

prevention. Police personnel expressed suggestions to mitigate cybercrime. One gray area that stood out to one participant (12.5%) was the jurisdiction component. Criminal complexities are evoked when electronic crime originates in one state or country and is then committed in another. What jurisdiction prudence law takes precedence? It emits thought-provoking answers that need clarification. The 12 comments were a segment of the suggestions utilized with an emphasis on social and economic cybercrime.

- Explain ransomware and the critical common threats for small businesses; also share the context and content of Ransom DDoS (R-DDoS).
- Understand what Ransom DDoS (R-DDoS) attacks are and that they are of greater risk than Ransomware.
- Present seminars and public service messages on the prevention of cyber-attacks.
- Provide strategies to eradicate data thefts by securing, checking credit cards daily, and making sure to never open unfamiliar or strange emails.
- Share the cybercrime vulnerabilities with the public and ensure they are secure, especially with the android and wide-open electronic smart devices.
- Recognize digital evidence is fragile; do not use automatically updated malware.
- Encourage individuals and businesses to report compromised cyber theft immediately and mandate companies to inform victims as soon as possible.
- Utilize strong coded diverse passwords (letters, numbers, and unique symbols) with documented ‘parked’ configured data.
- Employ strong inverted blended security apps and encrypt data to combat cyber-attacks and cybercrime.

- Activate digital cyber-forensics, complex cyber systems, and cybernetics with investigative incident reports and digital divide responses.
- Establish anti-virus and anti-fraud cyber networks with onion routing layers of encryption surrounding the data transmitted to the Internet for security.
- Support and work with the federal government in cyber-security policies to prevent escalating egregious international political cybercrime intrusions.

Data Inquiry 10 (Integration)

The greatest amount of data was submitted in data inquiry response #10. It produced an overwhelming amount of cybercrime feedback with many strategies and techniques. The statement was: List any other cybercrime police personnel preparedness, training, or procedures you believe will assist in fighting, mitigating, or eliminating cybercrime. The responses yielded facts and knowledge to combat cybercrime and cyber-attacks. The information and evidence manifested a sagacious amount of professional cyber skills and practical cyber terrorism preventive measures. The intellectual scholarly enlightenment of well-rounded cybercrime techniques was profound. I learned a wealth of abounding prolific strategies and an excessive amount of cybercrime preventive measures. However, information with additional clarity was needed in many areas.

The tenth data inquiry embellished a storehouse of cybercrime strategies, policies, and procedures to assist in ways to combat, mitigate, and uproot cybercrime, cyber-attacks, and cyber-terrorism. The valuable remarks procreated eight out of eight (100%) innovative comments. This particular data inquiry received the greatest number of responses. The participants submitted several pages of email attachments. I read

and was moved by the deep passion emitted by the police personnel. The scientific cybercrime strategies embraced the need to act now and not procrastinate. The crucial timing to implement many techniques was articulated as "now" and "extremely critical." Mandatory federal cybercrime policy changes were cited as an imminent crisis. The findings listed eight verbatim comments cited by the personnel expressing critical proactive needs for cybercrime, cyber-attacks, and cyber terrorism (Martin, 2021).

- "Due to perilous times and the increase of cybercrime, it is essential to activate many of these cybercrime strategies and techniques **NOW, not later."**
- "We must proactively move to deter the up-ticked foreign extremely critical cyber-attacks and cyber terrorism."
- "Cost should not be in the equation; the federal government must provide the billions and trillions to build, correct, and protect our USA electrical grids, infrastructures, and water-systems."
- "We must activate cybercrime elimination by employing the new innovative engineering using the virtual remote cyber-reality simulations."
- "Basic police cybercrime training and resource preparedness should highlight the integrating preventive cyber-attack configurations."
- "The expansive Silicon Valley and the projected cyber-designed inventions can reduce, rectify and control the massive cybercrime hacking,"
- "Signal intelligence can intercept, employ, and combat the cybercrime financial data employing the sophisticated code-breaking specializations."
- "The USA has the power and authority to intercept and combat cyber-attacks with

advanced electronic cybernetics and cyber-driven drones."

The data responses cited many systematic procedures with in-depth pro-activated cyber strategies. The feedback unified the cry for additional research for law enforcement personnel, cybercrime preparedness, and evolving cybercrime complicities. There is a great need for empirical qualitative, quantitative, evidence-based, and auto-ethnography cybercrime phenomenon research. The results magnify the embodiment and need for police personnel research with coordinated cybercrime preparedness and other integrated collaborative prevention entities, not only in Michigan but throughout the USA.

The research presented a synergistic operational plan that provided the understanding of variants in the lived experiences of police personnel and their prior cybercrime preparedness. In addition, the findings presented techniques and tactics to protect critical infrastructure and eliminate the complicity of ever-increasing cybercrime. Lushbaugh & Weston (2016, p. 268) emphasized the great need to protect the infrastructure. Our critical national infrastructure includes the energy grid, transportation, power plants, and government services. The communication systems, stock exchanges, and financial institutions are dependent on Internet networks for all operations. Cyber terrorists are attracted to these systems. They are energized with the potential to inflict massive damage with detrimental and devastating psychological and physical atrocities.

The law enforcement personnel communicated multiple technological strategies with encapsulated plans to mitigate cyber-attacks and eliminate cyber terrorism. Most infrastructures throughout the United States of America systems rely on computers.

Hackers are skilled to compromise computers and they possess the abilities to infiltrate and implement major cyber-terrorist attacks. The techniques are egregious with cyber complicities often perfected by hackers' illegal actions. Holt & Bossler (2013) asserted that cybercrime has created extensive challenges for local police as the Internet has rapidly increased. The results are cybercrime transactions against victims allow exploited devastation of digital technology. Insidious cybercrimes have redesigned our nation in the rudiments of the information systems and power grids with opportunities to procreate a wealth of potential destruction as cybercrimes escalate.

The findings added to the literature review focused on police personnel and cybercrime preparedness. It extended the knowledge of the evolving nature of cybercrime preparedness with intense variants to fight cybercrime, reduce cyber-attacks, and abrogate cyber terrorism. Only one peer-review study was performed with a somewhat similar analogy. The research was performed by Holt and Bossler (2012) focusing on patrol officers and cybercrime training. However, it did not focus on all police personnel, cybercrime preparedness, or recommendations to combat and eliminate cyber terrorism.

The police personnel provided disciplined scientific intellectual data that evolved as significant evidence-based cybercrime research. Police are often the first responders contacted regarding cybercrime and are not adequately equipped to handle the emergent complicit transactions. Foundational cybercrime understanding is important that all police personnel and individuals have basic proactive information. Cybercrime mandates are needed to work with preventive techniques and the necessities for individuals to become somewhat computer savvy due to the escalating daily increase of cybercrime challenges.

Courses of preventive actions are necessary to eliminate the impetuous covert operations of advanced cyber-technological complicities. Illegal cybercrime continues to result in devastating aberrations.

The phenomenological research collected qualitative data inquiries of the law enforcement personnel's lived experiences drawing both on creative and critical thinking in their prior cybercrime preparedness and training. It collected the interactive process of experiential learning styles and workplace achievements with tactics to better equip the cybercrime phenomenon. Further implications included efficacious strategies to combat and uproot cybercrime with workable professional and scholarly recommendations.

Recommendations

It was imperative to understand the findings of the study drawn from the small number (N=8) and the overwhelming amount of pertinent data. It flowed in accordance with the purpose, rationale, and principles that undergirded the analytical process of qualitative phenomenology research. The data analyses procreated rich insight into operational ways to mitigate and eradicate cybercrime. The results from the study emitted a proliferation of proactive techniques that are significant with workable innovative procedures and plans. The egregious cybercrime challenges and daily confrontations constantly escalate; therefore, efficient procedures for the betterment of proactive operational actions are essential. The evolving cybercrime complicities can be deterred with the utilization of coordinated collaborative investigation cyber training teams and expert cyber-task forces. Many suggestions and recommendations were revealed.

The passion expressed by law enforcement personnel emanated the trajectory of great cybercrime sensitivity. The assertions expressed that computer science experts enjoy computers and are highly cognizant of software, operating systems, and the interconnections of hardware and networks. The cyber-engineering skills can assist with the infrastructures and assist in cybercrime training. The police personnel expressed a diversity of training styles and modalities to enhance cybercrime preparedness. Several comments were not clearly explained and needed additional clarity for greater comprehension. The research procured rich opinions concerning preparedness and the exceptional ways to combat and uproot cybercrime. The study was rich and indicative of supporting examples with valuable evidence. Eight major preventive and proactive strategies evolved from the data inquiries as creative tactics and techniques with a foundation for potential cybercrime policies articulated by police personnel.

Recommended Strategies, Tactics, and Policies

The qualitative findings indicated strategies, tactics, and policies collected from the inquiry tools with rich in-depth verbatim information. The eight are only a segment of the feedback collected from the data inquiries. They are not listed in sequential order.

1. **Inductive Analytical Design and Strategic Themes-**Two (25%) law enforcement personnel were contacted and expressed their personal views regarding the inductive analyses design with the following three verbatim comments (Martin, 2021).
    - "The inductive analysis design can be used for other research principles and serve as a foundation for the cybercrime policies."
    - "Now, others can build on the strategic themes presented for future studies."

- "It was good although other researchers might produce a totally different set of new information with various entities and substance for transformational change."

