2021

Security Awareness Strategies Used in the Prevention of Cybercrimes by Cybercriminals

Pascal Pouani Tientcheu
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Pascal Pouani Tientcheu

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. Gail Miles, Committee Chairperson, Information Technology Faculty
Dr. Jodine Burchell, Committee Member, Information Technology Faculty
Dr. Bob Duhainy, University Reviewer, Information Technology Faculty

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

Walden University
2021

Abstract

Security Awareness Strategies Used in the Prevention of Cybercrimes by Cybercriminals

by

Pascal Pouani Tientcheu

MS, American Public University System, 2013

BS, Columbia Southern University, 2011

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

August 2021

Abstract

Cybercrime is a growing phenomenon that impacts many lives worldwide. Businesses, organizations, and governments continue to search for ways to protect their data and intellectual property from cybercrimes. Grounded in the routine activity theory, the purpose of this general qualitative study was to explore strategies information security officers used to prevent cybercrimes. The participants included seven information security officers listed on social media who manage information security within organizations located in the northeast geographic region of the United States. Data were collected using semistructured interviews, the National Institute of Standards and Technology documentations and analyzed using thematic analysis. Four key themes emerged from the analysis: policies to prevent cybercrimes, cybersecurity response plan, cybersecurity awareness as a culture, and train end-users/employees. The key recommendation is that IT professionals work closely with other IT professionals, experts, and engineers to create relevant cybersecurity policies through compliance, develop efficient cybersecurity response plans, develop a culture of cybersecurity awareness, and implement cybersecurity training programs. The implications for positive social change include the potential for cybercrime crime reduction and a change of people's perceptions and knowledge of cybercrime threats in their communities, neighborhoods, and organizations.

Security Awareness Strategies Used in the Prevention of Cybercrimes by Cybercriminals

by

Pascal Pouani Tientcheu

MS, American Public University System, 2013

BS, Columbia Southern University, 2011

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

August 2021

Dedication

This study is a huge accomplishment that I dedicate to my Lord Jesus Christ who is my Savior and Redeemer. I would not forget my late father Tientcheu Joseph, my Mother Heuleu Marie Thérèse, my wife and my three kids. I was inspired by the encouragement of my parents and their profound desire to giving me a better education, so I become an example of inspiration in the family and I thank them for all the sacrifices consented in that regard.

I also would not forget the seven participants of this study and my classmates.

Acknowledgments

My acknowledgments go directly to Dr. Gail Miles, Dr. Jodine Burchell, and Dr. Bob Duhainy, who have served on my doctoral committee, and Jenny Martel. I have a special thanks to my Chair and Mentor Dr. Miles that I admire a lot for her dedication and hard work. I'm very grateful for all the assistance and support she provided to me in the achievement of my doctoral study.

I also would like to take this opportunity to thank Walden University and all the staff included all the instructors that have made my dream possible. I appreciate the education that I have received from that institution, which will benefit me in my future professional career.

Table of Contents

List of Tables

Section 1: Foundation of the Study

Background of the Problem

Cybercrime is one of the recurrent crimes perpetrated online. The social, economic, and security impacts of the phenomenon are enormous. Organizations are increasingly becoming victims of cybercrime and looking for effective means of preventing and managing cyber threats and cybercrimes (Enigbokan & Ajayi, 2017). However, the lack of knowledge regarding the cybercrime phenomenon impacts decisions to prevent these activities (Nallaperumal, 2018). Preventing cybercrimes depends on strengthening the individual protection mechanism by regularly updating computer systems, protecting systems with high antivirus, and implementing a strong password policy (N. Goyal & D. Goyal, 2017). Although those measures are efficient regarding the prevention of cybercrimes, it is essential to develop a culture of vigilance in terms of the understanding of the cybercrime phenomenon and the learning best security practices, which are part of the key factors in the prevention of cyberattacks. Researching and developing countermeasures is a constant need for organizations to protect sensitive data from getting infected from unauthorized sources (Khan & Hasan, 2017). States must prepare for new threats in cyberspace through actions taken by the highest authorities, central administrative bodies, state audit organizations, security formations, as well as within the scientific and research environment (Babinski, 2015). Globally, the need for implementing successful security awareness strategies to prevent cybercrimes is the fundamental reason for this study.

Problem Statement

For the last decade, cybercrime has become the primary concern of governments worldwide (Y. Nawafleh et al., 2016). However, cybersecurity awareness culture is still in its infancy, and the subject's knowledge is not bounded and defined (Gcaza et al., 2017). According to Harrison and Jürjens (2017), an average of 23.66% of organizations classified in three economic branches, respectively known as the Bank, Automobile, and FinTech startup suffer a lack of security awareness training initiatives. The general IT problem is the lack of successful security awareness strategies to prevent cybercrimes by employees. The specific IT problem is that some information security officers lack security awareness strategies to prevent cybercrimes by cybercriminals.

Purpose Statement

The purpose of this general qualitative design study was to address strategies used for security awareness by information security officers in the prevention of cybercrimes by cybercriminals. The population was information security officers who are currently in charge of managing information security within their organizations and located on the northeast coast of the United Stated of America, listed on social media such as LinkedIn and Facebook. The implications for positive social change include the potential to develop a culture of prevention based on knowledge of cybersecurity awareness. In addition, implementing a strategic plan to prevent cybercrimes may contribute to users' understanding of cybercrimes and increase vigilance when exposed to the internet and social media.

Nature of the Study

Qualitative research was the research method chosen for this study. Qualitative research is a systematic and subjective approach to highlighting and explaining daily life experiences and giving them proper meaning (Mohajan, 2018). Qualitative research helps describe a process and experience, and the goal is to make meaning of experiences or phenomena by following data as they emerge (Cruz & Tantia, 2017). Qualitative research was appropriate because I studied IT professional experiences, which helped me understand the strategies to prevent end-users from being exposed to cybercrimes as part of my research topic. According to Goertzen (2017), quantitative research methods collect and analyze data that is structured and can be represented numerically, contributing to building accurate and reliable measurements that allow for statistical analysis.

Quantitative research was not appropriate for this study because it involves statistical tests, and I am not collecting quantifiable data. The mixed-methods methodology allows the convergence of both quantitative and qualitative research phases (Yapıcıoğlu & Kaptan, 2017). The mixed-method methodology was not appropriate for this study because it would require combining qualitative and quantitative methods, which is not consistent with this research approach. A general qualitative design study is the research design chosen for this study. Among the existing research designs, there is phenomenological, ethnography, and narrative. Phenomenological research is the study of experiences from the first-person perspective (Spaulding, 2015). This design method was not appropriate for this study because lived experiences are not the focus. The

ethnography design uses observations to study people and cultures and helps develop a practice to bring about that knowledge according to certain methodological principles (Howell, 2017). Ethnography was not appropriate for this study because it does not study the culture of a particular group in the research. The narrative design seeks to understand and interpret, focus on the specific story, and use the story as the anchor of analysis (Bruce et al., 2016). The narrative design was not appropriate for this study because it does not encourage participants to share their stories. A multiple case study examines many cases to understand the differences and similarities (Neubert, 2016). A multiple case study was not appropriate for this study because it has many constraints in reaching out to participants within organizations to collect data needed for a study.

A general qualitative design study was the most appropriate research design for this study because it allows the comprehension of a complex social phenomenon that enables participants to bring their real-life experience to explain and overcome that issue. In addition, Levitt et al. (2018) suggested that a general qualitative design study tends to engage data sets in intensive analyses, to value open-ended discovery rather than verification of hypotheses, to emphasize specific histories or settings in which experiences occur rather than expect findings to endure across all contexts, and to recursively combine inquiry with methods that require researchers' self-examination about their influence upon research process.

Research Question

What strategies for security awareness do information security officers use in the prevention of cybercrimes by cybercriminals?

Interview Questions

Here below are the relevant interview questions of this research topic:

1. What do you do when your organization is the victim of a cyberattack?
2. What policies do you have to avoid a cyberattack?
3. What strategies does your organization use for security awareness?
4. What strategies do you use to prevent cybercrimes?
5. Who within your organization is more exposed to cyberattacks and why?
6. What types of cyberattacks do employees of your organization face daily?
7. What are the frequencies of cyberattacks in your organization?
8. What are the economic impacts of cybercrimes on your organization?
9. What are the categories of information targeted by cybercriminals?
10. What sensitive information is more targeted by cybercriminals?

Conceptual Framework

The routine activities theory (RAT) was used as the conceptual framework for this study. Cohen and Felson developed the RAT in 1979, which is used as the foundation of many criminological theories. RAT clearly explains how and why crime occurs. Over time, RAT was used to explain changes in criminal tendencies and prevent and reduce crimes. Moreover, RAT explains the victimization of individuals through their way of behaving that makes them the potential victims of cybercrimes. Boetig (2006) extended research on the RAT by explaining the variation of crime rate due to people and their social interaction, such as employment, recreation, educational endeavors, and leisure activities. The author also explains the type of population that may be more exposed to

cybercrimes. Marcum (2009) used the RAT to address protective measures to take against victimization to improve guardianship. The RAT theory was advanced with the cyber lifestyle-RAT developed by Reyns et al. (2011). The authors explain that the factors of time and space are no longer relevant to measure the degree of the risk exposure of the targets towards motivated offenders in contrast with the traditional idea of victims and offenders in real-time and physical space. RAT has been used to explain Cybercrime at the individual level (Kigerl, 2012). One of the best ways to address the rationale behind any crime is evoking the RAT. That is the primary justification of the choice of the RAT as the conceptual framework for my research topic.

RAT contributes to the evolution of social crime prevention. Cybercriminals use the vulnerabilities of their victims to perpetrate their crimes. Cybercrimes are related to the spatial and temporal disconnect between the theories and the cyber environment (Vakhitova et al., 2016). Using RAT to address cybercrimes will help information security officers to develop successful security awareness approaches to help end-users, who are commonly viewed as the targets. It additionally helps to identify threats coming from the internet and social media to prepare to prevent cybercrimes. RAT is chosen in this study to address the threats of cybercrimes on employees that suffer from a lack of security awareness plans, which is also used to identify security awareness plans in the prevention of cybercrimes.

Operational Definitions

Below are definitions of relevant terms in my research study:

Cybercrime: Cybercrime is generally defined as any criminal act in which a perpetrator breaks or hacks into a computer or computer network to illegally obtain sensitive information or disseminate destructive computer software (Gupta & Mata-Toledo, 2016).

Cybercriminals: Cybercriminals are people who seek financial profit by stealing and selling information via different methods (Sabillon et al., 2019).

Cybersecurity: Cybersecurity is the process of preventing unauthorized access, modification, misuse, or denial of use (Lechner, 2017).

DDoS: A DDoS attack attempts to make a target computer or server unavailable to its intended users by preventing the target from functioning. During a DDOS attack, the attacker(s) generates many connection attempts directed at the target's IP address or addresses (Wong, 2016).

Information security: Information security is defined as protecting information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability (Nieles et al., 2017).

Security awareness: Security awareness is a continual process of learning by which trainees realize the importance of information security issues, the security level required by the organization, and individuals' security duties (Al-Daeef et al., 2017).

Threat: Threat is a circumstance or event that has or indicates the potential to exploit vulnerabilities and negatively impact organizational operations, organizational assets, individuals, other organizations, or society (Lechner, 2017).

Victimization: According to Spalek (2016), victimization is the process of being victimized. To victimize is to treat someone in an intentionally unjust way.

Vulnerability: Vulnerability is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source (Lechner, 2017).

Assumptions, Limitations, and Delimitations

Assumptions

An assumption in research is an accepted theory that you use to base your research on, which can also be used to build your model, theory, and/or test your hypotheses (Rahbek, 2018). I assume that all the participants in the interview process provided accurate responses to all the questions that I addressed to them relative to my research topic. I was truthful by reporting what was said during the interview process to tackle all the strategies that an information security officer (ISO) needs to implement to prevent cybercrimes.

Limitations

Limitations of a study are influences that could affect results but cannot be controlled by the researcher (Marshall & Rossman, 2016). For example, in this study, the geographic area has been limited to the northeast coast of the United States of America. The budget is one factor that has led to the study limitation in collecting interview feedback to support my research study. Another limitation is the number of participants part of the interview process, which could have been extended to have more feedback regarding the research questions.

Delimitations

Delimitations of a study are those characteristics that limit the scope of the study by the conscious exclusionary and inclusionary decisions made during the development of the study (Simon & Goes, 2013). They are defined as features that bind the scope and define the study's boundaries and include the choice of objectives, the research questions, variables of interest, theoretical perspectives that we choose to implement, and the population to be investigated. For example, this study does not have a global overview of the geographic area of the study. Instead, participants are selected in a specific geographic area, and their roles are related to their competencies relative to the studied topic. That allows the focus on a group of participants that helped to support my research topic. Besides, the delimitation facilitated a better face-to-face interview with the selected participants.

Significance of the Study

Contribution to Information Technology Practice

The impact of cybercrimes in terms of business financial losses and national security threats is high. Therefore, it is vital to create an awareness culture as part of the best practices for understanding cybercrimes that spread quickly and negatively impact people, organizations, businesses, and governments worldwide. Security awareness considerably affects perceived severity, response efficacy, self-efficacy, and response cost (Hanus & Wu, 2016). The significance of this study for IT practice may be the awareness of end-users about the risks encountered when they are exposed to cybercrimes and to offer successful strategies to prevent such crimes. The current study

will study security awareness plans that may support culture to positively affect the impact of cybercrimes by making uses aware in terms of the seriousness and understanding of the causes, consequences, and operation mode of such phenomenon. Confident users perceive less cybercriminal risk, highlighting the importance of end-user education (Riek et al., 2016).

Implications for Social Change

With the increase of cybercrimes, individuals, organizations, businesses, and governments are seeking relevant and efficient solutions to prevent or fight against their data being compromised. The repercussion of this study in terms of positive social change may increase people's awareness about protecting themselves when they use the internet and social media platforms. Moreover, the study may help organizations improve moral and financial prejudices linked to cyberattacks. The study may also help identify best practices for cybersecurity awareness that are essential to safeguard personal data and prevent cybercrimes in the long run. Social technologies related to user awareness contribute significantly to preventing victimization, and social networking services should provide appropriate controls to protect individual information (Saridakis et al., 2016).

A Review of the Professional and Academic Literature

Cybercrimes have always fascinated researchers and brought their attention to the methods used by cybercriminals to perpetrate their crimes by analyzing the real motivation behind their behaviors and actions. Wiley et al. (2020) suggested that a better understanding of the employees' information security awareness and contributing factors

is essential in mitigating information security risks. Therefore, I organized this literature review content to reflect different aspects of my research topic to speak about strategies to prevent cybercrimes.