The other six (75%) police personnel did not have the opportunity to read and express their opinions regarding the inductive analysis design. I know different comments would have been expressed if all participants had cited their thoughts and perceptions.

2. **Strong Passwords, Security Apps, and Encrypted Data-**It was expressed that it should be mandatory to understand how to set up strong passwords, security apps, and encrypted data for protected cyber terrorism security. Verbatim statements from the participants were readily articulated from the collected data (Martin, 2021): "There is a need to provide cybercrime preparedness to learn the latest technological cybercrime skills." "Equip police personnel with innovative cybercrime knowledge and provide opportunities to become a part of a cybercrime team to assist in writing federal/state policies and guidelines." "Police agencies should provide police personnel, that desire additional training to participate in enhanced technological cybercrime training. They can then return to the agencies and provide Train the Trainer Cybercrime Courses."

3. **Increased Security to Prevent Cyber-Attacks-**The uniform consensus entailed that police personnel should be trained with basic security measures to prevent and eliminate cyber-attacks during the annual In-Service Training. Certain specific comments and clarifications were cited with stipulations (Martin, 2021) "Make sure the individual has a passion for cybercrime training when selecting the police personnel and make sure they truly enjoy computers." "Invest in computer science experts to assist in training."

"Civilians, as well as sworn officers, should be able to receive cybercrime training and become cybercrime experts; they can then train others." Federal agencies are equipped to investigate cybercrime, as well as train local law enforcement (Lyman, 2016). The FBI and Secret Service work closely with local police departments in cybercrime training. One police personnel expressed "Law enforcement agencies must request more cybercrime training with policies from the FBI and other cybercrime experts."

4. **Public Awareness and Training with Police Personnel Experts-**Verbatim comments cited the need to distribute cybercrime prevention fliers before and during training sessions (Martin, 2021). "Ensure cybercrime training and cyber-attack DVDs and CDs are made available." "Inform public of security cybercrime policies and procedures; ensure they are free and available with hand-out material disseminated." "Have cybercrime training material and one-page handouts in libraries and resource centers to reduce cyber-attacks and threats." "Present cybercrime, cyber-attack seminars, and Public Service Messages (PSM) to assist public and businesses." Two repeated expressions were emphasized several times. The need was to define and articulate what ransomware, cybercrime threats, and attacks entail. Explain that ransomware is one of the greatest and most common threats by cyber-attackers. Added comments expressed the need to provide a list of available iPods and Tic Toks describing cyber-attacks on social media and ensure that clear professional anti-cybercrime steps are included.

5. **Critical Infrastructure, Economic Espionage, and Deep Web**-Much data emanated regarding the critical infrastructure and cybercrime policies needed throughout the USA. Listed are verbatim statements cited by police personnel from the data inquiry

instruments (Martin, 2021): “Provide new local and state cyber-technologies to eliminate old infrastructure improprieties and preventive disasters.” “Establish strong cyber-attack security and deter interferences and tampering with critical infrastructure.” “Document the need for cyber-security and eradicate cybercrime meddling from Russia and China.” “Implement protective rationale and laws to prevent weapons of cybercrime mass destruction (WCMD) that kill thousands with chemicals, biological, radioactive agents, and nuclear cybercrime terrorism as well as material stolen from military bases.” “USA should invest in critical infrastructures-waterways, electricity grids, financial, educational institutions, hospitals, and pipelines.“ “Cyber-attacks across the Internet are dangerous because there are no physical borders, no barriers, or custom agents to be confrontational-given the many critical infrastructures challenges.”

“The Internet is wide open to exploit critical infrastructures with horrible devastations.” “Cyber-terrorism is real and foreign-attacks on our critical infrastructures are destructions waiting to happen.” “Economic espionage is theft of trade secrets; whereas, social engineering relies on the shortcomings of human nature to determine and locate individual passwords.” ”Social engineering focuses on the shortcomings of human nature. A blunt force attack requires cyber software to systematically enter documents until a password is discovered.” “The Deep Dark Web is a haven for cybercriminals and was initially set up by the USA Naval Laboratory for encryption.” “The Deep Web is free and can be downloaded in a few minutes allowing computer users to access the Internet with total anonymity, without divulging their identity.” “Onion routing consists of layers of encryption surrounding the data that is being transmitted over the Internet.” “Onion

routing opens the door for detrimental havoc against critical infrastructures." "The public should be aware of bitcoins that are traded on the Internet anonymous and unregulated." Many verbatim statements depicted the demand to protect the infrastructures and stop economic exploitation. There were multiple risks listed providing economic and political devastation that emphasized the weak firewalls and potential detrimental vulnerabilities.

6. **Cybercrime Preparedness and Additional Police Personnel Training**-Listed are verbatim comments regarding cybercrime training with potential policy-making changes (Martin, 2021): "Establish proactive strategic plans with techniques to enhance police personnel preparedness and training." "Set up problem-solving and decision-making federal cybercrime policy changes." "Police agencies must engage in coordinated collaborations with the FBI and other agencies to combine, unite and present a greater understanding to strengthen and implement proactive strategies to combat cybercrime." "Cyber teams are necessary to write and enforce cyber policies." "RCFL (Regional Computer Forensics Laboratories) consists of a digital forensic lab, as well as training centers to provide support for cyber-criminal investigations involving the digital data with availabilities to train police." Lushbaugh and Weston (2016) cited FBI has 15 operational and organizational RCFL Centers nationwide with plans for additional labs.

7. **Data Analytics and Intelligence**-Police personnel cited verbatim comments to align and establish federal and state policies. They added guidelines for law enforcement personnel as they engage in data analytics and intelligence assisting areas to combat, mitigate, and eliminate cyber-attacks and cyber-terrorism (Martin, 2021). "Diverse agencies are essential and united as collaborative coordination to eradicate the ongoing

cybercrime and cyber-terrorism." "It is imperative to work as a cohesive network sharing proactive cyber-crime information." "Activate cybercrime investigators, identify cybercrime co-conspirators and interview cybercrime victims." "Pursue cybercrime terrorists and apprehend individuals connected with cyber-terrorism and cyber-conspiracy." "ID cyber aiders and abettors and upgrade cybercrime preventive intelligence." "Assist in establishing foreign worldwide cybercrime policies with hardcore results." A collaborative federal, state, and local law enforcement cyber team is needed to work with the CIA, FBI, NSA, and DIA. Their concentrated efforts are on cyber analytics and intelligence that gather and write proactive international policies.

8. **In-Depth Critical Retrieval Procedures Obtaining Forensic Digital Data-** Great knowledge and understanding were provided describing the suggested cybercrime forensic digital data investigation. The police personnel expressed the need for cybercrime investigation, analysis, and acquisition with in-depth retrieval to obtain critical forensic digital data. There was an overwhelming amount of scholarly forensic cybercrime expressions concerning investigative tools. Unprecedented innovative cyber-forensic trajectories were included. The key findings and recommendations presented by the law enforcement personnel indicated 12 cybercrime digital forensic suggestions.

- Predicate digital forensic evidence skills working with cybercrime as the forensic specialists incorporate innovative proactive high-level cyber investigative tools.
- Prepare the digital forensic cyber-attacks by reporting acquisition and analysis.
- Manage forensic apps, uninstall ones not currently used, and carefully handle the critical digital cybercrime evidence with federal cybercrime investigation training.

- Establish and train a police network of cybercrime analytical forensic teams utilizing the Internet Crime Complaint Center (IC3) with federal agents.
- Assemble cyber-crime analytical forensic tools with targeted intelligence expert investigators and employ data-recovery accredited cyber security analysts.
- Reboot and connect cyber systems with proactive encrypted digital applications and skills to interconnect with the geo-forensics analytical networks.
- Investigate digital forensic evidence, retrieve, and encrypt the cyber-digital data with underlying software and IC3 supervised cybercrime prevention teams.
- Efficiently handle the process of cybercrime digital forensic procedures as recognized critical scientific forensic systems with federal prosecutors.
- Acquire and develop criminal investigation skills with the precipice for proactive cyber-attack intrusions and breaches of intellectual property rights (IPR).
- Protect, rectify, and engage the alternating cybercrime forensic evidence with other skilled certified systematic security analysts and cyber safety engineers.
- Apply digital forensic investigations as an extension of the cybercrime reports containing the designated click-jacking and cyber terrorism investigation tools.
- Perfect the cyber security skills, logic bomb recovery, converted electronic bits, and employ criminal investigation techniques with the cyber-terrorism tools.

The trajectories provided proactive cybercrime strategic tactics. The concerted retrieval procured forensic digital data providing evidence-based significance for personnel and cybercrime research with practical applications. The process included critical thinking with actions for efficacious preventive forensic cybercrime actions. The cybercrime

study resulted in tremendous modalities, techniques, and proactive measures focusing on many components transcribed from participants addressing answers to the 10 data inquiries. I learned a tremendous amount as police personnel articulated their scholarly cybercrime skills. Many of the participants were well-equipped with high-level expert computer intelligence, cyber-certifications, and technical cybercrime knowledge. I was in awe of the overwhelming data submitted. There were multiple terms I was not familiar with or aware of in the scholarly cybercrime vernacular and terminology. The police personnel were well-versed and trained with much cybercrime professionalism.

Cybercrime Proactive Measures

The cybercrime proactive measures aligned multiple components to enhance and prevent the daily escalation and increase of cybercrime. Multiple cybercrime tactics were expressed by the police personnel addressing innovative approaches.

- Establish a checklist with plans to prevent cybercrime, and identity theft, and demonstrate how to reinforce strong passwords with safe encrypted security.
- Reinforce major cyber essentials in the use of cheap cloud services that open the Internet's use as a target, a tool, or incidents to offenses for vulnerabilities.
- Set up evolving cybercrime preventions with a vision, mission, plans, and goals.

Many measures serve as preventive strategies to ensure police personnel are equipped with cyber security integrated with regulated federal laws, policies, and techniques.

Alignment of Phenomenological Research

The empirical qualitative phenomenological study explored perceptions of law enforcement personnel's cybercrime preparedness. The ethical data inquiries allowed the

police personnel to experience a comfort zone with open genuine expressions. It captured the descriptive data and employed the rich theoretical underpinnings of Moustakas (1994) based on the work of Husserl (1970) and others. Concepts were collaboratively coordinated in understanding the categories, patterns, and strategic themes developed from the data collection. The phenomenological qualitative methodology evoked areas of interest with the design and approach guiding the study (Dawidowicz, 2016).

The research study consisted of quality criteria of excellence that focused on the lived experiences of police personnel and their prior cybercrime preparedness, applications, and workable ways to combat, mitigate, and eradicate cybercrime. The inductive inquiry analyses were built on systematic arrangements of the personnel's detailed statements and quotations. The cybercrime preparedness research was assessed and analytically evaluated. It produced rich perceptions in experiential learning that evoked insight and valuable evidence-based contributions with transferable entities.

The local police receive the initial cybercrime reports, and an investigation is performed by Federal Trade Commission, FBI, Internet Crime Complaint Center, U.S. Postal Inspection Service, or U.S. Secret Service (Siegel & Worrall, 2012). There is only a small segment operated by private agencies and the military does not rely on federal agencies. The military handles its own cybercrime investigations utilizing trained internal military staff. Some of the cybercrime investigation tools utilized by investigators are the Bulk Extractor, CAINE, Digital Forensics, Exit-Tool, Computer Forensics Architecture, SIFT, Cyber-INVEST, Sleuth Kit, and X-Ways Forensics, to name a few. The data collection provided a great understanding of the cybercrime phenomenon rendering a

foundation to bring about positive social change and tools for future research studies.

Future Studies

The study presented multiple challenges as I attempted to collect the police personnel's cybercrime preparedness in the qualitative phenomenological study. The research provided significant data for productive social change with transferability. The empirical qualitative phenomenological research encapsulated a conundrum of police personnel perspectives, cybercrime preparedness, and experiential learning. The rich technological recommendations better equip the prevention of cybercrime. Proactive cyber skills promulgated tactics and techniques to combat cybercrime, mitigate cyber-attacks, and eliminate cyber terrorism. The information procreated a plethora of creative strategies with great wisdom and counteractive knowledge to combat cybercrime.

The research aligned a format for future studies to include more USA states. Ingenuity and scholarly applications worked efficiently with cybercrime technology and research (Long, 2019). The research achieved the purpose of closing the gap between law enforcement personnel and prior cybercrime preparedness, training, and experiential learning. I believe the study might have benefitted from a short survey incorporating a mixed method of quantitative and qualitative research. Future research studies are essential to obtain circumventive information. It could answer more cybercrime preparedness and forensic investigations revealing additional conclusions.

Conclusions

The empirical qualitative research findings were added to the literature review. There were no peer studies concerning police personnel and cybercrime preparedness.

The qualitative research added scholarly knowledge in closing a literary gap. The cybercrime preparedness expressed by police personnel encompassed experiential learning emanating rich data. In addition, the proactive measures to combat, mitigate, and eradicate cybercrime produced rich in-depth insight. Only one somewhat similar research study was found with close similarities. It was the research by Holt and Bossler (2012) regarding the cybercrime training of local patrol officers in two cities. The one agreed-upon consensus in both studies expressed that law enforcement patrol officers currently have an excessive number of duties and responsibilities and do not have the time or availability to handle additional cybercrime.

This study included the experiential learning theory (ELT) of Kolb (1984). The methodological approach was Moustakas (1994) encompassing the cybercrime preparedness. It incorporated van Kaam's (1966) data analyses that evaluated the inductive inquiry analyses and procreated extensive well-informed professional recommendations. The police personnel cited valuable ideas and perspectives with significant contributions to cybercrime preparedness. The findings systematically revealed an inductive analytical cyclic design with the evolution from planning to synergism. The personnel documented a tantamount of strategies and techniques to mitigate cyber-attacks. The research produced suggestions with systematic methods, scientific approaches, and skillful technological cyber components to combat the complicities of cybercrime resulting in positive social change with transferability.

The research contributed great results despite the many obstacles. There was an overwhelming amount of data collected from the personnel emitting a plethora of rich

information. The cybercrime preparedness postulated the inductive inquiry analyses with ideas and opportunities for future research. The study broke up the fallow ground in the trajectory of law enforcement personnel and cybercrime preparedness that contributed to the inquisition of cybercrime and digital jurisdictions for future research.

Contributions to the Knowledge of Cybercrime

The contributions to the body of cybercrime preparedness provided rich creative and innovative information. The study was constructive in explaining the closing of the literary gap. The research provided the groundwork for additional police personnel and cybercrime preparedness to better equip, build, and enhance the preparations for diverse and unique learning styles and skills. Seven strategic themes emerged and were aligned as pragmatically applied entities. The advantages of Kolb's (1984) experiential learning, the underpinnings of Moustakas (1984), and van Kaam's data analyses (1966) served as a logical systematic blueprint throughout the research. The transcribed data collected was analytically assessed that procreated coherent and inductive analogies capturing integrated meaningful and significant in-depth cybercrime research information.

Meaningful and Significant Research

The meaningful and significant research heightened the field of cybercrime preparedness, training, and experiential learning with the lived experiences of law enforcement personnel. The phenomenological qualitative study explored the police personnel's perceptions and perspectives. The research presented ways to enhance cybercrime preparedness with a variety of scholarly learning modalities and styles. Provisions added exponentially to mitigate cyber-attacks and eliminate cyber terrorism.

The research served to be meaningful to scholars, educators, and entrepreneurs. It enriched the lives of scientists, engineers, professors, attorneys, legislators, criminal justice individuals, and others. In addition, cognitive awareness of software and hardware for businesses and individuals was strengthened with proper cybercrime procedures. The evolving cybercrime inventions require additional research in this quintessential technological information-age system. The uphill cybercrime journey is critical and decisive in the daily complicit cybercrime battle. Actions are essential to deter cybercrime and employ workable positive social changes. The designated broadband that transmits the cyber information is critical; the sound bites expressed by police personnel have stirred a wealth of profound needed information (Martin, 2015). The study expresses the imminent need to introduce a more complex cyber-controlled continuum of coordination with perhaps Cyber Crimes Units to expand a more proactive USA worldwide global economy of cyberspace and preventive measures. The law enforcement personnel rendered a storehouse of cybercrime components for positive social change with transferability to federal, state, local, public, and private entities.

Based on my research the individuals who are assigned to a Cyber Crimes Unit could be sworn or civilian personnel or a combination of the two. The persons should have a passion and interest in pursuing cybercrime investigations. Any individuals investigating cybercrimes should initially receive at least 40 to 80 hours of training at the state or federal level. A segment of this training should discuss resource and information sharing with stakeholders who have a vested interest to prevent, protect, mitigate, respond to, and recover from cyber security incidents. Each investigative unit has its

limitations and prior to becoming overwhelmed, they need to know and develop relationships with other investigators that can assist them. These can include larger law enforcement agencies, county sheriffs, state police, military agencies, US Secret Service, and the FBI as well as others who have cybercrime investigators, somewhat similar to fusion centers.

Summary

Chapter 1 addressed the evolving cybercrime, background, problem statement, and purpose. The research questions, theories, definitions, assumptions, and significance of the research were aligned. Chapter 2 focused on the literary review with the wide range of diverse undertakings in the complicity of cybercrime, cyber-attacks, and cyber terrorism. It addressed the gap in the literature and viewed Kolb's experiential learning theory (ELT). Chapter 3 provided the cybercrime phenomenon through the empirical qualitative research method of Moustakas. The design encompassed purposeful sampling, data collection, and the development of the data inquiry instrument. The data analyses of van Kaam were addressed by aligning the analytical steps with ethical trustworthiness. Chapter 4 discussed the collection of the data inquiries and data analysis identifying the inductive analyses. The narrative explained how the research closed the gap between police personnel and prior cybercrime preparedness. The arrangement defined the codes, categories, patterns, segments, and strategic themes. Chapter 5 provided the discussion, recommendations, and conclusion. The findings evaluated the research questions and the outcome. The study prepared a foundation for additional research. The recommendations and strategies presented opportunities for positive social change with transferability.

References

American Psychological Association. (2019). Publication manual of the American Psychological Association (7th ed.). https://doi.org/10.1037/0000165-000

American Psychological Association. (2010). Publication manual of the American Psychological Association (6th ed.).