This study aims to effectively address security awareness strategies that information security officers use to prevent cybercrimes by cybercriminals. RAT is the conceptual framework of my research study. Routine activity theorists see the simple presence in proximity to the potential target as crucial prevention. Cyberspace is supplied with physical or technological guardians, automated agents that exercise permanent awareness. RAT's concept of capable guardianship is similar to cyberspace (Yar, 2005).

I collected sources and relevant information from Walden Library, Google Scholar, ProQuest, and EBSCO for this literature review. I gathered 252 sources, with 94% (236 articles) peer-reviewed and 95% (232 articles) less than five years from their publication until the estimated graduation date. I used Walden Library, Google search, ProQuest, and EBSCO tools to filter articles based on their titles, publication dates, subject areas, or center of interest. Finally, all selected peer-reviewed articles were verified through the Ulrichsweb Global Serials Directory website.

The routine activity theory is the conceptual framework for this study. The exposure and unguarded information over the internet has led to deviant behaviors by cybercriminals who have walked away from societal norms and laws, which have made it difficult to investigate and prosecute the authors. Intrusion detection systems such as capturing the user's facial image and biometric fingers provide real-time evidence for people in charge of enforcing laws and cybercriminal persecutors (Agana & Wario,

2018). RAT assumed that motivated offenders are present and focus instead on suitable targets and guardianship measures. Because of this focus, routine activities theory is well-suited for preventing property crime (Argun & Dağlar, 2016). Moreover, RAT is a valuable instrument to evaluate problems linked to crimes, including crime opportunities in people's daily activities (Argun & Dağlar, 2016). I grouped the gathered sources in criteria based-contexts that help understand the RAT, the evolution of the theory, and the convergences and divergence points, including criticism points and contrasting theories in relationship with cybercrimes and strategic preventions of such phenomenon.

Routine Activity Theory

Cohen and Felson developed RAT in 1979, which became the foundation of many criminological theories. RAT is based on three elements determining a crime situation: a motivated offender, a suitable target, and the absence of a capable guardian. Even if the explanation of a crime, in this case, is perpetrated physically, the same crime approach can be committed in the same way online using a computer. The motivation of the offender, the suitable target, and the absence of a guardian describe the three fundamental elements behind a crime situation (Cohen & Felson, 1979). The combination of the mentioned three elements is necessary for a crime to occur. Moir et al. (2018) stated that personal and situational characteristics influence how and when people provide guardianship over where they live.

The Evolution of the RAT

RAT has evolved with the progress of technologies that shifted the traditional crime territories to virtual territories, especially with the development of the Internet and

social networks. Researchers focus more on guardianship victimization, which is the inability of a victim to make a rational decision regarding his protection against cyberattacks. Guardianship focuses on any careless control over potential victims (Reynald et al., 2018). Offline guardianship is a crucial element against online victimization along with individuals' online routine activities (Reyns et al., 2016a). Schaefer and Mazerolle (2017) suggested a different vision of the RAT that offers a perspective focused on crime events rather than criminal propensities, which has evolved to provide practical solutions to crime problems. Reyns and Scherer (2018) used the routine activity perspective and incorporated measures of disability to examine the underexplored relationship between disability status and stalking victimization and suggested that measurements of disability should be incorporated into future research testing the routine activities perspective for interpersonal victimization.

Stephan et al. (2016) viewed positive social change as a process that is proactively initiated, multilevel in nature, and includes bottom-up dynamics. Besides, change in its social and economic structure opens more doors for offenders to perpetrate crimes of different forms (Argun & Dağlar, 2016). Brady et al. (2016) expanded core elements of Cohen and Felson's well-known work by focusing on technological, social changes that occurred with the development and commercialization of the Internet and reported that the number of adult Internet users in the United States increased from 14% in 1995 to 87% in 2014, with nearly 71% connected to the Internet in the daily basis, which has increased criminal activities over time by limiting the guardianship. Finally, Tyler (2018) suggested that RAT can be justified in preventing breaches of patient data in

the security of electronic medical records by creating awareness, which is the foundation for positive social change in implementing electronic health record cloud security. Besides, many kinds of research claimed that the discouragement of a criminal event today does nothing to reduce the likelihood that the offender will commit a similar crime at another time and place. As the argument goes, guardianship moves crime from one area to another (Argun & Dağlar, 2016).

Property crime includes the offenses of burglary, larceny-theft, motor vehicle theft, and arson. Faraji et al. (2018) suggested that the presence of a shelter appears to cause property crime to increase by 56% within 100m of that shelter, with thefts from motor vehicles, other thefts, and vandalism driving the increase. Additionally, the increasing and decreasing of property crime in the surrounding community is consistent with a causal effect relative to the distance from the shelter (Faraji et al., 2018). Argun and Dağlar (2016) explained the applicability of RAT in the prevention and reduction of property crimes in the context of some parameters related to burglary and auto theft incidents in the United States. They suggested that RAT may be used as a valuable tool by crime reduction or prevention practitioners to evaluate crime problems and take routine precautions and measures to reduce crime opportunities in people's daily activities. Leung et al. (2018) investigated crime related to hotels. They considered that hotel guests generated a higher fear of crime when the crime occurred inside guest rooms, especially in cases of burglary, theft, or fraud. To reduce fraud they suggested: (a) proper training of the staff, (b) guest education about credit card deposit policy, (c) counsel to

guests never to give personal information over the phone, and (d) the request of identification for all transactions on property.

Chetty et al. (2018) defined digital literacy as a set of basic skills required for working with digital media, information processing, and retrieval. Digital literacy also allows social networks to create and share knowledge and supports a wide range of professional computing skills. Additionally, digital literacy provides an individual with core capabilities to achieve valued outputs in life (Chetty et al., 2018). Graham and Triplett (2017), utilizing RAT, explored the role of digital literacy, a measure of guardianship, in the reception of a response to phishing. They found that digital literacy significantly affected phishing response and that it significantly affects the receipt and response to phishing victimization.

Digital forensics is forensic science used for digital crimes and attacks (Prasanthi et al., 2017). The emerging technologies increased the challenges in incident handling and digital forensics to provide effective guardianship. Alex and Kishore (2017) suggested that digital forensics viewed as applied science contributes to identifying an incident, collecting, examining, and analyzing evidence data. Neuner et al. (2016) indicated that the digital forensics process could be improved by automating related data analysis processes.

Deviant behavior is a social and psychological phenomenon that includes socially unacceptable behavior from an ethical point of view (Salakhova et al., 2016). Shoaib and Baruch (2019) suggested that the relationship between employee deviant behavior likelihood and affection for incentives in a moderated mediation framework of incentives

may have significant contributions towards the present literature of deviant behavior and incentives and encourage managers, academicians, and policymakers to reduce adverse behavior in professional employees through proper use of incentives. Ireland (2020) suggested that using privacy-enhancing technologies and techniques as a form of individual target hardening behavior may guide motivated offenders to target hardening behaviors, such as using two-factor authentication and antivirus software.

Drawve et al. (2017) applied RAT to examine whether measures of offender motivation, target suitability, and guardianship influence the likelihood of an offender's arrest in incidents of aggravated assault. Petrescu et al. (2018) suggested that the influence of proximity to motivated offenders, target suitability, and capable guardianship on consumers' attitudes and perceived subjective norms towards online software piracy is relevant to a perspective situational analysis of the routine activity related to the crime to individual offending and a broad range of deviant behaviors. Choi and Lee (2017) suggested that cyber interpersonal violence offending can be handling by educating on the potential hazards and stimulating more responsible online activity and engagement. In summary, the history of the RAT shows that the theory has evolved, and many researchers' works have demonstrated its relevance to support cybercrimes linked to lifestyle, deviant behavior, digital-capable guardianship, digital forensics, and digital literacy.

Analysis of Similar Theories

The history of RAT shows that they are convergences among thinkers in how they perceived a crime situation, which is the result of the victimization and the product of factors such as social life and the social environments.

Lifestyle and Routine Activities Theory (LRAT)

The theory perceives victimization the same way through the motivation of the offender, the attracted target, and the absence of capable guardianship. LRAT is described as an opportunity model of victimization in which motivated offenders and suitable targets converge in the absence of adult supervisors or capable guardians (Cho et al., 2017). Reyns et al. (2016) suggested that online lifestyles influence the theorized cycle of online victimization and preventative efforts. After examining the causes of cybercrime victimization through the prism of LRAT, Vakhitova et al. (2016), motivated offender and LRAT's exposure to risk and proximity to offenders reflect the offender's role in the crime event model. Therefore, the probability of being victimized is higher when it comes to the LRAT. RAT and LRAT are applied to analyze youth victimization and vulnerability by showing how there are more exposed than protected, especially for those engaged in risky behaviors such as coming home late, drinking alcohol, etc.

The RAT motivated offender, and the LRAT exposure to risk and proximity to offenders reflect the offender's role in the crime event model (Vakhitova et al., 2016). Singh and Bakar (2019) suggested that emerging technology impacts the cybercrime equation and crime catalyst in cyberspace due to its nature and characteristic, which conform to dynamic spatiotemporal coupled with identity flexibility, anonymity, and lack

of avoidance. Additionally, RAT takes on the assumption of time and space. The theorist argued that as long as the offender and the victim are within distances, and there is no guardian authority, crime will occur (Singh & Bakar, 2019). Thus, RAT provides a simple and powerful insight into the causes of crime problems (Argun & Dağlar, 2016). Wachs et al. (2020) addressed RAT by investigating a crime through the exposure of the victim to motivated offenders, capable guardianship, and target suitability, which might predict cyber grooming victimization among related victims. This theory remains one of the leading theoretical approaches in criminology and has garnered significant scientific support.

Lai et al. (2017) investigated the levels and determinants of residence-based fear of crime across three racial/ethnic groups-Whites, African Americans and non-White Hispanics by drawing upon routine activities theory and addressed the fact that proximity to motivated offenders measured by perception of crime was found to be the most salient predictor of fear, followed by the measures of target vulnerability and capable guardianship. Cho et al. (2017) indicated that the exposure of students and proximity to motivated offenders, school environment, capable guardianship, and target attractiveness is associated with the risk of peer victimization and reveals that risk factors varied depending on the type of victimization. The convergence points of the RAT with LRAT are emphasized on multiple vulnerabilities linked to race and ethnicity that may motive offenders to commit a crime in the absence of guardianship.

Crime Opportunity Theory (COT)

Dijk (1994) helped formulate the COT as crimes that are not premeditated by the offender but rely on circumstances that may contribute to a crime occurrence and suggested that offenders choose the targets based on the compensation, effort, and effort, and risk factors. Thus, two things should occur for a crime opportunity to happen: the presence of at least one motivated offender who is ready to engage in a crime and the environmental crime opportunity. For the COT, crime is conditioned by a motivated offender but not sufficient to justify the commission of a crime because of the environment in which the crime is perpetrated.

Crime opportunity occurs with the ability of the offender to benefit from the crime as part of daily routine activities. Beck and Hopkins (2017) suggested that crime opportunity theory is made on rationality regarding the choice of the offender's decision about a crime opportunity presented to him. Zabyelina (2017) suggested that the presence of a motivated offender is a necessary element for the commission of an offense but not a sufficient one. There has to be an opportunity for crime in the environment in which that offender is located.

Crime opportunity theory was not chosen for this study because it does not explain the reason behind a crime sufficiently.

Situational Crime Prevention Theory (SCPT)

SCPT theory expands the reduction of the crime perspective beyond the justice system. Anandarajan and Malik (2018) suggested situational crime prevention theory offers a theoretical perspective for organizing the dimensions or indices used to analyze

security vulnerabilities and risks of victimization from Cybercrime in public access Internet facilities. However, situational crime prevention theory was not chosen for this study. It does not explain the motivation to commit a crime but instead tries to explain the conditions and circumstances that create the opportunity to commit a crime (Anandarajan & Malik, 2018).

Preventing criminal activity requires changing the environment to increase the efforts and risks involved in committing a crime, reducing the compensations an offender expects to gain from the crime, and making an attack difficult for criminals to justify their activities using common explanations (Anandarajan & Malik, 2018). The situational crime prevention framework provides a mechanism for operatively analyzing specific situations to design and implement prevention methods. It explores crime settings so that opportunities can be designed to deflect offenders and raise the perceived risks of being caught (Tunley et al., 2018). Borrion and Dehghanniri (2019) suggested that crime prevention works by varying potential offenders' judgments of risk and compensation. Drew and Farrell (2018) suggested that by analyzing situational crime prevention application of the 25 situational crime prevention techniques to reduce cyberstalking victimization, there was potential to reduce victimization risk by taking a victim focus to cybercrime prevention, particularly target hardening strategies. SCPT was not chosen for this study because it could not reduce vulnerabilities in an existing environment, especially when dealing with cybercrimes.

Analysis of Contrasting Theories

RAT and LRAT have some points of convergence but differ in how they view the behaviors that contribute to the creation of risk for victimization. For example, RAT focuses on describing the events' victimization, whereas the LRAT considers victimization in terms of risk probability for a crime to occur (Pratt & Turanovic, 2016). Reyns et al. (2016b) utilized the LRAT perspective to identify risk factors for victimization and gender-based theoretical models estimated to assess the possible moderating effects of gender on the relationship between lifestyle-routine activity concepts and victimization risk. I did not choose LRAT as the conceptual framework for this study because it views behavior as a significant risk for victimization even if the RAT and LRAT address crime in the same way.

Situational Opportunity Theories of Crime (SOTOC)

In contrast with LRAT, SOTOC examines situational opportunities that explain the process of offending. Wilcox and Cullen (2018) suggested that SOTOC can be linked with victimization among different groups of people and showed gradually that delinquent lifestyles are among the riskiest related to the victimization of younger people. They also suggested that exposure to offenders via unsafe activities in environments with poor or absent guardianship has contributed to rising victimization risks. SOTOC has gained popularity in criminological research, which has also impacted crime opportunities. For example, Cohen and Felson (1979) used situational opportunity to explain white-collar crimes. However, a situational opportunity theory of crime was not

chosen for this study because it is not practical to prevent crimes, especially when dealing with committed offenders.

Rational Choice Theory (RCT)

RCT theory has been part of various criminological theories and used calculations to rational choices to achieve self-objectives. Paternoster et al. (2017) suggested that criminologists recognize the RCT theory, implying that offending is based upon a self-interested estimation of the costs and benefits of alternative courses of action. The action taken is viewed as the one with the most significant perceived utility. Van Wegberg et al. (2017) suggested that crime and punishment need to be analyzed based on individual cost and benefits for the economics of organized crimes, which is alarming compared to the growing amount of economic studies on individual crime and criminal laws also linked to cybercrimes. RCT was not chosen for this study because it involved clear decision-making from the criminal when deciding to commit a crime, not allied with the RAT/LRAT concepts.

Criticism of RAT

One of the major arguments used in the criticism of RAT questions is its efficacy, moral and political legitimacy, and tendency to blame the victim. Crime in general and routine activity theory, in particular, have been attacked by authors. De Waal et al. (2018) stated that authors have theorized that patients susceptible to criticism may avoid relationships with individuals prone to violent behavior. Besides, the relationship between some disease's symptoms, such as borderline personality disorder and experiences of violent victimization, is fully regulated by emotion regulation difficulties,

which increases patients' vulnerability to violent victimization, and patients who find it challenging to regulate intense emotional experiences may be more prone to risky behaviors and involvement in abusive relationships (De Waal et al., 2018). RAT may have a limitation when it comes to the perception of the promotion of guardianship. Choi et al. (2016a) argued that there is a limitation in terms of the arrest authority from law enforcement but acknowledge the importance of the promotion of guardianship around the health and safety concern. The view of RAT and the officer's perception regarding the promotion of guardianship and reduction target suitability of young people are most at risk for bullying victimization. Although there is some criticism of the RAT, RAT is a good foundation for studying successful strategies for preventing cybercrimes through security awareness training programs. RAT works when used to explain more crime prevalence for certain groups, including certain types of crime that occur more often.

RAT and Security Awareness Best Practices

Ghazvini and Shukur (2018) suggested that training programs enhance employees' awareness of information security and attempt to raise employees' awareness of information security and help them adhere to appropriate behaviors that do not compromise the security of information assets and with long-run impact. The security awareness training programs helped businesses and employees so that they can gain an understanding of potential cyber hazards, as well as mitigating strategies available for self and business protection (Ghafir et al., 2018). Security Education, Training, and Awareness (SETA) play a considerable role in preventing cybercrime. Yaokumah et al.

(2019) suggested that SETA enhances security behavior and prepares employees for a more mediating role in monitoring and accountability.

Education and awareness have played a considerable role in dealing with insider threats and preventing future threats from happening within organizations. Vasileiou and Furnell (2019) outlined that the percentage of outsider attacks is higher than insider attacks. Awareness, training, and education would contribute in the information of employees about the importance of security and its application in the daily operation of an organization, which can be achieved by recalling the information provided, remembering organizational security, and be conscious of this security as they deal with vital information as they carry out their daily responsibilities in their place of work. Besides, tailoring awareness program is an efficient way to manage and deal with insider threats that face organizations by considering that each employee is an individual with a different personality that needs to be taking into account when it comes to compliance to cybersecurity policies and the customization of any related security education, training, and awareness program (Vasileiou & Furnell, 2019). The primary approach to tailoring is personalization. Tailoring awareness will allow a better design of specific security awareness programs applied to individuals based on their field of responsibility, including the type of information security system they are managing. For example, a security awareness program designed for individuals with a security clearance will differ from individuals without security clearance. Tailoring would also help develop my research question by focusing on interview questions specifically related to my research

topic. There is a certainty to have clear participant feedback during the interview process by considering their IT profile in the field.

The sophistication and organization of cybercrimes today have led to the use of the RAT by including the suitability of target and motivation behind Cybercrime for creating a unified framework used to develop appropriate laws and policies to effectively organize cybercrime regulation and legislation (Schreck, 2017). Hui et al. (2017) suggested that governments should be more proactive to discourage potential attackers from entering a hacking career by enforcing the convention on Cybercrime on deterring distributed denial of service (DDoS) attack because cybercriminals are more and more rational and strategic in the way they operate. Mittal and Sharma (2017) suggested that applicable laws and conflicting jurisdiction that impact the cybercrime fight can be handled by regulating the structural design of the internet through special laws of cyberspace.

The collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, assurance, and technologies are used to protect the cyber environment and organization and user's assets, which will protect the information in terms of its confidentiality, integrity, and availability (Seissa et al., 2017). Besides, Seissa et al. (2017) suggested as best security awareness practices the importance of motivating staff to be more inclined to participate in security policies; upgrading employees' cybersecurity skills; allowing employees to be aware of their role in preventing and reducing cyber threats; enforcing information security management system that addresses people, processes, and technologies to minimize cyber intrusion

incidences as well as government guidelines and mandates for system security. Butt et al. (2020) estimated that organizations and the systems involved in online activities need security measures to protect integrity and availability, which will help avoid any malfunctioning to their operations due to the cyberattacks; building mutual trust with people online is essential to keep a safe online environment. Srivastava et al. (2020) suggested that policymakers should focus on challenging cybersecurity aspects such as the legal, technical, organizational, and soft aspects such as the training and co-operational to reduce cybercrime incidences within a nation.

RAT to evaluate Cybercrime

RAT could be used to evaluate cybercrimes**.** Researchers have tried to assess crime theory by using simulation models. Chastain et al. (2016) suggested that criminologists have found that most offenders are motivated to commit crimes close to their homes, with the average crime trip ranging only in the short range from 0.5 to 2 miles from home. The developed Journey to Crime (JTC) model to simulate burglary crimes JTC offered insights into offender motivation and the location of the offense, which contribute to the explanation of the target interest for residential burglary regarding the expansion of guardianship into the larger geographical space of a neighborhood when examining residential burglary routine activity, and social disorganization theories. Chen et al. (2017) suggested that threat appraisal comprises the outcomes of risk-taking, including perceptions of vulnerability, severity, and the rewards of risky behavior. Chen et al. (2017) suggested that threat appraisal comprises the outcomes of risk-taking, including perceptions of vulnerability, severity, and the rewards of risky behavior.

Cybercrime against an individual, individual property, society, private organization, and government are the five types of Cybercrime perpetrated today. The consequences of such phenomenon are the loss of revenue, the waste of time to detect the crime, the damaged reputations, and the reduction of the productivity for companies, the influence of cyber terrorism that impact the economy of nations (Malik & Younis, 2016).

Cybercriminals, over time, have developed cyberbullying. Cyberbullying occurs over digital devices like cell phones, computers, and tablets and can happen through SMS, Text, and apps, or online in social media, forums, or gaming where people can view, participate in, and participate in or share content. Routine activity theory is used to address cyberbullying within the social networking sites (SNS) by reviewing the activities within the SNS that contribute to any risk of experiencing cyberbullying (Navarro et al., 2017). Corcoran et al. (2016) suggested that the application of routine activity theory allows understanding the geography of crime related to fire events and the fact that it incites through behavioral regularities. However, Leukfeldt and Yar (2016) identified 11 eleven studies that use RAT to explain victimization in cybercrimes. The studies show different outcomes when it comes to using RAT for cybercrimes, making it difficult to estimate the value of RAT in explaining Cybercrime. N. Goyal and D. Goyal (2017) suggested that cybercrimes result from the vulnerabilities of the computing systems and tied the theories for crime preventions to the motivation behind criminal tendency to commit a crime by two factors by referring to the internet and the computer.

Cyber fraud is any crime that is committed with the use of a computer or computer data. They represent one of the significant aspects of cybercrimes. The

emotional and sociodemographic characteristics of cybercrime are associated with routine activities, and younger people are more likely to engage in routine activities that potentially expose them to cyber-frauds. In contrast, older people are more likely to engage in online guardianship behaviors, and there is some advantage in considering whether personal dispositions predict cyber-fraud victimhood (Whitty, 2019). Liao et al. (2017) suggested that law enforcement agencies and legislative bodies should evaluate their current practices to reduce social justice, which is facilitated by information technology, and denounced the computer-assisted frauds that are victims a lot of people and organizations by pointing the importance of the legislation to enforce any law toward convicted offenders. Computer frauds are predictable as IT systems become increasingly complex and globally interconnected. Hackers will target websites or critical infrastructure to create service disruption and downtime, with associated financial and reputational costs (Urquhart & McAuley, 2018).

Privacy Behaviors and Confidentiality

Privacy is about protecting the right from unauthorized intrusion that contributes to the measurement of privacy protection behaviors. The protection of citizen privacy in the investigation and prosecution of Cybercrime is a big concern since the right to privacy is protected under many national constitutions and is also an element of various legal traditions (Ngo & Jaishankar, 2017).

RAT suggested that deviant behavior occurs in the presence of three elements linked to a suitable target, a lack of a suitable guardian and a motivated offender (Argun & Dağlar, 2016). Opening emails from unknown resources can lead users to access

websites that are not safe and may see their computers infected with malicious codes (Chen et al., 2017). The use of phishing emails by cybercriminals allows for personal and sensitive information, which are substantial online privacy concerns (Kumar et al., 2016). By using a structural equation modeling on data room based on a survey of 11534 internet users from different races and ages, Chen et al. (2017) showed that 87% of the respondents reported having installed protection software on their laptops or computers due to internet scams as part of online privacy and the privacy protection behaviors. The innovative conceptual model suggested that the fight against Cybercrime can take signs from health behavior studies indicating the role of perceptions and beliefs in reducing online threats (Dodel & Mesch, 2017). Fear and awareness of crime influence perceptions of risk that constrain behavior and redirect from risky routine activities online (Williams et al., 2019).

End-user behavior is relevant to privacy behaviors and confidentiality. Alohali et al. (2018) suggested that a complex password is the most common protection used by end-users to access systems and data. Poor password behavior could be caused by the lack of user knowledge and motivation. The study found that personality traits do play a significant role in affecting users' security behavior risk levels, which may link to their offline personality, especially in the conscientiousness personality trait and from the attacking perspective, social engineering is a simple yet effective attack that is widely used to obtain end-users information, such as login credentials. Short passwords can be cracked easily by attackers using pre-computing rainbow tables (Mun et al., 2018). As noted by these researchers, the effectiveness of a strong password to protect against

attacks is linked to computer infiltration. It highlights the importance for an organization to have strong password policies to avoid end-user behavior when choosing their passwords and providing any training in that regard.

Violence Victimization

Many researchers have evaluated the influence of routine activities on the likelihood of online victimization, and research indicates that those individuals who spend more time online, employ the Internet for a broader range of economic-related and social activities, and engage in cyber deviance are more likely to experience online victimization (Nedelec, 2018). Research on online victimization about gender shows some inconsistency. According to Poster (2018), women in the United States are 26% more likely exposed to identity theft than men. Räsänen et al. (2016) suggested that gender is a significant factor in offline and online victimization. However, the relationship between gender and victimization might vary depending on the type of hate for which the respondent was targeted. Choi et al. (2016a) suggested that bullying victimization reflects the RAT because of the person's motivation to commit a crime with the absence of guardianship and physical surveillance, metal detectors, and security officers influence bullying victimization. DeLiema (2017) viewed RAT as a model for elder financial victimization and affirmed that 46% of fraud victims and 56% of financial exploitation victim are female between 83 and 84 years old based on data abstract from 53 Forensic Center elder mistreatment cases drawn from a pool of 924 cases presented between March 2006 and August 2013. Violence victimization could be very costly for

victims without guardianship, especially female elder populations that seem more exposed to financial fraud than other targeted populations.

Online identity theft, consumer fraud, and phishing are some of the victimization types facing people today. Cyber-harassment and cyber-impersonation are two forms of action that characterize cyber-interpersonal violence victimization. Respondents who engage in risky online leisure activities are more likely to experience interpersonal violence in cyberspace, interpersonal violence on social networking sites due to poor online security management, and the perpetration of cyber-interpersonal due to the risk of engagement in social networking site activities (Choi & Lee, 2017). Reyns et al. (2019) examined the fact that online harassment, hacking, identity theft, and receiving nude photos or explicit content are four types of crime victimization experiences and found that low self-control is linked to a primary type of cybercrime victimization, which make difficult the appreciation of any nature of Cybercrime. Applying RAT decreases the risk of cyber victimization (Wick et al., 2017). Besides, Wick et al. (2017) affirmed that harassment victimization is higher for females than males based on an anonymous online survey taken by 298 undergraduate students. However, online exposure was predictive of more experiences of being victimized by cyber harassment, particularly for women. De Letter et al. (2017) suggested based on an online survey on 886 participants that sexual harassment victimization and general harassment victimization are strongly associated with the determinants such as guardianship and target suitability likely exposed to sexual harassment than men. Cybercriminals can use online identity theft to harass or cause harm to their victims by targeting them.

Näsi et al. (2017) suggested the applicability of the RAT in online harassment victimization of people aged 15 to 30 years in the USA, Finland, Germany, and the UK even if the victimization may occur despite the lack of any physical face to face contact. The analysis of different samples showed that 19%t of respondents reported having been victims of online harassment. In contrast, 17% of the Americans, 19 % of Germans, and 15% percent of British respondents reported being victims and showed that the likelihood of the harassment victimization rate varies from one country to another. The cyber-victimization literature tends to focus on the proximities, available barriers, or guardians, and contexts in which Cybercrime occurs. This accent leaves a gap in the conceptualization and modeling of behaviors to prevent cyber victimization (Dodel & Mesch, 2017). This summary provides a clear explanation of the probability of being victimized online when living in a specific area of the world and targets a fringe of the population within a certain age that is likely exposed to online harassment. These topics are essential to understand the necessity to start educating people at an early age about the risks they may face when they are connected online.

Financial losses resulting from cybercrimes are enormous. Chaudhry (2017) suggested that the billion-dollar internet ad business with double-digit growth has attracted cybercriminals who can earn illicit ad revenue in basically two ways and digital thieves and the Hijacking of the Online Ad Business, “experts estimate that $209 million internet ad revenue was derived from the 589 illicit sites”. Youth victimization through online hate is one the preoccupation of researchers.

Online hate is widespread online and redirected towards communities based on race, religion, ethnicity, sexual orientation, disability, gender, and culture. Among online hate crimes, hate speech online is more common, in which the purpose is to attack a person, or a group based on the mentioned criteria. Räsänen et al. (2016) suggested that online hate has increased by the internet that exposes hate material such as text, image, video, music toward some collective, which might be applied to both predatory street crimes as well as to crimes occurring in cyberspace in terms of the hate victimization. Besides, Räsänen et al. (2016) indicated that the risk of online hate victimization among youth fluent in information and communication technology is higher when they are concerned about possible online victimization. Social media is the platform that allows the development and the increase of racial hate crime (Chan et al. (2016); Silva et al. (2016)). Online hate has always been used to victimize and justify a crime without any guardianship. Therefore, there is a need to have clear regulations because it promotes the fear, intimidation, and harassment of persons, which is also a severe violation of human dignity that may cause depression in concerned victims. Statistically, victimization crime is associated with criminal offending based on multiple variable contexts. It is in part attenuated by factors such as low self-control, depression, and how time is spent (Reisig & Holtfreter, 2018). Leukfeldt and Yar (2016) suggested that RAT fundamentally explains victimization by how someone is a suitable target for a motivated offender in behaviors that may increase the exposure of motivated offender and appropriate target, including any likelihood victimization. These studies provide an understanding of cyber victimization that targets young people of certain ages and addresses the responsibility of

parents in the control and the regulation of young people's behaviors so they don't become the next victims of cybercrimes.