Baker, S., & Edwards, R. (2008). How many qualitative interviews are enough? NCRM https://howmanyqualitativeinterviewsareenough.com/15808

Barnett, M., Steingruebl, A., & Smith, B. (2011). Combating cybercrime: Principles, policies and program. http://go.microsoft.com?linkid=97

Bartunek, J. M., & Louis, M. R. (1996). Insider/Outsider team research. https://www.researchgate.net/publication/240280424_InsiderOutsider_Research_

Berg, T. (2007). The changing face of cybercrime: New internet threats create challenges to law enforcement. Michigan: United States Attorney General Eastern Michigan.

Bloom, B. S. (1956). Key to the classification of educational objectives. https://www.uky.edu/.../Bloom/Taxonomy-Educational

Bloom, B. S., Engelhart, M.D., Furst, E.J., Hill, W.H., & Krathwohl, D.R. (1966). Beyond cognitive taxonomy and educational objectives. https://www.beyond cognitive taxonomy and educational objectives

Borum, R., Felker, J., Kern, S., Dennesen, K., & Feyes, T. (2016). Strategic cyber intelligence. Information and Computer Security, (23)3. http://search.proquest.com.ezp.waldenlibrary.org/central/docview/1786145781

Brannen, J. (1982). The process of seeking help. https://www.books.google.com/books/about/process

Brinkerhoff, R.O. (2001). High impact learning: New perspectives in organizational learning. https://www.amazon.com/Impact-learning-perspective …/dp/0738205389

Brink, P. J., & Wood, M. J., (1998). The critique process: Reviewing and critiquing research. https://education.nova.edu/summer/howtoread

Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. Policing: An International Journal of Police Strategies and Management, 29(3), 408-433. https://doi:10.1108/13639510610684674

Broadhurst, R., Grabosky, P., Alazub, M., & Chon, S. (2014). Organizations and cybercrime: An analysis of the nature of groups engaged in cybercrime. International Journal of Cyber Criminology, 8(1). https:www.anu.cybercrime conservatory.

Bruner, M. (1960). Learning theory in education: Simply psychology. https://www.simplypsychology.org/bruner.html

Byrne, M. (2009). Understanding life experiences through a phenomenological approach to research. http://findarticles.com/p/articles/mi_OFSL/is.

Capelli, D., Flynn, L., Moore, A., Shimeall, T., Silowash, G. & Trzeciak, R. (2012). Common sense guide to mitigating insider threats (4th ed.). Pittsburg: Carnegie

Chabinsky, S. (2014). Wireless is not worry-less. http://intelligence.senate.gov/130312/

Chernukhin, I. (2014). New challenges to information security caused by the introduction of Wi-Fi technologies. Information & Security, (31)1, 79-86

Cilluffo, F. J., & Cardash, S. L. (2013). Cyber domain conflict in the 21st century. The Whitehead Journal of Diplomacy and International Relations, (14)1, 41-47

Clapper, J. R. (2013, March 12). Worldwide threat assessment of the US intelligence community. http://intelligence.senate.gov/130312/clapper.pdf

Clark, R.V., & Eck, J. E. (2003). Become a problem-solving crimeanalyst—In 55 steps. London: Jill Dando Institute of Crime Science.

Clark, R.V., & Newman, G. R. (2007). Terrorism and the local police. Police and the prevention of terrorism. Policing, 1(1). London: Oxford University Press.

Clinard, M. B., & Meir, R. F. (2016). Sociology of deviant behavior. https://www.amazon.com/Sociology-Deviant-Behavior...Clinard/dp/1133594158

Cross Cultural Adaption. (1976). http:www. google.com/search?q,cross

Cross Domain Solutions. (2013). Ensuring complete data security. http:www. Crossdomainsolutions.com/cyber-crime

Cybercrime Statistics (2014). Retrieved from https:www.cybercrimestatistics.com/cyber-

Cyber Disruption Response Planning Guide (2016). National Association of State Chief Information Officers. http://cyberdrpg.mi.gov

Cyber Terrorism: Preventing online assault-Is your agency's network ready to withstand cyber terrorism attacks from anonymous technology. (2014). http://policemag.com.channel/technology/articles/2014/09 Cyber-terrorism

Czescik, R., & Siemianowski, T. (2014). “Invisible” threats to the railway infrastructure-an attempted analysis. Internal Security, (6)1, 71-84 http://search.proquest.com.ezp. Waldenulibrary.org/central

Dallas Police Department (February 2012). Website Hacked. NBC Dallas-Fort Worth, Texas. http:www.nbcdfw.com/news/tech/Dallas-Police-Departments-Website-Hacked-138823209.html

Davies, C. (January 2010). Welcome to darkmarket-global one shop for cybercrime and banking fraud. The Guardian. https:www. Theguardian.com/technology/2010/jan/14/darkmarket-online-fraud-

Davis, J. T. (2010). Computer crime in North Carolina: Assessing the needs of local law enforcement. Raleigh, N.C: Governor’s Crime Commission. https:www.ncgccd.

Dawidowicz, P. (2016). Phenomenology. https://www waldenu.edu https://www.researchgate.net/.../308889486_Conceptualizing_Aligned_Story

Dempsey, J. S., & Forst, L. S. (2013). Police. Clifton Park, NY: Cengage Learning.

Denzin, N., & Lincoln, Y. S. (2008). The Sage Handbook of Qualitative Research. CA: Sage Publications.

Denzin, N., & Lincoln, Y. (2001). Interpretative Interactionism. (2nd ed.) Sage

Denzin, N., & Lincoln, Y. (1998). Strategies of qualitative inquiry. Sage Publications.

Denzin, N. K., & Lincoln, Y. S. (2011). Sage handbook of qualitative research (3rd ed.) Sage Publications.

Department of Defense. (2011). DOD strategy for operating in cyberspace. http://www.defense.gov/home/features/2011/0411

Department of Homeland Security. (2011). Fact Sheet. http://www.dhs.gov/files/prog

Department of Homeland Security. (2016). Combating cyber-crime. http://www.dhs.gov/files/programs/combating cybercrime

Derrickson, D. (1997). Informed consent to human subject research. Fordham Urban Law Journal, 25(1), 143-165. http://ir.lawnet.fordhham.edu/ulj

Devault, G. J. K. (2018). Pennsylvania superior court. Retrieved from https://law.justia.com/cases/pennsylvania/superior-court/2018/582-wda-2017.html

Dewey, J. (1938). Life and works: Theory of knowledge experience and education. https://www.iep.utm.edu/dewey

Dretzin, R., Dretzin, R., & Maggio, J. (2010). "Growing up online." MA: WGBH.

Dunlap, Dobrovolny, & Young (2008). Preparing e-learning using kolb's experiential learning. http://www.nsuworksnova edu/innovate/vol4/iss4/3

Etges, R., & Sutcliffe, E. (2008). An overview of transnational organized cyber-crime. Information Security Journal: A Global Perspective, 17(2), 87-94. https://doi:10.1080/19393550802036631

Federal Bureau of Investigation. (FBI, 2002). http://www.fbi.gov

Federal Bureau of Investigation. (FBI, 2014). http://www.fbi.gov

Fenwick, T. J. (2001). Workplace learning. https://www.onlinelibrary.wiley.com/doi/abs

Finklea, K. M., & Theohary, C. A. (2013). Cybercrime: Conceptual issues for Congress and U.S. law enforcement. Congressional Research Service Report for Congress. https:www.crs.gov/r42547

Finn, P., & Horwitz, S. (2013). U.S. charges Snowden with espionage. http://www.washingtonpost.com/world/national -security/us-charges-snowden-with-espionage/2013/o6/21/507497d8-dab1-11e2-a016-92547bf094cc-story.html

Finnie, T., Petee, T., & Jarvis, J. (2010). Future challenges of cybercrime: Proceedings of the future working group. Quantico, Virginia: Federal Bureau of Investigation.

Flory, T. A. C. (2016). Digital forensics in law enforcement: A needs based analysis of *The Journal of Digital Forensics, Security and Law.* JDFSL; Farmville, (11)1, 7-37 http://search.proquest.com.ezp.waldenulibrary.org/central

Forst, L. (2000). Handbook for police officers. Springfield, Ill: Thomas Publishers.

Forst, L. S., & Dempsey, J. S. (2013). Police. Clifton Park, NY: Cengage Publications.

Fowler, J. Experiential learning and its facilitation. https://www.researchgate.net › publication › 5962186_Experiential_learning...

Fritsch, E. J., Trulson, C. R., & Blackburn, A. G. (2014). Applied research methods in criminal justice and criminology. New York, NY: McGraw-Hill.

Furht, B., & Escalante, A. (Eds.). (2011). Handbook of data intensive computing, Springer.

Gallagher, S., & Zahiva, J. (2008). The phenomenological mind (2nd ed.). https://www.amazon.com/Phenomenological-mind-Sh-Gallagher/dp/0415610370

Gandhi, V. K. (2012). An overview study on cyber-crimes in internet. Journal of Information Engineering and Applications. (March 28, 2003). http://www.ajiste.or

Geers, K. (2010). The challenge of cyber-attack deterrence. Computer Law & Security Review, 26(3), 298-303. https://doi:10.1016/j.clsr.2010.03.003

Gercke, M. (2012). Understanding cybercrime: Phenomena, challenges and legal response. http://www.itu/ITU-cyb/cybersecurity/docs/ cybercrimelegislationEV.pdf

Gerdes, L. (2005). Opposing viewpoints: The patriot act. Greenhaven.

Giorgi, A. (2009). A descriptive phenomenological method in psychology: A modified Husserlian approach. Duquesne University Press.

Giorgi, A. (1997). The theory, practice and evaluation of the phenomenological method as a qualitative research procedure. Journal of Phenomenological Psychology, 28(2): 235–61.

Glenny, M. (2011). DarkMarket. Cyber-thieves, cyber cops and you. https://onlinelibrary.wiley.com>doi>full>j.1756-2589.2012.00138.x

Glennon, P. (2012). Data from published research. https://onlinelibrary.wiley.com>doi>full>j.1756-2589.2012.00138.x

Gonzales, J. P., Esworthy, M.A.S., & Gauger, N. J. (2016). Cases without borders: The challenges of international cybercrime investigation. http://search.proquest.com.ezp.waldenlibrary.org/central/docview/1784178560/

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. Journal of Computer Virology. DOI 10.1007/s+11416-006-005-z

Gray, K. (2015). Hacker attacks besieging Michigan computer network. The Detroit Free Press Lansing Bureau. http://freep.com/story/news/local/ /2015/02/24/michigan-computer-network-security-cyber

Grabosky, P. (2016). Cybercrime. New York, NY: Oxford University Press.

Griggs. S. Q., (2018). Experiences in the learning process. Thesis Paper. MI: State of Michigan Paper. Unpublished Thesis

Guba, E. G. & Lincoln, Y. S. (1989). Fourth generation evaluation. Sage.

Hammond, B. (2015). Cyber-security seen as common challenge among policy-makers at wsis+10 event. Cybersecurity Policy Report. http://search.proquest.com.ezp.w

Hess, K. M., Orthmann, C. H., & Cho, H. L. (2017). Criminal investigation. Cengage Publications.

Hinduja, S. (2004), Perceptions of local and state law enforcement concerning the role of computer crime investigative teams, Policing, (27)3: An International Journal of Police Strategies & Management, pp. 341-57.

Hinduja, S. (January 2007). Computer crime investigations in the United States: Leveraging knowledge from the past to address the future. International Journal of Cyber Criminology, 1(1). https:www.hinduja@fau.edu

Hinduja, S., & Schafer, J. (2009). US cybercrime units on the World Wide Web. Policing, (32)2, 278-296.

Hoepfl, M. (1997). Choosing qualitative research: A primer for technology researchers. http://scholar.lib.vt.edu/ejournals/JTE/v9nI/hoepfl.html

Holloway, T. M., &Wheeler, S. J. (1996). Revisiting qualitative inquiry. https://journals.sagepub.com/doi/abs/10.1177/136140960100600111

Holt, T. J. (2013). Examining the forces shaping cybercrime markets. https://journals.sagepub.com/doi/abs/10.1177/0894439312452998

Holt, T. J., & Bossler, A. M. (2013). "Predictors of patrol officer interest in cybercrime training and investigation in selected United States police departments," Cyberpsychology, Behavior and Social Networking, (15)9: pp. 464-473. (http://doi 10.1089/cyber.2011.0625)

Howarth, D. M. P. (July 4, 2010). Address to the third cambridge-NPIA international conference on evidence-based policing. Cambridge University

Husserl, E. (1931). Phenomenology and anthropology. https://www.scribd.com/document/.../Husserl-Phenomenology-and-Anthropolog

Husserl, E. (1965). The phenomenology of internal time consciousness, Indiana University Press.

Husserl, E. H. (1970). The crisis of European sciences and transcendental phenomenology philosophy. An introduction of phenomenological philosophy. Northwestern University Press.

Husserl, E. (1977). Phenomenology: Internet Encyclopedia of Philosophy https://www.iep.utm.edu/phenomenologpology

Inciardi, J. A. (2010). Criminal justice (9th ed.). NY: McGraw-Hill Publishers.

Ionita, M., Patriciuc, V. & Hinduja, S. (July 2016). Defending against attacks from the Dark Web using neural networks and automated malware analysis. International Journal, 14(7), 226-237

International Association of Chiefs of Police (May 2005). From hometown security to homeland security. Alexandria, VA. http://www.the iacp.org/LinkClick.aspx?ticket=78X8uKjLa0U%3D&tabid=392

Jasper , M. A. (1994). Issues in phenomenology. https://onlinelibrary.wiley.com>doi>abs>j.1365-2648.1994.+601085.x

Jeffray, C. (March 2015). The cybercrime challenge. International Cyber Policy Centre ASPI Journal. http:www.aspi.org.au

Jeffrey, A. (2011). Public-private partnerships in the fight against crime. Journal of Financial Crime (18)3, 282-291. http://search.proquest.com.ezp.

Jensen, E. T. (2012). Cyber deterrence. Emory International Law Review. Brigham Young University School of Law. http://ssrn.com

Jordan, T. (2016). A genealogy of hacking. Convergence: The International Journal Research into NewMedia Technologies. http://search.con.sagepub.com.ezp.

Kelly, J. J. III., & Almann, L. (2009). EWMDs- Electronic weapons of mass destruction. Policy Review.

Kolb, A. (2019). Eight things to know about the experiential learning cycle". Experience Based Learning Systems. https://learningfromexperience.com/themes/experiential-learning-

Kolb, D. A. (1984). Experiential learning: experience as the source of learning. https://www.researchgate.net/.../235701029_Experiential_Learning

Kolb, D. A. (2014). Experiential Learning. gmedia.pearsoncmg.com/images/9780133892

Koppel, T. (2013). An attack on the grid. https://www.usatoday.com/story/money/columnist/2016/06/..

Koppel, T. (2016). Lights out: Cyberattack, A nation unprepared. Random house.

Lang, J. M. (2014). Learning on the edge: classroom activities to promote deep learning. www.facultyfocus.com effective-teaching-strategies

Levi, M., Doig, A., Gundur, R., Wall, D., & Williams, M. (2015). The implications of economic cybercrime for policing. Cardiff University. www.cityoflondon/gov.uk/business/researchpublications

Lewin, K. (1939). Field theory and experiment in social psychology: Concept and methods. American Journal of Sociology, 44, 868-896. http://dx.doi.org/10.1086/218177

Lewis, L. H., & Williams, C. J. (1994). Experiential learning. https://www.semanticscholar.org › paper›Experiential-learning:-Past-and-pr...

Liberman, A. V. (2017). Terrorism, the internet, and propaganda: A deadly combination. Journal of National Security Law & Policy. 9(1). https://search.proquest.com.ezp.waldenulibrary.org/criminaljusticeperiodicals

Lincoln, Y. S., & Guba, E. G. (1985). Naturalistic inquiry. CA: Sage.

Long. T. M. R., (2019). Cyber, ingenuity and technology. Master Plan B Thesis Paper. MI: University of Detroit Mercy Plan B Paper. Unpublished Master Thesis

Lushbaugh, C. A., & Weston, P. B. (2016). Criminal investigation. NY: Pearson.

Lyman, M. D. (2016). Criminal investigation. NY: Pearson.

Marshall, C., & Rossman, G., (1999). Designing qualitative research. (3rd ed.). CA: Sage. https://www.worldcat.org/title/designing-qualitative-research/oclc/

Martin. L. Y., (2015). The evolving process of cybercrime. Master Plan B Thesis Paper. MI: University of Detroit Mercy Plan B Paper. Unpublished Master Thesis

Maxwell, J. (2013).Qualitative research design: An interactive approach. (3rd ed.). Sage

McCaghy, C. H., Capron, T. A., Jamieson, J. D., & Carey, S. H. (2008). (8th ed.). Deviant behavior: Crime, conflict, and interest groups. Pearson.

McCourt, M. (2014). The predictive revolution. http://search.proquest.com.ezp.waldenulibraty.org/criminaljusticeperiodicals

McCuster, R. (2006). Transnational organized cyber-crime: Distinguishing threat from reality. Crime Law Social Change, 46,257-273. DOI: 10.1007/s10611-007-9059-3

McLeod, J. (2013). Experiential learning cycle. https:// www.t/.../McLeod-2013-Experiential-learning-cycle_fig1_288004...

McMahon, R., Bressler, M.S., Bressler, L. (2016). New global cybercrime calls for high-tech cyber-cops. Journal of Legal, Ethical and Regulatory Issues, 19(1)

McMillan, J. H., & Schumacher, S. (2001). Research in education. https://www.pearson.com/us/higher-education/product/.../9780205455300.html

McMillan, J.H. & Schumacher, S. (2006). Research in education. https://www.pearson.com/us/higher-education/product/.../9780505458300.html

Microsoft Security Intelligence Report. (June 2008). Microsoft.com/download/b/2/9/b29bee13.ceca.48fo.b4ad.53cf85fe8/. Microsoft_Security_Intelligence_Report_v5.pdf.

Miles, M. B., & Huberman, A. M. (1994). Qualitative data analysis: An expanded sourcebook (2nd ed.). Sage.

Miller, L. S., Hess, K. M., & Orthmann, C.H. (2014).Community policing: Partnerships for problem solving (7th ed.). Cengage Learning Wadsworth.

Moshiri, M. (2015). 3 steps for timely cyber intrusion detection, 52(9), 60-62. http://search.proquest.com.ezp.waldenulibraty.org/criminaljusticeperiodicals

Moustakas, C. (1994). Phenomenological research methods. Sage.