End-users Exposure to Cyberattacks by Cybercriminals

Krasznay and Hámornik (2018) estimated that people in charge of cyber defense could not define predictable rules from past events than developed attack strategies and tools linked to the development of new technologies. Therefore, countermeasures must be emphasized by combining traditional security approaches using rules and known patterns with machine learning to prevent cyberattacks by cybercriminals. Research from IBM and Google suggested that the most sophisticated hacking groups operate with a top-down organizational structure featuring a CEO-like leader who broadly defines the organization's goals and turns much of the detailed work over to a layer of middle management. Krasznay and Hámornik (2018) suggested that cybercriminals build on end-users 'ignorance when they target them by considering that they do not understand the cyberspace world. Yeboah-ofori et al. (2018) estimated that cybercriminals in their need cause harm and may disrupt services either for fame, revenge, political motive, economic war, cyber terrorism, and cyberwar. Law and legislative framework may address the Jurisdictional issues posed by the development of the internet and the council's treatment of the jurisdictional conflicts that underline cybercrime rules.

Park et al. (2019) suggested that cybercriminal activities are contingent upon socioeconomic factors, connection speed, and Cybercrime requires a skilled perpetrator and infrastructure that will motivate a crime situation. The fact to target non-executive staff within the wealth chain, whether a broker or admin assistant, with a malicious email

or similar, cybercriminals can potentially gain access to a server and, by extension, millions of pounds worth of financial data. Kocsis and Palermo (2016) believed that criminal profiling has steadily increased over the past five decades throughout the world and suggested that behavioral crime analysis is supported by the profiler validity research and could be regarded as potentially admissible expert witness evidence, which is surprisingly compatible with the extant legal principles.

Ongoing digitalization has contributed to increasing the perpetuation of Cybercrime. Dimitriadis et al. (2020) estimated the lack of cybersecurity as the major obstacle to digitalization and believe that cyberattacks, which are imperative threats to intelligent manufacturing systems, need to be considered very seriously by every company. According to Moir et al. (2018), personal and situational characteristics influence how and when residents provide guardianship over where they live. Digitalization has opened the door to cybercrimes and allowed cybercriminals to use sophisticated technologies to target their victims.

Ransomware is another operation mode used by cybercriminals to perpetrate cybercrimes by asking for a ransom. Ransomware allows cybercriminals to withhold relevant data from users' computers and companies’ computers until they paid a ransom with relative ease and anonymity. Two hundred nine million dollars was collected within the first few months of 2016 due to ransomware (Choi et al., 2016b). Police are also the victims of ransomware. On February 25, 2016, an email was sent to every member of the police department. Once a department member opened the email, the ransomware began encrypting files in the police department’s network. It seized complete control over one

of the signature pieces of software, TriTech, which constrained the police to pay a ransom to get their files decrypted (Choi et al., 2016b). Ransomware provides the sophistication of the method used by cybercriminals to cause economic harm to organizations, which may be very costly in terms of finances. Understanding the damage of ransomware contributes to waking up organizations on how they should protect their data and communicate on the issue with their employers to detect better and prevent such economic crimes that may impact business continuity.

In 2015, the internet crime complaints center estimated that they had collected 288,012 complaints with a global financial loss of $1,070,711,552 (Levi, 2017). Furthermore, Hawdon et al. (2017) estimated based on the analysis of four datasets of youth and youth-adult relative to the predictors of exposure to online hate materials in Finland, Germany, the United Kingdom, and the United States, that 53% of respondents report being exposed to hate material, while 48% of Finns, 39% of Brits, and 31% of Germans are exposed to these materials, explaining that some countries are more exposed to online hate materials than other. In that regard, Americans have nearly a 23% higher chance of being exposed to online hate materials.

White-collar crime is another phenomenon that exists in our society. Simpson (2019) suggested that white-collar is either a corporate crime or crimes by businesses. Gottschalk (2017) estimated that profit-driven crime linked to favorable economic situation is behind the white-collar crime and suggested that white-collar crime is usually not offenses of passion, unstructured or emotional, but calculated risks for a convenient solution to a challenge or problem by rational actors. Payne et al. (2019) suggested that

not all cybercrimes are white-collar crimes; however, it is not clear the degree to which white-collar crimes comprise all forms of cybercrimes; few studies have considered cybercrime solely as a form of white-collar crime. White-collar crimes are not violent but are financially motivated to cause harm to a person of particular esteem.

Strategies in the Prevention of Cybercrimes

Cybersecurity Awareness Program. Security awareness is an essential part of the fighting and prevention of cybercrimes. Edwards et al. (2016) suggested that the frequency of data breaches has increased over time and continues to expose the personal information of hundreds of millions of people. Wiley et al. (2020) suggested that organizations should focus on security culture rather than organizational culture to improve information security awareness and save times and resources, which depend on the importance of leaders in the encouragement of positive security behaviors through strategic management and planning, communication, and transparent decision-making processes. Sabillon et al. (2019) estimated that a cybersecurity awareness program must include adequate training aligned with the organization's objectives and long-term investment to help create a cybersecurity culture if training is delivered continuously. Security awareness training programs' success depends on how it is delivered. The security awareness approach may differ from one country to another. Tambo and Adama (2017) estimated that 11 out of 54 African countries had taken concrete actions essential in preventing and countermeasures against cybercrimes by implementing laws and regulations about cybersecurity.

Moreover, the continent has seen cybercrimes and mobile money fraud increase significantly over time due to the absence of laws and regulations in that regard and by the rise of the internet penetrations that have to contribute to enormous financial losses in terms of cyberattacks for countries like South Africa, Morocco, and Uganda. In that regard, the need to increase cybersecurity capabilities and cooperation by investing in building safe, reliable, and persistent cyberspace decision making platforms and frameworks and release cybersecurity leadership role and commitment is essential to create cybersecurity and operating platform of all stakeholders that includes Microsoft Google, Apple, Facebook, Banks, governments, and others private sectors on cyberattacks incidents that affect the local and global market and share losses (Bouveret, 2019). Furthermore, the cybercrimes can be reduced by building public and community cybersecurity communication and engagement resilience, readiness, and capability to promote public and community cybersecurity and cyber-wellness policy and capabilities, awareness campaigns, meeting, and empowerment.

Person-centered Information Security Awareness (PCISA). PCSISA is helpful to maintain information security and protect data assets for organizations. Ki-Aries and Faily (2017) suggested the PCISA contributes to the identification of the audience needs and security risks and enables a tailored approach to business-specific awareness activities, which contributes to the reduction of information security risks through security and allows a better adaptation to the time and resource needed for its implementation within the organization. Information security can be maintained by building a security-conscious culture, providing end-user training to reinforce security

awareness, developing proper guidelines for disposal of storage media, performing audit security systems regularly and testing staff, and developing procedures that will help to report an incident.

Policies and Procedures. With the rise of cybercrime activities, the adoption of policies and procedures becomes relevant in fighting and preventing such a phenomenon. Aldawood and Skinner (2019) suggested that policies and procedures play a huge role in the security awareness education training by demonstrating the ability of the organization to provide training to employees through a general session on security awareness for all the new employees by focusing on commitment to ethical business behavior. Kayser et al. (2019) suggested the importance of having solid policies and procedures related to cybercrime protection and the necessity of working with private and government to ensure that human rights standards will be applied in the cyberspace environment. Addressing any change in policies and procedures and intensive training for specific employees for areas of responsibility is helpful to refresh from time-to-time exposed employees of the organization by explaining any committed crimes and monitoring and reporting them (Aldawood & Skinner, 2019).

Cyber Detection. Daily routines characteristic of a population affects the quantity and location of crime by determining how frequently potential offenders are victimized. The development of the Internet changed the lifestyle and routine activities of the population and opened a decrease in traditional police-based crime prevention strategies (Caneppele & Aebi, 2017). Malik and Younis (2016) suggested that the cyber detection technique such as checking mistakes from many authority's claims, the email inspection

through internet protocol, and the use of network intrusion detection system to track and detect incoming and outcoming traffic on the network system help in the prevention of cybercrimes. Malik and Younis (2016) suggested that imposing local law regarding the report of cyber incidents to the state police allows them to fight more efficiently about cybercrimes by collecting information about the victims to develop an incident response plan to manage cyber risks better. Chavez and Bichler (2019) suggested that the increasing disadvantages over anticipated rewards would lead potential offenders to refrain from committing a specific crime, influencing the rational decision-making process to prevent crime. As businesses start to take into account very seriously the impacts of cybercrimes on their daily activities, it becomes more vital for them to make that issue a priority as part of their social change culture, which will contribute to awake and aware their employees of the necessity to keep eyes open on security threats that they may face in the daily basis.

Positive Social Change Implication. Many researchers have addressed the importance of positive social change in the reduction of cybercrimes. For example, Tankard and Paluck (2016) suggested that positive social change interventions may influence the perception of norms and behaviors regarding the deviance of social values. Payne et al. (2019) suggested that the evolution of cybercrimes is the result of building broadly effort and the use of a category of presumption as a guide in the understanding of traditional crime, white color crime, international crime, and socially constructed crime as part of positive social change. According to Barosy (2019), social change can be viewed positively when it includes a safe and secure environment in which business and

consumer confidence are increased strengthened by protecting personal and confidential information.

Safe Internet Environment. Having a safe internet environment is essential to prevent cybercrimes. Barosy (2019) suggested that establishing and sustaining a secure Internet environment may create a climate of trust and safety for the online community. Kakucha and Buya (2018) indicated that establishing a comprehensive framework to enable the development, institutionalization, assessment, and improvement of an information security program is a way to develop a typical information security strategy. Besides, there should be a need to deploy countermeasures that will block all attacks on the organization, which can be used to avoid information leakage (Kakucha, & Buya, 2018).

Network Protection. Cyber attackers infiltrate organization networks that are not protected from committing cybercrimes. Malware is any software used to disrupt computer operation, gather sensitive information, gain unauthorized access to private computer systems, and make illegal profit for malware owners (Bai et al., 2019). Holt et al. (2018) suggested that wireless networks as part of any organization network infrastructure should be secured to prevent malware from spraying when users engage to download activities that are not securely monitored. Critical elements contribute to cybercrimes and different approaches to mitigate them through a culture of prevention and security awareness that is very useful. Leukfeldt et al. (2017) suggested that cybercriminals can use malware such as viruses, worms, Trojan horses, and spyware to access credentials or manipulate the entire system sessions. Although there are many

tools to detect and prevent malware, it remains, however, one of the most common ways that cybercriminals use to infiltrate and cause significant harms to businesses and organization computers around the world, which needs to be taken into account when building and implementing security strategies in the prevention of cybercrimes.

Artificial Intelligence in the Prevention of Cybercrimes. Artificial intelligence applications are being found efficient in the prevention of cybercrimes. According to Hamet and Tremblay (2017), artificial intelligence is a general term that implies using a computer to model intelligent behavior with minimal human intervention. Siddiqui et al. (2018) suggested that artificial intelligence is helping humanity in addressing the issues of cybersecurity because of its intelligent nature and flexibility. Artificial intelligent techniques and applications such as heuristics, data mining, neural networks, and artificial immune systems have proven efficient in preventing and mitigating cybercrimes (Siddiqui et al., 2018).

Situational Prevention Factors and Social Bond Factors. Safa et al. (2018), by examining information security concern for organizations, suggested that situational prevention factors and social bond factors such as a commitment to organizational policies and procedures, involvement in information security activities, and personal norms for organizations promoted the adoption of negative attitudes toward misbehavior, which influenced the employees' intentions towards engaging in misconduct positively, and this, in turn, reduced insider threat behavior. In addition, surveillance in cyberspace may contribute to preventing situational crime. Testa et al. (2017) suggested that a situational deterring indication reduced the probability of system trespassers with fewer

administration privileges on the attacked computer system entering activity commands. In contrast, these indications in the attacked system did not affect the probability of system trespassers with the administration level of privileges to enter activity commands. Moeller et al. (2016) suggested that gaining access to counter-surveillance information and human capital by cybercriminals that directly affect people's success in online forums reduces the likelihood of capture and diminishes informal threats of burglaries. They also proposed that the fear of sanctions may motivate some criminals to cut off their ties to unfamiliar people and reinforce ties to criminal others due to restrictive prevention that emphasizes a behavior change.

Techniques in the Prevention of Cybercrimes

Data Privacy Prevention. Data are valuable assets for an organization and represent constituents that are the most targeted by cybercriminals. Fraudulent access to organization data without authorization can lead to data breaches. Martin et al. (2017) estimated that data breaches are bad for performance and the effect of data breach reaches a worse level when a firm is affected more than one time. Thomas et al. (2017) also estimated that data breaches at primary online services had become a regular occurrence in recent years. Based on a survey, 26% of adults affirmed that they had received a notice related to a data breach in the past year. Alotaibi et al. (2016) suggested that the very high cost of cybercrimes affects many consumers through the breach of data privacy and may drive them to use mobile gaming applications in the creation and learning of cybersecurity awareness. Therefore, it is vital to limit access to sensitive data by granting access only to authorized entities and monitoring any existing data storage system access.

Besides, organizations should adopt an information assurance approach to ensure data protection regarding confidentiality, integrity, authentication, and availability. Muller and Lind (2020) suggested that compliance with information security rules among information assurance professionals may prevent organizational data from risks.

Alerts and Anti-phishing. Anti-phishing methods are more used and taught in security averseness training, such as interactive game methods to allow users to identify risky emails and websites. The Importance of human factors in the fight against cybercrimes is essential in reducing cyberattacks by learning security best practices and security awareness training. Phishing is an activity that consists of stealing sensitive information online, such as username, password, and online banking details, from its victims (Arachchilage et al., 2016). Martin et al. (2018) suggested that understanding and quantifying end-user phishing susceptibility relative to their failure to incorporate expectation factors are crucial preconditions for developing adequate protection. Besides, Arachchilage et al. (2016) suggested that cybercriminals use the technique of phishing to attack victims. Therefore, alerting end-users about any phishing activity may prevent them from opening any phishing emails (Jansen & Leukfeldt, 2016). Thus, alerts are a way to avoid phishing, which contributes to the prevention of cybercrimes.

Honeypot. A honeypot is a system intentionally initiated to probably target cyberattacks and designed to attract intruders' attention and gather and report information. Litchfield et al. (2016) suggested that honeypots derive much value from their ability to fool attackers into believing they are authentic machines. According to the Pothumani and Anuradha (2017) decoy method, a new technique to detect the insider

attacker and end the amount of focus information to the attacker and redirect the attacker from the original data, appears as the best method to solve the threats of data security. Honeypots are vital in terms of keeping away data from any inside or outside intrusion.