Murphy, (2007). Qualitative research and evaluation methods (3rd ed.). Sage

Norman, G. (2018). Trump and the North Korea talks. https://www.nytimes.com/2018/05/24/opinion/trump-north-korea.html

Orthmann, C. H., & Hess, K. M. (2013). Criminal investigation (10th ed.). Cengage Learning Wadsworth.

Patton, M. Q. (1990). Qualitative evaluation and research methods. Sage.

Patton, M. Q. (2002). Qualitative research and evaluation methods (3rd ed.). Sage.

Pelgrin, W. (2013, May/June). Cybercrime: Threats, techniques and defenses sheriff need to know: Cyber-attacks ahead. Sheriff.

Pearson, M., & Smith, M. (2013). Feds start building case against NSA leaker. http://www.cnn.com/2013/06/10/politics/nsa-leak/index.html

Percy, M., & Caroll, I. (2015**).** Experiential learning. .bhcarroll.edu/files/session-2-toward-a-learning-century/experiential-learning.pdf

Piaget, J. (1952). Piaget's structural theory. https://thejeanpiaget.wordpress.com/schemas

Pisaric, M. (2017). Specialization of criminal justice authorities in dealing with cybercrime, Journal of Criminal Justice and Security (1)2, 230-242.

Pladna, B. (2009). The lack of attention in prevention of cyber-crime and how to improve it. East Carolina University. http://www.infosecwriters.com/cyber

Podgor, E. S. (2002). Computer crime. http://www.encyclopedia.com/topic/Computer_Crime.aspx

Police Executive Research Forum. (2014). The role of local law enforcement agencies in preventing and investigating cybercrime. Washington, D. C: PERF.

Pollock, J. M. (2007). Ethical dilemmas and decisions in criminal justice (5th ed.) Thomson.

Poonia, A. S. (2014). Cybercrime. https://www.ijettcs.org/Volume3Issue6/IJETTCS-2014-12-08-96.pdf

Quick, J., & Hall, S. (2015). Qualitative research. Retrieved from journals.sagepub.com/doi/abs/10.1177/1750458915025007-803

Ramirez, R., King, K., & Ding, L. (2016). Location! Location! Location!: Data technologies and the fourth Amendment. Criminal Justice, (30)4, 19-25 http://search.proquest.com.ezp. Waldenulibrary.org/

Roberts, J. W. (2012). Beyond learning by doing: Theoretical currents in experiential education. New York: Routledge.

Roberts, J. N., Jaeckle, T., Petee, T. A., & Jarvis, J. P. (2010). Cyber victimization. Proceedings of futures working group. Future challenges of cybercrime. Virginia: FBI Behavioral Science.

Rosenzweig, P. (2013). Thinking of cybersecurity: From cyber-crime to cyberwar-fare. Washington University Law School.

Rubin, H. J., & Rubin, I. S. (1995). Qualitative interviewing: The art of hearing data. Sage

Rudestam, K. E., & Newton, R. R. (1992). Surviving your dissertation. Sage.

Sak, A., & Burke Smalley, L. (2014). Investigation into training and evaluation. researchgate.net/.../239768250_An_investigation_relationship

Sales, N. A. (2015). Can technology prevent leaks? Journal of National Security (8)1. http://search,proquest.com.ezp. waldenulibrary,org/central

Schell, B. H., & Martin, C. (2004). Cybercrime: A reference handbook. Santa Barbara, ABC-CLIO, Inc.

Schiff, A. B. (2017). Cybercrime. https://www.library.lawsonstate.edu/eds?...Adam-Schif

Schjolberg, S. (2008). The history of global harmonization on cybercrime. http://www.cybercrimelaw.net/documents

Siegel, L. J., & Worrall, J. L. (2017). Essentials of criminal justice. (14th ed.). Cengage Learning.

Siegel, L. J., & Worrall, J. L. (2014). Introduction to criminal justice. (13th ed.). Cengage Learning Wadsworth.

Siegel, L. J., & Worrall, J. L. (2012). Introduction to criminal justice. (12th ed.). Cengage Learning Wadsworth.

Silverman, D. (2005). Doing qualitative research: A practical handbook. (2nd ed.). Sage.

Smallridge, J., Wagner, P., & Crowl, J. (2016). Understanding cyber-vigilantism: A conceptual framework. Journal of Theological & Philosophical Criminology. http:www.search.proquest,com.ezp.waldenulibrary.org/central/docview/178775

Smart, L. (May 2015). Staying safe in cyberland. CIO New York Power Authority. https://www. Scmagazine.com

Stambaugh, H., Beaupre, D., Icove, D. J., Baker, R., Cassady, W., & Williams, W. P. (2000). State and local law enforcement needs to combat electronic crime. Washington, D.C: U.S. Department of Justice, Office of Justice Programs.

Streubert, H., &Carpenter, D. **(**1999**).** Qualitative Research Humanistic Perspective (2nd ed.). Lippincott Williams

Sund, C. (2007). Towards an international road-map for cybersecurity. Online Information Review (31)5. http:www.search.proquest,com.ezp.waldenulibrary.org/central/docview

Talmadge, E. (May 2017). Experts question North Korea role in global wannnacry cyber-attack. Detroit Free Press Associated Press. Detroit, Michigan.

Tafoya, W. L. (2011). Cyber Terror. FBI Law Enforcement Bulletin (11)1-7 http:www.fbilawenforcementbulletin-2011

van Kaam, A. (1959). Phenomenal analysis: Exemplified by a study of the experience of "really feeling understood." Journal of Individual Psychology, (15)1, 66-72.

van Kaam, A. (1966). Existential foundations of psychology. Duquesne Press.

van Kaam, A. (2011). Modified van kaam analysis. http://www.phenomenologicalresearch.wordpress.com/2011/05/07/organizing

van Manen, M. (1990). Researching lived experience. www.scirp.org/(S(351jmbntvnsjt1aadkposzje))/reference

Van Voorhis, P. A., Braswell, & Lester, D. (2007). Correctional counseling and rehabilitation (6th ed.). Andersen.

Walker, S. & Katz., C. M. (2013). The police in America. McGraw-Hill:

Wall, D. (2008). Cybercrime, media and insecurity: the shaping of public perceptions of cybercrime. International Review of Law Computers & Technology, 22(1-2), 45-63 https//doi: 10.1080/13600860801924907

Wall, D., & Williams (2007). Policing diversity in the digital age. Criminology and Criminal Justice. 7(4), 391-415.

Wall, D. S. (2011). Policing cybercrimes: Situating the public police in networks of security within cyberspace. http://ssm.com/abstract=853225

Waters, N., & Doll, Y. (2012). Time to assign a law enforcement agency exclusively to combat terrorism. Journal of Law Enforcement, 2(5). www.jghcs.info

Weiss, R. S. (1994). Learning from strangers: The art and method of qualitative interviewing. Free Press.

Wexler, C. (2014). Cybercrime: A new critical issue. Critical issues in policing series: The role of local law enforcement in preventing and investigating cybercrime. Washington, D. C: Police Executive Research Forum.

Zahiva, D. (2003). Philosophical issues. (http:// www.https:psycnet.apa.orgrecord)

Appendix A: Demographics

DEMOGRAPHIC INFORMATION FORM

EVOLVING CYBERCRIME LAW ENFORCEMENT PERSONNEL PREPAREDNESS

Please Enter on Line: **Job Title**: _____

Position: _____

Please Mark, Underline, or Check One ALL Pertinent Data on Each Line:

1} EMPLOYMENT OR VOLUNTEERISM: 2 Months-1 Yr 1 Yr-3 Yrs 3 Years +

2} GENDER: Male Female Other LGBTQ N/A

3} AGE: 18-30 31-43 44-56 57 +

4} EDUCATION: GED/HS Associate Degree Bachelor Degree Graduate Degree

5} POLICE AGENCY: Rural Township City Urban County Tribunal

State Medical Education Facility Other (List)_____

6} TELEPHONE NUMBER: (Optional) _____

7} ALTERNATE # CELL: (Optional) _____

8} EMAIL: (Required)_____

[Note: You can set up a free temporary email (gmail, hot mail, yahoo, aol) for additional anonymity to submit your data]

9} TYPES OF CYBERCRIME TRAINING/PREPAREDNESS (Circle as many as apply):

Instructor/Trainer **DVD** **CD** **Video** **GOOGLE** **College/Training Site**

On-the-Job-Training (OJT) **You Tube** **Twitter** **ZOOM** **On-Line**

Internet/YouTube **Self-Taught/Experience**

OTHER COMMENTS: _____

****

Confidential Form with the Option to Exit at any time!

Police personnel may exit at any time of their own volition without negative repercussions.

Please send Email results to XXXXXXX@xxx.xxx; Call for any additional information @ 2X1.XXX.XXXX

Ic-xxevx.2021- Walden's IRB [Date: XXXX'].
IRB Code: [Walden University]

Appendix B: Data Inquiry

DATA INQUIRY COLLECTION FORM

CYBERCRIME AND POLICE PERSONNEL PARTICIPANT

INSTRUCTIONS: Each of the ten (10) data collection open-ended inquiries and comments will be answered by police personnel with your ideas, thoughts, perspectives, and opinions and emailed to the researcher. [Replies are confidential and password protected].

1.. What are your perceptions, perspectives, and thoughts regarding your previous cybercrime training and preparedness?

2. In what ways was the cybercrime (fraud, bullying, thefts, contraband, human trafficking) preparation meaningful, relevant, and interesting?