Relationship of Literature to this Study

RAT has been used as a model to establish the relationship and evidence between crime and victimization data as part of the literature application to cybercrimes. Leukfeldt and Yar (2016) addressed the empirical application of the RAT to many online crimes and viewed virtual criminality the same as global crime, which demonstrates the ability of the theory to recognize the veracity of a crime when it also occurs in cyberspace. My study that deals with the security awareness strategies used in the prevention of cybercrimes by cybercriminals fit well with this literature framework and shows at which point crime victimization remains the same whether it is perpetrated in a physical or virtual world. Kayser et al. (2019) suggested that criminological theory can reduce crime rates relative to social engineering. Motivated offenders, suitable targets, and the absence of capable guardians, which are considered the core elements of the RAT diagram leading to a crime situation tested for their applicability in the virtual environment (Leukfeldt & Yar, 2016).

Transition and Summary

Section 1 addressed the foundation of my research study, including the background of the problem, the problem statement, the purpose statement, the nature of the study, the research question, the interview questions, the conceptual framework, the operational definitions, and the significance of the study. I provided relevant data and

information in a literature review to better understand my research topic, which deals with the security awareness strategies used to prevent cybercrimes by cybercriminals.

Section 2 will address several key points that will contribute to collect data for this study. That includes the research purpose statement and other components such as the role of the researcher, the participant implication, the research method design, the population and sampling, the ethical research, the data collection method and techniques, and data analysis techniques.

Section 2: The Project

Purpose Statement

The purpose of this general qualitative design study was to address strategies used for security awareness by information security officers in the prevention of cybercrimes by cybercriminals. The population was information security officers who were currently in charge of managing information security within their organizations and located in the United States of America, listed on LinkedIn, Facebook, or other social media. The implications for positive social change include the potential to develop a culture of prevention based on knowledge of cybersecurity awareness. In addition, implementing a strategic plan to prevent cybercrimes may contribute to users' knowledge of cybercrimes and increase vigilance when exposed to the internet and social media.

Role of the Researcher

I was the primary instrument in this qualitative study. The role of the researcher is to address a research subject by providing evidence that is accurate and valid through the creation of a trustworthiness protocol (Amankwaa, 2016). With more than 17 years of work experience in many government entities such as the Navy, Department of Defense (DoD), State Department, Department of Commerce, and some private organizations in relation with Information Technology, I dealt with a lot of security awareness training as part of requirements for most IT positions that I occupied primarily as a System Administrator and I understand its importance in the building of security awareness culture that will contribute in the prevention of the cybercrime phenomenon. Besides, I do not have any relationship to further participants.

I followed the Belmont report for this study to ensure the respect of ethical research guidelines regarding the protection of human subjects. I obtained relevant information related to my research study from the interviews that I conducted with the selected participants with strict respect to the interviewees and their viewpoints on any interview questions. The interview questions were designed for participants with knowledge of the topic who have overseen managing information security within an organization or have occupied a function as ISO (Appendix E). Weller et al. (2018) suggested that interview questions explore topics in-depth, understand processes, and identify potential causes of observed correlations; produce lists, short answers, or lengthy narratives.

An interview protocol is a way to get good quality interview data regarding reliability (Yeong et al., 2018). The use of the interview protocol (Appendix B) was used to mitigate bias. It was appropriate for this study because it helped create an atmosphere so the interviewees feel comfortable to provide an answer to the subject that can be analyzed later. Interview protocol will help to describe the development of interview questions (Kallio et al., 2016). The rationale for an interview protocol was to walk the participant through the way the interview was conducted and ensure that the participant will agree upon the process. Amankwaa (2016) suggested that creating a protocol is a way to show trustworthiness with details noting the characteristic of rigor, the process used to document the rigor, and then a timeline directing the planned time for conducting trustworthiness activities.

Triangulation in the data collection process reduced the risk of bias and increased the evidence of credibility that contributes to providing reliability (Abdalla et al., 2018). Methodological triangulation was used by comparing the results of the interviews with the participants and relevant documents from the National Institute of Standards and Technology (NIST) or other sources that meet industry standards. According to Joslin and Müller (2016), methodological triangulation uses multiple methods to study a research problem. Methodological triangulation enhanced the analysis and the interpretation of findings and reinforces data validity and the study's credibility. Triangulation was achieved when the viewpoints of the participants of the interview converged in the result of the answers that were provided on interview questions. The similarity of the answers to questions obtained from the participants and NIST documents or other sources that met industry standards will probably determine the level of acceptability in terms of methodological triangulation.

Ethical guidelines may influence decisions and behavior when communicated more efficiently (Hassan et al., 2020). The Belmont report is used in research and is related to protecting all research subjects or participants (Miracle, 2016). The Belmont report is used as an ethical framework for research; it played and continues to play in research ethics today in terms of protecting human subjects (Friesen et al., 2017). My research study followed the ethics and the Belmont report protocol, which guarantees the ethical protection of participants as part of my roles as a researcher concerning ethics and the Belmont Report protocol. Barlow (2020) estimated that the Belmont report that the National Commission published on April 18, 1978, outlines the basic ethical principles

for protecting human subjects. The Belmont report provides directives in human experimentation, including guidelines to evaluate the informed consent process, protection from harm, risks versus benefits, and the avoidance of unnecessary physical and mental suffering within the clinical trial. Besides, I followed all these ethical guidelines in my study. Friesen et al. (2017) suggested that Belmont advocates for a deductive relationship. Each principle is matched with one aspect of the research process: Respect for persons applies to informed consent, beneficence to risk/benefit analysis, and justice to subject selection.

Participants

The participants of this study were IT professionals with a good understanding of the cybercrime phenomenon and had the opportunity to deal with concrete issues. Besides, they were information security officers with a minimum of five years of experience in the IT field. They oversaw managing information security within their organization located on the northeast coast of the United States of America**.** I selected participants via LinkedIn and Facebook, which are online platforms that advertise people competences and their affiliations, making it easier to find the appropriate participant for a research study based on his/her job profile and work experience. Whitaker et al. (2017) suggested that social media is a popular online tool that allows users to communicate and exchange information. Advertisements can be posted and promoted to specific target audiences by demographics such as region, age, or gender, and recruitments may be faster and cheaper. Gelinas et al. (2017) suggested that the use of social media for recruitment is continuing to grow even though there is no specific regulatory guidance in

that regard at this time. Moreover, social media platforms contribute to developing and sustaining shared connections through effective online communication and allowing users to extend their social networks (Cheng et al., 2017).

I researched and identified participants that met my research criteria using the chosen social media search tool. Once I completed that process, I connected individually with each selected participant by sending a brief introduction message about myself and my research study via the social media portal. When the connection was established successfully with the participant, I invited the participant to participate in my research study by providing the participant with an invitation letter alone with the study consent form. Finally, data were gathered through open-ended questions. According to Awada (2016), open-ended questions are used to collect qualitative data, generally reflecting the feelings and perceptions of the respondents.

I established a working relationship with the selected participants by communicating with them courteously via the social media communication interface. Communication via phone, personal email, mail, or face-to-face is not excluded in that process when a good relationship was established with the participant. Woodward and Marrfurra McTaggart (2016) suggested that the development of trust through the slow building of a relationship based on place-based dialogue, an essential aspect of participatory action research, created the ground from which a mutually beneficial and respectful research partnership was able and continues to evolve. Relationships with participants were done honestly, and any communication met all participant requirements. In the face-to-face interview, nonverbal language and cues can be vibrant,

including dress, body language, mannerisms. They can give the interviewer a lot of extra information that can be added to the verbal answer of the interviewee (Oltmann, 2016). The interview was performed by following an interview protocol. Each participant was free to participate or answer the interview questions, which was conducted in all clearness and respect of the participants. Hershberger and Kavanaugh (2017) suggested that participants in both the email and phone interviews reported they were satisfied or very satisfied with their ability to express their true feelings throughout the interview.

All the participants were informed about the research study before the interview process to align with the overarching research question. The participant was provided with a consent form and interview protocol, including all the information provided via a regular communication channel such as email, mail, phone call, which will give a clear overview of the study and the process that was followed during the interview. Participant-led research can advance health knowledge by challenging and complementing traditional research (Vayena et al., 2016).

Research Method and Design

I extended qualitative research as the research method for this study and addressed the reasons for which quantitative and mixed-methods methodologies were not appropriate for this study.

Research Method

My research study was a qualitative approach that uses a general qualitative design study. I chose this method because it helped in the comprehension of complex social phenomena that allow people within the field to bring their real-life experience and

expertise in that regard, which is essential in understanding security awareness strategies used in the prevention of cybercrimes cybercriminals. Hammarberg et al. (2016) suggested that qualitative methods answer questions about experience, meaning, and perspective, most often from the participant's standpoint, which includes small-group discussions for investigating the beliefs, attitudes, and attitudes, and concepts of normative behavior, semistructured interviews. Additionally, Gerring (2017) believed that qualitative methodology works to understand or interpret social reality as it exists. According to Rutberg and Bouikidis (2018), qualitative research is often employed when the problem is not well understood, and there is an existing desire to explore the problem thoroughly. Therefore, qualitative research was appropriate for this study because it helped explore cybercrimes and prevent them. Saunders et al. (2018) suggested that qualitative research contributes to the small body of literature that examines the complexities of the concept and its underlying assumptions.

Quantitative research methods are the collection and analysis of structured data and can be represented numerically, which contributes to building accurate and reliable measurements that allow for statistical analysis (Goertzen, 2017). Furthermore, quantitative research is conducted in a more structured environment that enables the researcher to control study variables, environment, and research questions. Quantitative research may be used to determine relationships between variables and outcomes (Rutberg & Bouikidis, 2018). However, quantitative research is not appropriate for this study because it involves statistical tests, and I am not collecting quantifiable data.

The mixed-method methodology allows the convergence of both quantitative and qualitative research phases (Yapıcıoğlu & Kaptan, 2017). A mixed-methods approach involves research in which the researcher collects and analyzes data, integrates the findings, and draws inferences using both qualitative and quantitative methods in a single study or program of inquiry; besides, the approach has the potential to allow the researcher to collect two sets of data (Rutberg & Bouikidis, 2018). Whitmarsh and Corner (2017) suggested that mixed methods bring strength to study that used narrative design. However, the mixed-method methodology is not appropriate for this study because it would require a combination of qualitative and quantitative methods, which is not consistent with this research approach.

Research Design

I chose to use a general qualitative design study for this research study. Coker et al. (2019) suggested that a general qualitative design study incorporates semistructured interviews. Vaismoradi and Snelgrove (2019) indicated that general qualitative design study consists of various approaches towards data collection that researchers can use to help with the provision of both cultural and contextual description and interpretation of social phenomena in terms of content analysis and thematic analysis, which is a suitable qualitative approach to answer the study question. A general qualitative design study was appropriate for this study because it contributed to the prevention of cybercrimes through relevant security awareness strategies provided by real-time experience in the information security field.

Phenomenological research is the study of experiences from the first-person perspective (Spaulding, 2015). The phenomenological approach offers educational researchers' fundamental empiricism, a flexible structure, and dialogical community support (Sohn et al., 2017). This design method is not appropriate for this study because lived experiences are not the focus. The ethnography design uses the observations to study people and cultures and helps develop the practice to bring about that knowledge according to certain methodological principles (Howell, 2017). Hammersley (2018) suggested that ethnography is a holistic, deep description of the interactive processes involving discovering important recurring variables in the society as they relate to one another, under specified conditions, and as they affect or produce specific results and outcomes in the society. Ethnography is not appropriate for this study because it does not study the culture of a particular group in the research. According to Hammersley, ethnography may be seen as an inefficient way of producing relevant findings. The narrative design seeks to understand and interpret, focus on the particular story, and use the story as the anchor of analysis (Bruce et al., 2016). De Vries (2018) suggested that narrative research sets out to use the narrative nature of knowledge and understanding in its data collection methods and data analysis. According to De Vries, narrative research may support reflexive design by providing the methods to collect and analyze people's perspectives on a situation in-depth and resonance concept. The many stories that are present come together and organically grown into one shared story. Narrative design is not appropriate for this study because it interprets individual stories and is adapted for mixed methods.

For this study, data saturation was met when the participants' different viewpoints converged using the interview data and relevant NIST documents or other sources that meet industry standards. There was no need to interview additional participants because additional data was redundant. Aldiabat and Le Navenec (2018) recommended prolonged engagement, persistent observation, and thick, rich description; inter-rater reliability, negative case analysis; peer review or debriefing; clarifying researcher bias; member checking; external audits, and triangulation as strategies to achieve data saturation. Aldiabat and Le Navenec (2018) also suggested the importance of addressing several aspects of the sampling process, including the number of participants and the number of contacts with each participant. The length of each contact is a strategy to achieve data saturation. Nelson (2016) suggested that it is the role of a researcher to not only take care of how decisions are made around reaching saturation but of how these are reported within the research because of the impact in terms of the validly that the failure of reaching data saturation may have on the quality of the study.

Population and Sampling

This study population was listed on LinkedIn, Facebook, or other social media that work for an organization on the northeast coast of the Washington District of Columbia, which are currently managing information security within their organizations with at least five years of experience in IT. Once I completed that process, I connected individually with each selected participant by sending a brief introduction message about myself and my research study via the social media portal. When the connection is established successfully with the participant, I invited the participant to participate in my

research study and provided him with an invitation letter. Once participants agreed to participate in my research, I emailed them a copy of the consent form that participants acknowledged with the words “I consent” and returned to me and kept one copy for his/her own record.

Participants identified on social media were chosen to represent a true diversity in terms of IT security skills and experiences needed for this study based on the eligibility criteria. Kapoor et al. (2018) suggested that social media has attracted the attention of researchers from various fields, including information systems, to the point that they have to expend an enormous amount of time and effort to collate, analyze, and synthesize what they found from existing works before they embark on a new research project. The homogeneous purposeful sampling was used to identify seven participants selected on social media that work for an organization that will capture relevant information from different information security officers who manage information security within their work environment. I chose to use 10 selected participants because of their IT experiences and related positions relevant to data quality collection. Alase (2017) suggested that researchers should interview between five to ten participants who have all experienced similar phenomena; as such, the commonality of their experiences can be captured and interpreted**.** Homogeneous purposeful sampling is the choice for this study. Sedlander et al. (2018) suggested that the homogeneous sampling method reduces variation, facilitates group discussion, and describes a particular subgroup in dept. Kalu (2019) advised choosing a homogenous sampling to understand the participants' meaning to their lived experience. Rahi (2017) defined sampling as a process of selecting a segment of the

population for investigation; it is also a selection of a sample of units from a data set to measure the people's characteristics, beliefs, and attitudes. According to Asiamah et al. (2017), the population is the group of individuals having one or more characteristics of interest, and a population may be more important than can be expected. For this research, the population was chosen among potential participants with the specificity of being a manager of information security in an organization located in the Washington DC area. I used the social media selected research tool to select participants that meet the eligibility criteria. Participants should have at least five years of experience in the IT field and be currently in charge of managing information security within their organizations located in the United States of America's northeast coast. The number of participants reflected diverse viewpoints and approaches to addressing security awareness strategies in the prevention of cybercrimes. The 10 open-ended questions of the interview were sufficient to cover the essentials of the research study.

Hammarberg et al. (2016) asserted that the term ‘saturation’ refers to decisions about sample size in research using qualitative methods. Data saturation has been expanded to describe a situation where data tend towards repetition or where data cease to offer new directions and raises further questions. Researchers must show the validity of their analysis and conclusions, resulting in longer papers and occasional frustration with the word limits of appropriate journals (Hammarberg et al., 2016). Researchers use methodological triangulation to justify the internal validity by comparing the qualitative findings obtained from the interview transcripts with the quantitative findings (Wong & Cooper, 2016). Methodological triangulation refers to the use of multiple methods to

obtain more complete and detailed data about the phenomenon (Abdalla et al., 2018). Data collected from interviews and relevant NIST documents or other sources that meet industry standards will reach methodological triangulation and ensure data saturation. Therefore, the choice of a semi-structured interview was appropriate for this study.

Ethical Research

I addressed ethical issues in my research study by requiring the consent of the participants when it comes to collect data and personal information. Gavin and Rodham (2017) suggested that members who carry out research online should ensure that they are familiar with ongoing debates on internet research ethics and might wish to consider erring on the side of caution in making judgments affecting the protection of online research participants. The selected participants were free to participate in the interview process to collect data for this study. Participants were also free to withdraw from the interview without any pressure by informing me by email or phone. There was no pressure exercised towards them regarding their interview schedule, and any proposed availability was accepted. The participants signed a consent form (Appendix C) agreement, which will include the closures of the participation in the research study topic.

Moreover, an interview protocol (Appendix B) was provided to the participants, which provided an overview of the research topic and the multiple questions addressed during the interview process. Besides, all the participants were assured verbally or/and by email that the data collected from them was maintained in a safe place for five years to protect their confidentiality. After five years, the participant's information was destroyed accordingly. By referring to Blair et al. (2017), "researchers should not harm the safety,

dignity or privacy of the people with whom they work or who might reasonably be thought to be affected by their research." The certificate of completion of the National Institutes of Health (NIH) number is 2398160 confirmed that I understood the ethical aspect of collecting data and protecting human research participants, as shown in Appendix A. Data collection would occur only after receiving the Walden IRB approval. This study IRB approval number was 08-31-20-0582900.

Each participant received a unique number that located the participant data and the folder's name where his data was stored. The participant and personal information that are digitals or electronics were stored in an encrypted USB drive under each participant folder and kept in a secured physical location until the end of the retention period, which is five years. Participants were thanked with a gift card for their contribution to this study but received a copy of their interview transcript within two weeks of the interview completion. Participants were allowed to withdraw anytime from the study by sending me an email that expresses their need for withdrawal from the study. Once a withdrawal email is received from a participant, I securely destroy any related information. Harriss et al. (2017) suggested that human participants have the right to refuse to participate or withdraw consent without punishment. After the end of the retention period, all the stored information was destroyed using safe techniques.

Data Collection

Data collection is the process of gathering and measuring information on targeted variables in an established system to answer relevant questions and evaluate the outcome (Rosalina & Jayanto, 2018). D. Whitehead and L. Whitehead (2016) suggested that the

process of data collection follows the identification of the sample, which can take the form of direct data or indirect data. Direct data include recordable spoken or written words and also observable body language, actions, and interactions and indirect data are generated, in the first instance, by someone or something else, such as with documents or photographs reporting an event or an artistic rendition of an event or experience (D. Whitehead & L. Whitehead, 2016). Data collection instruments, data collection techniques, and data organization techniques were the main focuses in this section regarding the approaches to collect, analyze, and organize data. I also used the document review method to check the accuracy, integrity, and availability of documents related to this study. I used relevant NIST documents or sources with the same industry standard to support my research study. Johnson et al. (2017) suggested that document review provided contextual information and increased our understanding of the organizational context of the study. Therefore, I reviewed relevant NIST documents or other sources that meet industry standards related to my research study. Documents for review can be obtained by searching the information needed on the NIST website or conducting Google searches on other websites that meet the same standards. They are documents containing relevant information that talks about the research topic, the insight into the research question, which can be exploited during the data analysis process. Genç et al. (2019) also suggested that documents retrieved through the Scopus database should be analyzed, integrated by correlation with each other, and analyzed through content analysis.

Data Collection Instruments

As the primary data collection instrument, I collected data using a questionnaire of 10 open-ended questions (Appendix B). I used semistructured interviews as the first data collection method and document review as the second method of data collection, which will provide the methodological triangulation of data for this research. The semi-structured interview is the data collection method generally used (Kallio et al., 2016). Semi-structured interviews allow the researcher to collect open-ended data, explore participant thoughts, feelings, and beliefs about a particular topic and delve deeply into personal and sometimes sensitive issues (DeJonckheere & Vaughn, 2019). According to DeJonckheere and Vaughn (2019), semistructured interviews consist of a dialogue between researcher and participant, guided by a flexible interview protocol and supplemented by follow-up questions, probes, and comments.

The semi-structured interview was a face-to-face interview with a verbal interchange with the participants that could also occur on Skype or Zoom. Semistructured interviewing requires both a relational focus and practice in facilitation skills (DeJonckheere & Vaughn, 2019). I followed a code of conduct and an interview protocol (Appendix B) during the interview process. Castillo-Montoya (2016) suggested that the interview protocol improves the quality of data obtained from research interviews. Questions (Appendix B) presented to the selected participants were done courteously by following any ethical behavior in that regard given the position of each selected participant. Holmes et al. (2016) suggested that the code of conduct represents a synthesis of the participants' community narrative, incorporating participant stories,

interpretations, and feedback, which can help inform visitors better and challenge predetermined notions. I interviewed participants using a semi-structured interview following the interview protocol (Appendix B) and will provide the participants with some instructions. I asked participants to sign a consent form (Appendix C) and explain how the interview was conducted by allowing them to address any suggestion in that regard. Dwyer and Chauveron (2016) suggested that the respect of trustworthiness with the participants is a way to achieve member checking, elevating the quality of the work and promoting credibility through dependability, transferability, and confirmability. Trustworthiness resides in the degree of confidence in data, interpretation, and methods used to ensure the quality of a study (Connelly, 2016). Researchers should establish the protocols and procedures necessary for a study to be considered worthy of consideration by readers (Amankwaa, 2016). Member checking was used to verify the authenticity of the information collected with participants during the semi-structured interviews. I conducted member checking by setting up a second interview with each participant held on the phone, via Skype, or Zoom to check the accuracy of my interpretation of the interview. If a participant cannot be reached on the phone, I send an email to the participant to reschedule a second meeting until I get participant feedback. All the described approaches and techniques helped to ensure member checking. By doing so, participants helped validate the interpretation of the data collected during the interviews. Amankwaa (2016) suggested that researchers need to mitigate bias in data collection with member checking. Relevant NIST documents or other sources that meet industry

standards and data collected from open-ended interviews were used as data sources to perform methodological triangulation.

I built a good partnership and trust with the participants to ensure a complete and valid set of qualitative data to ensure data accuracy provided in the transcript for evaluation. In addition, I conducted member checking using communication channels such as face-to-face meetings, email, mail, or phone call.

Data Collection Technique

Semistructured Interviews and relevant NIST documents or other sources that meet industry standards are the data collection technique used for this study. Relevant NIST documents or other sources that meet industry standards were considered as my secondary data collection technique. NIST or other similar documents describe handling and procedures used by organizations to deal with technical/security issues related to this study, which can be found directly on the NIST website or online via Google searches. I used related documentation combined with the notes taken during the interview to perform document reviews and analysis. Genç et al. (2019) suggested that document analysis resides in the content analysis, which is the compilation of similar data within the structure of specified concepts and themes and their interpretation, including their organization, so that the person who reads can understand. Therefore, the semi-structured interviews were considered as my primary data collection technique. Only selected participants that met the selection criteria of my research study participated in a scheduled face-to-face interview. Social media helped to locate participants via their profiles. Bhatia-Lin et al. (2019) suggested that profiles on social media are maintained

over time by participants themselves and make it easy to track or contact them directly. Participants were contacted using emails, phone calls, Skype, or Zoom and were provided with the participant consent form (Appendix C) and the interview protocol (Appendix B) before the interview process. I briefed them about my research topic and the role they played in that regard.

Once the participant agreed to sign the consent form (Appendix C), a semi-structured face-to-face interview was conducted following the interview protocol (Appendix B). During the interview, participants answered ten probing open-ended questions (Appendix B). This process was only possible after I received the IRB approval in that regard. The interview was recorded on an audio recorder in an electronic or digital format that is easy for transcription with the participant's consent. Transcripts should be created in a fashion that facilitates the simplicity of review and shows any nuanced techniques employed for a participant (Fritz & Vandermause, 2018). I used my notebook to take relevant notes during and after the interview process. The interview was done in a location agreed upon by the participant. Birt et al. (2016) suggested that member checking allows the exploration of the credibility of results, which are returned to participants to check for truthfulness and resonance with their experiences.

Member checking steps consisted of reconnecting with the participants using existing communication channels such as emails, phone calls, Skype, Zoom, face-to-face meetings that helped schedule meetings with them to review the accuracy of work done during the interviews. Smith and McGannon (2018) suggested that the confirmation of participants relative to the accuracy of the data and/or results, the findings can be deemed

credible and ensure the validity of the research. The advantages of face-to-face interviews are to allow the researcher to interject where necessary and ensure that the subject understands the topic or question under scrutiny; in addition to this, interviewers get to use their interpersonal skills to explore significant issues raised by the participant, aspects that are central to comprehensive data collection (Adhabi & Anozie, 2017). The disadvantage of face-to-face interviews is the time it takes to recruit participants and conduct interviews, which can deliver biased responses and require more vet in terms of the respondents' answers (Marshall & Rossman, 2016). Tsai et al. (2016) suggested that discrepant data may be critical in increasing familiarity with a particular interviewer. The fact of sharing qualitative data is consistent with ethical standards in research. A member checks are reviewed to identify the purposes and procedures for seeking feedback from research participants and outcomes reported from member checks (Thomas, 2017). Member checking was done by having a second interview with participants to verify my interpretation of their interviews. The procedure consisted of reaching out to participants by scheduling additional meetings through existing communication channels such as emails, phone calls, text messages, Skype, Zoom, or face-to-face meetings. Thomas (2017) suggested that member checks can be helpful in specific circumstances such as obtaining participant approval for the use of extended quotations or case studies and where anonymity cannot be guaranteed.

Data Organization Technique

One of the first rules of data organization is consistency. Data entered and organized should be consistent to prevent time spending from harmonizing the data later

(Broman & Woo, 2018). For this study, I kept track of all the data that was collected during the interview process. I maintained the journal and notes that I have taken to reflect the objective viewpoint of the participants on the research topic. Data coded into each theme should be checked and rechecked by coding every segment of the text. Data coded reduce lots of data into small chunks of meaning (Maguire & Delahunt, 2017). Each code was used to keep track of collected data that was labeled and dated accordingly. Fletcher (2017) estimated that the flexible deductive process of coding is consistent with the data organization. I used NVivo software to keep track of the data. Woods et al. (2016) suggested that the NVivo application provides better data analysis. Microsoft Excel spreadsheets were also used to generate reports, graphics on different data stored on NVivo. NVivo enhances data transparency in qualitative research, allows data extraction, data import, and data synthesis (Houghton et al., 2017). After performing member checking of the interviews, I loaded the data into the NVivo application, coded and analyzed it accordingly. After loading the data into NVivo, I assigned a unique number to each participant for identification purposes. The unique number helped to track the content of the records of the participants relative to the answers to the interview questions. Carter et al. (2019) suggested that participants be assigned a unique participant number as each focus group is transcribed. Transcription can be a very lengthy process depending on the quality of the recording and the experience of the transcriber but is necessary for the analytic process and to maintain the confidentiality of participants (Rosenthal, 2016). Data collected and analyzed were stored on a secure external storage encrypted USB drive with a large capacity and kept in a secured physical location. I

ensured that participants' personal information and data are protected. Bender et al. (2017) suggested that individuals should have the opportunity to exercise control over personal information by consenting to, or withholding consent for, the collection, use, and/or disclosure of information. I securely stored the data in electronic and hard copies in a secured and encrypted USB drive with a large capacity, which was destroyed after five years.

Data Analysis Technique

Thematic analysis was used as the data analysis technique for this general qualitative design study, which uses two data sources to collect data. Drinkwater et al. (2017) suggested that thematic analysis is a method for identifying, examining, and reporting themes/configurations within data sets. In this study, interviews and relevant NIST documents or other sources that meet industry standards were used for thematic analysis. Additionally, Deighton-Smith and Bell (2018) suggested that thematic analysis may be instrumental where the interpretation of both written and visual text is required, such as research using newspapers, magazines, advertising brochures, or social media. Participants will respond to ten open-ended questions (Appendix B) related to the purpose of this study. A semistructured interview was used to collect information following the interview protocol (Appendix B). Hadi and Closs (2016) suggested that developing rigorous conduct of semistructured interviews contributes to the trustworthiness of the semi-structured interview. According to Shalhoub et al. (2017), semistructured interviews help avoid superficial responses and offer the flexibility to follow up on and seek detail and clarification on key points. Interviews were recorded in

real-time with an electronic recorder device to ensure accuracy and transparency. This process saves time and prevents from collecting the same information twice.

After collecting the interview data and member checking completed, I used Microsoft Excel and NVivo to analyze data. Microsoft Excel will allow me to sort and filter data easily from different variables and generate graphics. NVivo helped to code collected data for meaningful analysis, which will help extract relevant information to support the findings. Erlingsson and Brysiewicz (2017) suggested that labeling condensed meaning units by formulating codes helps group these codes into categories.

The focus was on grouping data based on key themes that support the prevention of cybercrimes using relevant security awareness strategies. Cunningham et al. (2017) stated that researchers must be particularly conscious and consistent with their use and interpretation of key themes. They built their studies around the themes and suggested they enable researchers to work on relevant research fields offering further insights into previously neglected research areas. Data analysis helped in the validation of pertinent information that was collected from interviews and organization documents. According to Munch (2017), data analysis attempted to produce a collection of techniques stemming from the idea that data has a shape and can be carefully quantified to investigate data.