Meaningful-(important/understood)

Relevant-(consistent/pertinent)

Interesting-(exciting/pleasurable)

3. How did other computer training experiences assist you in the cybercrime police personnel experiential learning?

4. What geographical locations, sites, cities, or states did you receive your cybercrime training and preparedness?

5. How did you apply your cybercrime preparedness and learning in a pragmatic manner at the workplace or community?

6. Can you list several ways you believe cybercrime training and preparedness can be enhanced?

7.. In what ways have you applied cybercrime training, learning, and preparedness in positive ways in the workplace?

8..What are your recommendations to better equip police personnel to combat (fight) and mitigate (reduce) cybercrime?

9..What methods and/or strategies do you believe can assist in uprooting (eliminating) the prevailing cyber-attacks, cybercrime, and cyber-terrorism?

10.. List any other cybercrime law enforcement police personnel preparedness, training, or procedures you believe will assist in fighting, mitigating, or eliminating cybercrime.

Send email results to XXXX.XX; Call for additional information @ XX.3XX.XXX

Walden's IRB [Date: XXXX]
Idt.05.04..2021.ho.ps
Conditional IRB Code

Appendix C: Request Letter

September 03, 20XX

Chief of Police
Police Department
City, Michigan

RE: REQUEST LETTER OF COOPERATION FOR PARTICIPATION IN DOCTORAL RESEARCH

Dear Chief ,

I am requesting a **"Letter of Cooperation"** submitted to my email from the XXXXXX Police Department to perform my doctoral research. I am a Ph.D. candidate currently completing my doctoral degree at Walden University in Public Policy and Administration. The title of my dissertation is ***"The* Evolving *Challenges, Issues of Cybercrime, Law Enforcement Personnel Preparedness and Training in Michigan."*** It is an empirical phenomenological qualitative dissertation with a concentration in *Terrorism, Mediation, and Peace.*

I am the researcher, Eileen V Martin, a retired 30-year urban police sergeant, trainer, researcher, and developer. I currently serve as an adjunct college/university professor and senior pastor. I am requesting a "**Letter of Cooperation or Approval**" to enlist voluntary police personnel from your police department to participate in my research. After I receive the l**etter of approval or cooperation,** I will submit a copy to Walden University Institutional Review Board (IRB) for full approval to begin my research.

I will enlist one or two police personnel volunteers, who have worked with cybercrime or identity-theft preparedness or training**.** Neither the police agency nor the participants will be identified in the research study. **I ensure the utmost ethical confidentiality, anonymity, and integrity.** I am requesting your contact telephone number and email address to submit the documents that will be distributed to the police personnel.

I am aware this is a highly difficult time due to the Coronavirus (COVID-19). My prayers are with you. The research is remote with no face-to-face contact. The participants will express their thoughts, ideas, perceptions, and perspectives regarding cybercrime and training via email or other electronic devices. The agency and volunteers can exit at any time. **All data is anonymous and confidential**. The data collection will be placed in a lockbox (I am the only one with the combination). I will personally destroy all stored documents, research items, and drives within five years.

I am thanking you in advance. I appreciate your leadership and cooperation. The study will evoke evidence-based research regarding police personnel's cybercrime preparedness and social change with transferability. If there are any questions, please email me at **XXX.@xxxxx or call 3XX-3X2- Thank you.**

Respectively yours,

Eileen V. Martin
XXX.X78-3XX-XXXX…….
XX1-5XX-7XXXX …… (cell)
xxxxxx……..@xxxxxx.xxx

Attachments: Informed Consent/Demographics/Data Inquiry
[Walden's IRB [Date:XXX]
Idt.05.04.2021.ho.ps

Appendix D: Sample Letter of Cooperation

"Potential Approval Notification"
"Please Submit on Police Department Letterhead"

XXXXXXXX Police Department

To: Researcher Eileen V Martin
…….@xxx.com

Dear Ms. Martin,

The Approval Notification Cooperation Letter provides permission for the researcher, Eileen V Martin, to conduct the Walden University doctoral research. We have assigned a designated contact person, Designee ----------, who will provide a list of potentially qualified law enforcement personnel. The research is titled *"The Evolving Challenges, Issues of Cybercrime, Law Enforcement Personnel Preparedness and Training in Michigan."* The study is virtual-remote with no face-to-face interactions.

The police personnel volunteer at their own discretion. The participants will submit **"*I Accept*"** to my email or another electronic device after reading and agreeing with the *Informed Consent*. The volunteers will fill out the *Demographics Information Form* and the one-time *Data Inquiry Collection Form* (10 inquiries). All completed data is emailed to the researcher. The law enforcement agency and participants reserve the right to withdraw from the study at any time.

The law enforcement agency and personnel remain anonymous with confidentiality and will not be identified in the research.

Best Regards,

Authorization Official Signature
Title/Agency Information
Re: Study-Walden University

Appendix E: Debriefing

DEBRIEFING

I personally thank you for your excellence in participating in this cybercrime preparedness/training law enforcement research project. The study would not have been possible without your active participation and valuable time. The knowledge you provided addressed a gap in the literature. The results enhanced the understanding of police preparedness and the cybercrime phenomenon with strategies to combat, mitigate, and uproot cybercrime, cyber-attacks, and cyber terrorism and bring positive social change. I thank you for your wisdom, willingness, and knowledge actively consenting to volunteer for the study.

Please feel free to contact me if you have any questions or comments.

Note: I will send you a one to two-page summary of the final research results if you request when the research study is complete.

Once again with sincere appreciation ……. Thank You!

Eileen V Martin XXXXXXxxx @xxxxxx XXX,XX7-XXXX XXX.XXXXXX

Integrity is of the Essence

dc-r.2021-Idt.05.04..2021.ho.ps
Walden's IRB [Date: 2020]

Appendix F: Copyright Permission

REQUEST KOLB'S COPYRIGHT WAIVER FOR MY DOCTORAL DISSERTATION

Sun, Jan 20, 20xx 8:32 pm

XXXXXX(xxxxxxxx@xxxxxx.xxx)

XXX,XXXX(xxxxxxx@xxxmail.xxx)To:you

Hello,

You are welcome to cite the references, but I would suggest you cite the revised book, David Kolb's Experiential Learning: Experience as the source of learning and development.

Use Person, 2015 instead of 1984 version.

Let me know if you have any questions.

Best,

XXXX XXXX Ph.D.

Executive President

XXXXXXX.XXXX.XXX, Inc.

www.xxxxxxxxxxxxxxx.xxxx

phone: XXX-XXX-XXXX

The xxxx.xxxxxxxxxxx Inventory xxxxxxx are available at:

xxxxxxxxxx.xxxxxxx.xxxxxxxxx.XXXXX

XXXX & XXXX*: XXXXXXXXX and XXXXXXXXXX.*XXXXX, HX

XXXX PressXXXX

Vita Mini Resume

VITA OF DR. EILEEN VICTORIA MARTIN

Walden U: Ph.D.-Public Policy& Administration-Concentration-Terrorism, Mediation & Peace

Current: Full-time Senior Pastor & Presiding Archbishop of International Pentecostal Diocese. Serving as an Adjunct Professor, Instructor, Key Speaker, and Visiting Professor

Active Positions: [Adjunct Professor Since 1974 -48 yrs] - Serving @ 12 different Colleges & Universities Visiting Professor @ Oxford University, UK: "Proactive Measures to Threat of Terrorism." Disciplines taught: **Law Enforcement Administration, Corrections, Criminal Justice, Psychology, Business Administration, Public Administration, Philosophy, Counseling, Mental Health, HUS, Religion, and Human Interactions.**

Additional Instructions: Stress Management, Public Safety, Adm, Mgt, Supervision, & Criminal Investigation.

Current: Law Enforcement Police & Public Safety Consultant–Four Diverse Michigan & Ohio Law Enforcement and Public Safety Departments …Since 2001
Establishes creative and innovative processing to secure, combat, mitigate, uproot, and prevent potential challenges. Serves as skillful scientific law enforcement, quality management, and technical engineer to plan, orchestrate, instruct, train, assess, and evaluate. Align and articulate operations to manifest productive and positive social change in leadership incorporating community policing, public safety, and proactive tactics.