Reliability and Validity

Reliability and validity are two techniques used in the evaluation of the quality of research. Both methods refer respectively to the consistency of a measure and the accuracy of the measure of research (Mohajan, 2017). Mohajan (2017) suggested that reliability is the degree to which a measurement tool produces constant and consistent

results, and validity is the degree to which the results are truthful. Korstjens and Moser (2018) suggested that qualitative researchers speak of trustworthiness in terms of criteria such as credibility, transferability, dependability, and confirmability. According to Hayashi Jr. et al. (2019), validity is better evidenced in quantitative studies. There are no universally accepted criteria to assess validity in qualitative studies; it supports good research and helps in its reflection and guidance. Researchers generally determine validity by asking a series of questions and will often look for the answers in other research; triangulation is a strategy used to improve the validity and reliability of research (Golafshani, 2003).

Dependability

Dependability involves the reliability and maintainability of the research findings. Korstjens and Moser (2018) suggested that dependability involves participants' evaluation of the study's findings, interpretation, and recommendations and is supported by the data received from participants of the study. The use of data saturation in this study contributed to establishing the necessity to reach an acceptable point of convergence with the collected data. Content analysis has changed from a counting game to a more interpretative approach and can be used at varying levels of abstraction and interpretation (Graneheim et al., 2017). Data collected from the interview and from NIST documents or other sources that meet industry standards are relevant to ensure the dependability of this study. Methodological triangulation contributes to detecting inconsistencies in data sets and allows better comprehensive data at the end. Fusch et al. (2018) suggested that the importance of triangulation cannot be underestimated to ensure

the reliability and validity of the data and results because it helps in the comparison of data from multiple data collection methods and helps in the mitigation of any researcher bias. I took notes and documented the processes that I did to gain access to participants and perform the participants' selection, including the interview process and the method used for the transcription of the collected data. I kept and updated the journal of everything that I have done and conducted during my research, including interview remarks, questionnaires, and observations. The interview method is often used as a way to conduct a study and to gather preliminary data. It requires the use of various skills and a well-planned strategy in terms of asking questions. McGrath et al. (2019) suggested that qualitative interviews afford researchers occasions to explore, in an in-depth manner, matters that are unique to the experiences of the interviewees, allowing insights into how different phenomena of interest are experienced and perceived. A questionnaire is a great way to explore participants' experiences, thoughts and gather information about sensitive topics, as it maintains participant anonymity. Daniels et al. (2020) suggested that a questionnaire is part of the multiple sources of evidence that increase the reliability and validity. Observation is a way to observe nonverbal and verbal behavior and things that surround us. Aspers and Corte (2019) suggested that observation allows researchers to routinely make several focus and research design adjustments as their studies progress.

Moreover, to deal with the dependability issue, I documented all the interview processes and will allow future researchers to repeat the work to obtain the same results. The use of the NVivo was a good asset in organizing data collected from the interviews, which is a good way to track all the research processes and ensure the dependability of

the information used in the analysis and the presentation of the research findings. Fusch et al. (2018) estimated that triangulation adds depth to the collected data, especially when using multiple data collection techniques.

Credibility

Credibility involves transparency and trustworthiness in the research results. Abernathy et al. (2017) suggested that credibility drives assurance, report integrity, standard frameworks and guidelines, and regulation. Korstjens and Moser (2018) presented the research findings that represent plausible information drawn from the participants' original data, and correct interpretation of the participants' actual views will help establish credibility. Using an electronic recorder device to record interviews allows the participants to review the transcript and ensure the credibility of the content of data collected data. Bengtsson (2016) suggested that there must be a chain of logic between the decisions made and how the study will be conducted to ensure credibility. To guarantee the credibility of this study, I followed the interview protocol (Appendix B) and ensured that every mentioned step was followed and executed accordingly. Smith (2018) stated that methodological triangulation is widely regarded to enhance the credibility of case studies. Methodological triangulation consistent with data collected from the interviews and relevant NIST documents or other sources that meet industry standards helped build solid trust and ensure the credibility of this study. I continued to gather different collected data until I reached data saturation. Triangulation adds depth to the collected data, especially when using multiple data collection techniques (Fusch et al., 2018).

Transferability

Transferability involves the establishment of evidence of the data collected for this research study. Cruz and Tantia (2017) suggested that transferability is the applicability of the finding to other contexts, but not in the sense of making broad claims. The reader was provided with evidence of the relevance of what has been found in data analysis that can be useful in the prevention of cybercrime. The use of heterogeneous sampling contributes to ensuring transferability through the criteria used to select participants of this study. The interest of heterogeneity sampling profoundly explores diverse groups of participants (Mason & Wronski, 2018). I provided a rich description of the process used to collect data in the most understandable way and made that available to my audience. I also ensured that I complied with the research protocol by detailing every step taken during the study, including my research findings and related results.

Confirmability

Confirmability involves the acceptability and expectation of the research results and depends on the purpose of the study. Methodological triangulation was used in this study to ensure confirmability. I kept a journal of every participant's opinions recorded during the interviews. I used the relevant NIST documents or other sources that meet industry standards to increase the validity of this study. Korstjens and Moser (2018) suggested that conformability establishes that data and interpretations of the findings are not figments of the inquirer’s imagination but derived from the data.

To ensure data saturation, participant opinions on the research topic should converge accordingly. I ensured that data collected from interviews and relevant NIST documents or other sources that meet industry standards are used as the point of convergence of the findings of this study. According to Hancock et al. (2016), data saturation is achieved when there are no new emerging ideas in the data. Placing the data in a chart or another figure provides a visual effect prompting the researcher to view the data differently, confirming saturation.

Transition and Summary

Section 2 addressed the approach used to collect and analyze data. My study used the qualitative method with multiple case studies as research design and data collected from the interview process contributed to detail the findings regarding the security awareness strategies used to prevent cybercrimes by cybercriminals.

Section 3 of this study provided more facts on the results. It addressed the study's applications to professional practice, including its implications for social change, recommendations for action, and future research, including the study reflections, summary, and conclusions.

Section 3: Application to Professional Practice and Implications for Change

Overview of Study

The objective of this qualitative general design study was to address strategies used for security awareness by information security officers in the prevention of cybercrimes by cybercriminals. In this part of the study, I presented the findings, applications to professional practice, implications for social change, recommendations for action, and recommendations for further study. I ended the section with a summary, reflections, and study conclusions.

Introduction

This qualitative general design study aimed to address security awareness strategies used by information security officers to prevent cybercrimes by cybercriminals. The study was conducted with a population of seven IT Information Security Officers selected on LinkedIn, all located on the Northeast coast of the United States of America with at least five years' experience in the IT field. I used semistructured interviews to interview the seven selected participants via the online communication platform called Zoom. I recorded the interviews and used NVivo to extract, transcribe interview data and code the interview' results. I also used data triangulation with data collected from interviews with selected participants and NIST documents addressed in that regard. Four themes emerged from the analysis and review of the collected data and NIST documents: (a) policies to prevent cybercrimes, (b) cybersecurity response plan, (c) awareness as a culture, (d) train end-users/employees.

Presentation of the Findings

This study's overarching research question was: what strategies for security awareness do information security officers use to prevent cybercrimes by cybercriminals? I collected data from my multiple open-ended semistructured interview questions with selected participants via the Zoom communication platform, and I reviewed NIST documents relative to the collected data. I completed interviews with 7 participants selected on LinkedIn who are Information Security Officers; two came from the private sector, four from a government entity (public sector); and one from a mixed sector (private/public sector). All participants are located on the northeast coast of the United States. After I recorded and completed all the interviews, I imported the interview records into the software NVivo included any NIST documentations mentioned during the interviews by the participants. In addition, I performed member checking after the interview process and ensured no new themes emerged from all the data collected.

Four themes emerged from the analysis of data collected, including NIST documentations, notes taken, and observations made during the interviews: (a) policies to prevent cybercrimes, (b) cybersecurity response, (c) cybersecurity awareness as a culture, (d) train end-users/employees as specified with more details in Table 1. Each participant has been identified with a unique identification number to ensure his privacy. Participant 1 was identified as PA1, Participant 2 as PA2, Participant 3 as PA3, Participant 4 as PA4, Participant 5 as PA5, Participant 6 as PA6, and Participant 7 as PA7. Table 2 provides demographic information of the seven selected participants regarding their activity sector,

years of experience, size of people supported in their organizations, and their geographic locations.

Table 1

Key Themes of the Study' Findings

Themes	NVivo' Word Count	Participant' Count	Participants
Policies to prevent cybercrimes	58	7	All
Cybersecurity response plan	36	7	All
Cybersecurity awareness as a culture	30	5	PA1, PA3, PA5, PA6, PA7
Train end-users/employees	30	7	All

Table 2

Demographic Information about the Participants

Participants	Sector	Year of IT Experience	People supported	Geographic Location
PA1	Public	15	500	Virginia
PA2	Private	5	10	Washington DC
PA3	Mixed	10	18	Washington DC
PA4	Public	10	30	Maryland
PA5	Private	5	7	Maryland
PA6	Public	6	10	Maryland
PA7	Public	7	10	Maryland

I used the RAT as the conceptual framework of this general qualitative study. The framework is vital in reducing crime rates relative to social engineering (Kayser et al., 2019). Leukfeldt and Yar (2016) estimated that the core element of the framework had

been tested for their applicability in the virtual environment. The findings revealed a remarkable convergence of viewpoints regarding the strategies used for security awareness by information security officers in preventing cybercrimes, which are translated in each theme with related tables.

Theme 1: Policies to Prevent Cybercrimes

Policies to prevent cybercrimes are the first theme that emerged from this study. Preventing cybercrimes depends on compliance with the security policies and procedures that each organization puts in place to prevent cybercrimes. Organizational procedures are essential for adequately implementing any general plan or policy (Maglaras et al., 2019). A specific NIST framework is part of the approach that contributes to implementing policies within the organizations. Gordon et al. (2020) suggested that the NIST cybersecurity framework is an approach that is collectively accepted and facilitates cybersecurity risk management within organizations. That approach fits very well with all the participants of this study. NIST frameworks have been instrumental in creating and implementing their organization policies in diverse aspects. Table 3 below shows different NIST frameworks used by the selected participants within their organizations to create and enforce their cybersecurity policies to prevent cyberattacks.

Table 3

NIST Frameworks expressed by Participants in the Prevention of Cyberattacks

NIST Framework	Participants	Document Page Count
NIST Framework 800-18	PA2	48
NIST Framework 800-30	PA4, PA5	95
NIST Framework 800-37	PA4	113
NIST Framework 800-39	PA4	88
NIST Framework 800-53	PA1, PA3, PA4, PA6	481
NIST Framework 800-53A	PA4	487
NIST Framework 800-61	PA4, PA5	65
NIST Framework 800-81	PA7	119
NIST Framework 800-82	PA7	171
NIST Framework 800-137	PA2	80
NIST Framework 800-161	PA5	282
NIST Framework 800-171	PA1	78
NIST Risk Management Framework	PA2	8

(The documents can be downloaded freely at https://www.nist.gov/)

All the participants agreed that organizations should have their own policies when it comes to preventing cybercrimes. All the participants acknowledged that they used specific NIST frameworks to create their policies, even if the framework used may be similar or different according to the activity domain in which they operate. They also expressed that it is essential to stimulate and educate end-users/employees to comply with the policies to reduce cyberattacks that could come from the outside than the inside of their organizations.

PA1 noted that he created a cybersecurity council to push down cybersecurity policies within his organization. PA1 stated,

> The first thing I did was to create a cybersecurity council, which comprised of the Chief Executive Officer (CEO), Chief Operating Officer (COO), Chief Financial Officer (CFO), Executive Vice President and HR, Senior Vice president, Strategy senior Vice president of marketing, then a couple more individuals, but you know cybersecurity is not just an IT or cyber problem. It's a corporation problem.

PA1 also acknowledged the importance of meeting those seniors to understand better the threats and risks included the cost linked to any cyber-attacks in his organization, which allowed him to push down the cybersecurity policies freely. PA2 confirmed that his company has put in place numerous security policies to deal more efficiently with cyberattacks in his organization, as enumerated in Table 4. PA2 and PA5 share identical policies when it comes to the password and backup policy. PA3 mentioned that his organization follows a higher standard framework as enumerated in Table 3 and used some of its relevant controls to address cybersecurity best practices based on its existing policies. All the policies implemented by the selected participants of this study are summarized in Table 4.

Table 4

Type of Policies implemented to prevent Cyberattacks by participants.

Participants	Policy Types
PA2	Anti-virus update policy
PA2, PA6	Backup policy
PA2	Patching management system policy
PA2	Software installation policy
PA2	Firewall policy
PA2, PA6	Password policy
PA2	Host intrusion detection system policy
PA4	Authentication method policy
PA4	Incident response policy
PA4, PA5	Emergency policy
PA5	Disaster recovery policy
PA6	Data replication policy
PA6	Application policy

PA4 reported that the creation of policies should be at two levels. One level should reflect the organization's policies and the other, the system policies. He noted that cyberattacks affect security measures and controls because they take advantage of vulnerabilities. That is why it is essential to create policies linked to configuration management, as shown in Table 4. PA4 also affirmed that his organization relied on numerous cybersecurity policies to prevent cybercrimes, as mentioned in Table 4. He also noted that his organization used many templates to create policies using different frameworks other than the one mentioned in Table 4, such as Federal Information Security Management Act (FISMA), Payment Card Industry Data Security Standard (PCI DSS), International Organization for Standardization 2700 (ISO 2700).

PA5 confirmed that his organization used many policies to combat cyberattacks, as shown in Table 4. In addition, both PA5 and PA4 have adopted emergency policies in case of cyberattacks. PA6 used the NIST framework, especially NIST 8700-50 (Table 3)

with its 341 controls implemented, to prevent cyberattacks. PA2 has implemented backup policies to protect its organization's data in case of data breaches and recovery.

PA7 implemented some policies based on NIST 800-71 and NIST 82 (Table 3) to prevent cyberattacks. His organization follows a protocol that ensures that everybody goes by those policies through continuous monitoring. Moreover, they also perform a vulnerability scan every three months to ensure no vulnerability in their system. Aldawood and Skinner (2019) expressed the commitment of new employees to follow ethical business behavior in that regard.