Archbishop (Hooded 2005)	Presiding Archbishop of Int'l Pentecostal Diocese Overseer of 112 Int'l Worldwide Pentecostal Churches	Since-2005
President & Chancellor	Christian Theological Seminary CEO & Instructional Professor	Since 1988
Bishop (Hooded 1998)	Trainer/Developer-Nevis St. Kitts-West Indies, Amedjofe, Accra Ghana, Liberia, Kwanta, W Africa, South Africa, Sierra Leone, Canada, Jamaica UK-England, Israel, USA & Carribean Islands	
Board of Directors Chair	Domestic Violence (501 c-3) Chair & President DV Agency & Shelter/Human Trafficking	Since 1992
National Certified Counselor	Counseling PTSD Military Veterans/Marriage-Family Group Adults & Children (NCC)	Since 1985
Senior Pastor & Founder	CVFG International Cathedral Church [40 years]	Since 08/1981

Previous Employment and Positions/Entrepreneurship/Appointed Positions/Political Run

Ran for Detroit Mayor - (Mayoral Candidate) **City of Detroit, Michigan in 2001**
Interim International Official – (West Africa) **Temporary Appointed Position**
Urban Police Department-Sworn Police Officer, Investigator, and Sergeant [30 years]
[7 yrs on Patrol & 23 yrs @ Police Training Academy/Trainer-Developer/Researcher -LEIN Administrator]
Principal & Founder–CVC Academy (Private Christian School-Kdg to 12th Grade) 1990-2000.-.10 years
Current & Previous College/University-Adjunct Professor, Workshop Admin-Instructor, & Key Speaker
[Positions-Mg College, NYU, MSU, WMU, OU, U of M, UD, WSU, FSU, WCCC, WCCCD, Union Institute]
Security PI Firm Entrepreneurship–Served as CEO-Security Officer, Mgr. & Administrator-Since 1998
Martin Christian Designs-CEO & Founder-Entrepreneur/Fashion Designer/Tailor Shoppe/Interior Designer
Active Board of Directors President and Board Member - 30 yrs-Profit & Not for Profit Businesses
(President/Vice President-Private and Public Policy Administrator/Executive Project Manager/Grant Writer)

Vita-Mini Resume

COMPLETED 14 EARNED DEGREES: [15th Degree (5th Doctorate) @ Walden University, PhD Candidate]

Public Policy Administration-{Terrorism, Mediation & Peace} Public Policy Admin/Empirical Qualitative Phenomenological Dissertation- Evolving Challenges, Issues of Cybercrime, Law Enforcement Personnel Preparedness, and Training in Michigan

PhD Candidate	Doctorate in Public Policy & Administration	WU-Projected Completion Date	2022
Master of Philosophy	Public Policy Administration.	Walden University	2020
PhD	Doctorate in Psychology	Kennedy-Western University	2004
D Min	Doctor of Ministry	Union Theological	2002
Ed D	Education: Curriculum Design	Berne University International	1999
PhD	International Government	Berne University International	1998
M.A.	Religious Studies/Psychology	Berne University International	1997
MPA	Master in Public Administration	Western Michigan University	1994
Ed S.	Gerontology (Psych of the Aged)	Wayne State University	1984
Ed S. Degree	Counseling Psychology (Specialist)	University of Detroit	1981
M.A. Degree	Master of Arts (Criminal Justice)	University of Detroit	1980
MCS. Degree	Master of Correctional Science	University of Detroit	1979
B.A. Degree	Sociology/Minor in Psychology	Wayne State University	1977
A.A.S. Degree	Dental Laboratory Technology	Ferris State University	1969
A.A. Degree	Nursing-St of MI-Licensed B [LPN]	Michigan School of Practical Nursing	

Workshops, Conferences, Training, Virtual Instructions, Seminars, and CJ Classroom Management Techniques

The management and techniques are implemented to improve course quality and coordinate cohesive collaborative unity with applied actions to equip learning, critical thinking, and experiential learning for excellence. Pragmatic applications enhance the theoretical components of various Criminal Justice, Law Enforcement Administration, and Corrections court cases intertwined with current events to enlarge learning. Information is aligned with enhanced quintessential practical criminal justice components. Critical interactive classroom skills, techniques, and field trips result in high-level course retention with skills and successful insight in achieving course goals. Students understand the critical interactions of observations and procedures with strategies allowing participants to set goals, and values, and develop short and long-range plans anticipating the unexpected. Classroom management provides information regarding Mental Health and positive family interactions. Stress Awareness and Management with PTSD proactive measures and effective group interactions assist in activating critical thinking. Productive endeavors for empowerment engage enhancement skills for administrators, managers, supervisors, and instructors. Positive revisions are extended for growth and development during experiential learning and teaching. Field trips bridge the theoretical and pragmatic gap for participants in all instructional segments. Opportunities are provided for the Questions and Answers (Q & A) to further expand and encapsulate skills, techniques, strategies, progress, and life's plethora of expeditious achievements.

Vita-Mini Resume

Workshops, Conferences, Training, Virtual Instructions, & Seminars presented during the last four years

Coronavirus (COVID-19) & Pandemic Attacks
Synaptic Integration and Memory
Understanding the Misconceptions of Science
Challenges of Teaching
Human Trafficking
Public Safety & Comprehension of the Universe
The Learning Brain
Children & Learning Teamwork
Early Childhood Talent Developmental Process
Values & Goals Improvement
OSHA and Public Safety
Strategies for Challenges & Disasters
Homeland Security & Departmental Policies
Sexual Harassment & EEOC
FBI and Cybercrime Policies
Social Problems & L.E. Structure
Counseling and Communication Techniques
Criminal Justice & Reform
Cruel & Unusual Behavior & Empirical Research
Psychology of Performance
Cognitive Youth Behavioral Therapy
Advanced Positive Psychology
Critical Thinking Skills
Challenges & Conflict Mgt as an Educator
Secrets in Learning & Art of Teaching
Effective Child Communication
Cognitive Coding and Counseling Therapy
Stylistic Images & Networks
Hidden Meanings & Complexities
Analysis of Intellectual Adventures
Powerful Life Lessons
Assess, Analyze & Achieve
Elements in Exploring New Perspectives
Forensic History-Crimes & Frauds
Understanding Genetics
Increased Security in Corrections
Philosophy of Theology
Philosophy of Remote and Virtual Learning
Biblical Hebrew & How We Learn
Public Health & the Urban Community
CBRN & Scientific Techniques
Kolb's Experiential Learning
Developing Internal Motivation & Counseling
Focused Attention Development
Concepts of Computer Science
Tai Chi and Mental & Physical Flow
Burnout & Need for Recovery
Retention of Students
Domestic Terrorism
Proactive Domestic Violence Strategies
Demographic Diversity
Youth Disaster Preparedness
Quest to Explain Reality
Immigration Law
Fundamentals of Great Professors
Tai and Qigong Strategies
Stress and Coping Methods
Education in Innovative CJ Engineering Fitness
How to Read & Understand
Old Testament and New Testament
Discovering Innovative Learning Techniques
Ethics in Teaching Children
Fundamentals of Machine Learning
Understanding Biblical Wisdom Literature
Rebuilding Dynamics
Engaging Rich Empowerment
Ancient Judaism & Roots of Jesus
Magnificent Riveting Revelations
Evaluate Evidence
Science and Technology Investigations
Public Safety Safeguards
Dependable Performance

Key Speaker: Prior Achievements, Workshops, Seminars, Inspirational Speaker-[USA & Int'l Global Leadership]

Trainer & Development/Instructor/Project Manager-MI State Law Enforcement Training Interim Dean-Marygrove College & University of Michigan-Rackham (Detroit)
Public Safety, Security, and Interactive Policing-St. Kitts-Nevis, W Indies, Kwanta, Accra Amedjofe, Ghana, Liberia-West Africa U K-England-South America-"Proactive Measures to the Threat of Terrorism"
Orchestrating Knowledge with Excellence/Consultant-Auto-ethnography and Phenomenology
Qualitative Evidence-Based Research in CJ, LEA Adm., & Corrections Strategic Framework in Criminal Investigation & Federal Investigative Agencies-Public Safety/Policing/Investigation
Prevention and Proactive Actions for Domestic Violence, Human Trafficking, and Child Abuse
Complexity of Evidence and Investigation of Terrorist -Inextricably Activities with Police Intelligence and Technological Intelligentsia-(Interconnectivity with the blueprint of Kolb's Experiential Learning Theory)

Vita-Mini Resume

VITA OF EILEEN VICTORIA MARTIN **2022** **4 of 4**

STATE OF MICHIGAN LICENSES & INTERNATIONAL AWARDS, CERTIFICATIONS, ORDINATIONS, HOODINGS, PLAQUES, AND HONORS

MI State Licensed Residential Builder-[Professional Corporations, Securities & Commercial Licensing] #2102128327/Bonded & Licensed Since 1995

National Certified Counselor Certification (NCC) & NBCC-National Board for Certified Counselors, Inc. (Worldwide) Since 1985 #16691

Michigan State Law Enforcement Coordinated Collaborative Training @ MSU

FBI Academy Certifications [24 hour/40 hour/80 hour Training] Quantico, Virginia

Special Congressional Recognition for Law Enforcement Washington, D.C.

Spirit of Detroit Awards 1998, 2003, 2012

Heritage Registration of Who's Who Certificates & Plaques 2007-2008

National Institute of Health (NIH) Training-"Protecting Human Research Participants" Certification #2503826/09.20.2017

U S Dept of Justice -Law Enforcement Domestic Violence-Child Abuse Certification…….....2002

Michigan State Licensed Real Estate Sales Agent……..Since 1978

Ordained as an International Minister of God under the Auspices of the Pentecostal Diocese 04/1974

Active Boards and Executive Committees (Chancellor/Chair/Vice President):

Women's Dedicated Palace (WDP) Detroit Christian P Fellowship & Bible Ins/Sem EVM, Inc

Women's Coalition CC MCD .Liv in Faith Effectively (LIFE) Counseling Ctr LRG, Inc

FHP Academy JBP Publications DR EVM P.I., Inc. DCPFI CVC Academy

LIFETIME MEMBERSHIPS: Tae Kwon Do NAACP Women's NAFE

CVFGIC, Inc. Women in LEA WMU FHPA, Inc

Alumni Memberships: FSU Alumni U of DM Alumni WSU Alumni WMU Alumni

National Society of Leadership and Success (NSLS)

References: Supplied upon request: Mini-Resume- WU-VITA.DREVM.-04.08.2022