The study's finding on using policies to prevent cybercrimes corroborates with the literature expressed by Kayser et al. (2019). Having solid policies and procedures related to cybercrime protection is very important for organizations (Kayser et al., 2019). Policies and procedures play a huge role in the security awareness education training by demonstrating the ability of the organization to provide training to employees through a general session on security awareness for all the new employees by focusing on commitment to ethical business behavior (Aldawood & Skinner, 2019). Schreck (2017) agreed on the need for organizations to have appropriate laws and policies to fight cybercrimes again. All the participants agreed that their organizations put in place several policies to prevent cyberattacks.

The theme of using policies to prevent cybercrimes supported the RAT framework of Cohen and Felson (1979). Marcum (2009) addressed protective measures to take against victimization to improve guardianship. Strong policies implemented by organizations contribute to preventing victims from being cyber-attacked. Cybercriminals

use the vulnerabilities of their victims to perpetrate their crimes (Vakhitova et al., 2016). Cybersecurity policies that are well implemented and addressed help to reduce those vulnerabilities and prevent cyberattacks. Reyns et al. (2016b) used RAT to address the importance of identifying the risk factors for victimization. Policies are created based on the risk factors that organizations face daily.

All the participants within their organizations used policies to prevent cybercrimes. In addition, the NIST documents cited by participants in this study addressed the importance of policies for organizations in preventing cyberattacks and corroborate with the participants' approach regarding this theme, as shown in Table 5.

Table 5

NIST Documents to support the Theme 1 expressed by participants.

NIST Documents	Policies to prevent Cybercrimes
NIST Framework 800-18	x
NIST Framework 800-30	x
NIST Framework 800-37	x
NIST Framework 800-39	x
NIST Framework 800-53	x
NIST Framework 800-53A	x
NIST Framework 800-61	x
NIST Framework 800-81	x
NIST Framework 800-82	x
NIST Framework 800-137	x
NIST Framework 800-161	x
NIST Framework 800-171	
NIST Risk Management	x

Theme 2: Cybersecurity Response

Cybersecurity response is the second theme that emerged from this study. This theme represents the approaches used by organizations when they are cyber-attacked.

Cybersecurity incidences often fall into three categories: Malware (22%), phishing (21%), and pharming (7%), according to the New York State Department of Financial Services (2014) cybersecurity survey report (Catota et al., 2018). These attacks were supported by the participants in this study regarding the recurrent security threats facing organizations today, as shown in Table 6.

Table 6

Common Security Threats of Organizations expressed by participants.

Cybersecurity Threats	Participant count
Phishing	7
Spear phishing	5
Malicious codes	1
Data infiltration	1
Unauthorized access	2
Social engineering	4

All the selected participants of this study verbally expressed their cybersecurity response approaches, as illustrated in the following lines. PA1 stated, “I followed things like the NIST 800-53 and NIST 800-171 to develop my incident response plan. The actual first response is detecting the event“. PA1 added that the one that he uses is a seven-step process that breaks down even further within the seven steps like the detection of the event, the analysis and identification of the event, the preliminary response of the event, the answers and analysis, response, and recovery, and then your post-incident analysis, which can be also break down a little bit further as the framework he used when it comes to cybersecurity attacks. PA2 stated,

> The first response is we access the breach to determine the cause of the breach by asking questions: Who has access to what? Let me talk in case of the server who

> has past access to which servers? Which network was affected? How was the attack initiated?

PA2 also stated that they might also check security data during the first response process, logs through firewalls, email providers, antivirus programs, and intrusion detections. PA3 noted, “So, the first response is to ensure that we are not affected first.” PA3 illustrated that with Microsoft Exchange Server vulnerabilities ongoing right now and different people trying to hack into organizations. So, his viewpoint was to make sure that there is no trace of any such attacks. And if yes, for instance, they know something or if it has been confirmed that those attacks are already in the organization, then they use a triage to understand where they could, first, to access and try to stop the progressions. PA3 also stated that those things also could be done via a complete forensic. PA4 stated,

> When a cyberattack takes place, the first response is first of all to identify this cyberattack. That is number one. We want to know what kind of cyberattack we dealt with. You cannot just start mitigating something that you don't know it.

PA4 also mentioned the importance of identifying the kind of attack they face by determining whether a brute-force attack or malware was sent in through phishing emails that identified the issue. PA4 added that it is not always advisable to counteract an attack. They always try to contain it to protect their selves rather than try to control counterattacks. So, where if they attack, then the next thing they do is try to contain it before it goes out of hand with cyberattacks. It might be malware or maybe a rootkit. It

may be a worm that is spreading the network. They need to try to contain the attack before it affects other systems on the network.

PA5 stated, “The first response globally is you need to communicate.” PA5 also indicated that different departments must be informed of the attack, reach out to national database vulnerability, communicate to the forensic investigators, communicate the incident to the people and make sure that the attack is contained. In summary, PA5 believed that the first response to a cyberattack is to communicate the attack and then contain the attack to not spread to other systems. PA6 stated,

> The first thing when there's an attack. Obviously, the user will make a complaint to the Helpdesk, and when something came to the Helpdesk, the Helpdesk is going to coordinate with the security team to alert that there was an attack or something or the system is down.

PA6 also stated the first response to a cyberattack depends on the type of attack. So, when an attack is known and notified to the security team, there will be the involvement of the ISO or various stakeholders. They will coordinate with the CP coordinator or suggested client coordinator for the damage assessment. When they had the initial damage assessment, the CP coordinator will look at it to ensure that this is an attack that can be remediated. PA6 acknowledged the responsibility of the business owner in the initiation of the damage assessment and his collaboration with other stakeholders to initiate the process to recover from the cyberattack and ask for lessons learned after the recovery is done.

PA7 stated, “My first response to a cyberattack is to contain the attack; then investigate totally that attack and making sure that we understand how the attack occurred, on how to prevent such attack from occurring in the previous in the future.” PA7 also insisted on the importance of the investigation of the attack by doing forensic investigation on how deep the attack occurred. In addition, PA4 stated that forensic investigation is useful to trace if data and the content were exported from the organization, to make sure to understand how far the attack occurred, to know the steps used to prevent it, how to retrieve the organization’ information, and notify the public of such attack.

The theme of cybersecurity response is consistent with the study literature and with the finding of Leukfeldt, Kleemans and Sto. Cybercriminals can use malware such as viruses, worms, Trojan horses, and spyware to access credentials or manipulate the entire system sessions (Leukfeldt et al., 2017). Cyber detection techniques such as checking mistakes from many authority' claims, email inspection through internet protocol, and network intrusion detection systems to track and detect incoming and outcoming traffic on the network system help prevent cybercrimes (Malik & Younis, 2016).

The theme of cybersecurity response is supported by the RAT conceptual framework. Kayser et al. (2019) suggested that criminological theory can reduce crime rates relative to social engineering. Organizations should be well prepared and develop capable cybersecurity responses to address on time and efficiently all the security threats they face daily; otherwise, the cost of being cyber-attacked will be very costly for them.

Martin et al. (2017) estimated that data breaches are bad for performance and the effect of data breach reaches a worse level when a firm is affected more than one time.

The NIST documents expressed by all the participants of this study during the interview reveal the use of cybersecurity response by organizations to prevent cybercrimes and support this theme, as shown in Table 7.

Table 7

NIST Documents to support the Theme 2 expressed by participants.

NIST Documents	Cybersecurity Response
NIST Framework 800-18	x
NIST Framework 800-30	
NIST Framework 800-37	x
NIST Framework 800-39	
NIST Framework 800-53	x
NIST Framework 800-53A	x
NIST Framework 800-61	x
NIST Framework 800-81	
NIST Framework 800-82	x
NIST Framework 800-137	x
NIST Framework 800-161	x
NIST Framework 800-171	x
NIST Risk Management	x

Theme 3: Cybersecurity Awareness as a Culture

Cybersecurity awareness as a culture emerged as the third theme of this study' findings. Information security culture can reduce the threat of humans to information protection and help mitigate data breaches or incidents in organizations (Da Veiga et al., 2020). Understanding organizational culture is essential in the understanding and the definition of security culture (Wiley et al., 2020). Awareness culture represents an expectation and practice adopted by organizations to ensure that cybersecurity culture is

taken seriously to prevent cyberattacks within the organization in the long run. The literature of this study supports this vision. Cybersecurity awareness culture encourages acceptable user behavior in the reality of cyberspace. It is also the intended and unintended way cyberspace is used from an international, national, organizational, or individual perspective regarding the attitudes, assumptions, beliefs, values, and knowledge of the cyber user (Gcaza & von Solms, 2017). Identifying important cyber security behaviors, establishing a winning cybersecurity network, developing a brand for the cyber-team, building a cybersecurity hub, and aligning security awareness activities with the internal and external campaign are essential to improve cybersecurity culture (Alshaikh, 2020). PA1, PA2, PA3, PA5, and PA7 of this study have expressed relevant viewpoints about culture. PA1 stated,

> You know you can't have employees or end-users who think that cybersecurity training or awareness is just another duty or responsibility they have to do, they've got to understand the importance of protecting the information and information systems, and ultimately you're protecting their jobs.

PA1 also noted the importance of the awareness culture, which help him to push down as a result of getting the senior leadership on board with the strategy and hopefully influencing cybersecurity culture.

PA2 stated," If you don't change somebody on preventing something, then that person is completely ignorant of it, cannot identify it." PA2 suggested that it is vital for organizations to train their employees to identify potential cyberattacks and to be able to

immediately report it as part of the awareness culture that says if you do not know something, or if you feel something, you say something.

PA3 estimated that awareness culture is something fundamental, and so far, all the organizations he has been working for took this as a natural culture. PA3 estimated that awareness culture is definitely something very important, and so far, all the organizations that he has been working for took this as a natural culture basically. PA3 also suggested that organization regardless of whether it's in nonprofit organization, private or governmental should really take into consideration the security aspects by making them a culture in their mind by ensuring all the time that all the critical assets are fully protected. In addition, organization should make sure to do some real annual or reviews on all the controls, pass all the audits, perform quarterly or BI yearly assessment, for any type of controls, ensure that twice a year, to go over all the standards, all the processes, all the workflow as well as all the policies that were already written and make sure that everything is working properly.

PA5 considered cybersecurity in his environment as something his organization takes seriously. When it comes to his organization, they invest a lot in security and ensure that they have everything they need to perform their duties. For PA5, awareness culture is part of his organization. When it comes to cybersecurity, before they hire a person, they screen him to make sure that this is where your passion, because they do not want to bring somebody in that is not passionate about cybersecurity because the first of what embrace cybersecurity as the main activity over there.

PA7 stated, “So, we don't play when it comes to cybercrimes, so it is a culture for us because we know where we are working and what the attackers are trying every day to hack our system.” PA7 also suggested that his organization paid attention to cybersecurity culture because he works in an environment where cyber-attackers seek confidential information. So, they are very hands-on in that aspect. PA6 commented on cybersecurity culture with his organization but pointed the importance of constantly keeping the eyes in preventing cyberattacks by constantly training employees/end-users because cybercriminals’ goal is to target relevant information. All participants of this study agree that cybersecurity is very costly for organizations every year, as shown in Table 8, which maintains a vigilance awareness culture within the organization.

Table 8

Organization Spending on Cybersecurity expressed by participants.

Participants	Organization Spending in US Dollar
PA1	3 million/year
PA2	Not disclosed
PA3	1 billion/5 years
PA4	1 million/year
PA5	Up to 700,000/year
PA6	Not disclosed
PA7	1 trillion/year

All participants stated that cybercriminals target essential information such as classified information, passwords, data, and personally identifiable information detailed in Table 9, which is vital in building an awareness culture to prevent cyberattacks.

Table 9

Most targeted Information by Cybercriminals expressed by participants.

Targeted Elements	Participant' Count
Classified Information	
Confidential Information	1
Secret Information	1
Top Secret Information	1
Organization 'Data	3
Password	1
Personally Identifiable Information (PII)	
Intellectual property	4
Social security number	1
Credit card information	2

All participants expressed their viewpoints on the impact of cyberattacks on their organizations, as detailed in Table 10, which is very important to have a good awareness culture that will avoid disastrous consequences for its image.

Table 10

Impacts of Cybercrimes on Organizations expressed by participants.

Impacted Elements	Participant' Count
Loss of revenue due to data breaches	2
Loss of intellectual property	2
Loss of confidential or/and sensitive information	3
Loss of employments	1
Loss of credibility and trust	1

One piece of the information from each participant is that cyber-attackers are not discouraged from cyberattack organization network infrastructure. The frequency of attacks and the techniques used depend on the type of organization and the information they are looking for, as shown in Table 11, showing the frequency and method of attacks that participants deal with within their organizations. So, an organization will be more targeted than others because of the nature of its activities. That also raises the importance of an awareness culture within organizations that contributes to developing a culture of vigilance on cybersecurity threats they face daily.

Table 11

Frequency of Cyberattacks expressed by participants.

Participants	Frequency of Cyberattacks
PA1	Daily (1000 Phishing attacks/Malicious emails)
PA2	Daily (Phishing, Social engineering attacks/Malicious emails)
PA3	Daily (Multiple attempts of phishing attacks/DoS attacks)
PA4	Yearly (Two times a year/Persistent threat/Advanced persistent threats)
PA5	Yearly (One to two a year/Phishing attacks)
PA6	Most of the time during Holidays (Juice Jacking attacks)
PA7	Daily (Phishing attacks)

The cybersecurity awareness as a culture theme supports the study literature and is consistent with Wiley et al. (2020). Organizations should focus on a security culture to improve information security awareness and save time and resources, which depend on the importance of leaders in the encouragement of positive security behaviors through strategic management and planning, communication, and transparent decision-making processes (Wiley et al., 2020). Barosy (2019) suggested that establishing and sustaining a

safe cyber environment may create a climate of trust and safety as part of the cybersecurity culture. In contrast, Kakucha and Buya (2018) estimated that establishing a comprehensive plan to enable the development, institutionalization, assessment, and improvement of an information security program is a way to develop a cybersecurity culture within organizations. Sabillon et al. (2019) insisted that cybersecurity culture must be the result of creating a cybersecurity awareness program that delivers training continuously.

RAT framework supports the cybersecurity awareness as a culture theme. Chen et al. (2017) suggested that the threat assessment comprises the outcomes of risk-taking, including perceptions of vulnerability, severity, and the rewards of risky behavior. This opinion is consistent with the approach of cybersecurity culture in which end-users/employees should be involved and part of the protection of all security aspects related to their organizations. Yar (2005) suggested that the concept of capable guardianship is similar to cyberspace. Protecting an organization from being cyber-attacked is the same as physically safeguarding an organization's property, which should be viewed as a normal way to operate any organization.

The NIST document reviewed supports these themes, as shown in Table 12. The participants expressed their opinions on this theme, which corroborate with information extracted from NIST documents cited during the interviews.

Table 12

NIST Documents to support the Theme 3 expressed by participants.

NIST Documents	Cybersecurity as a Culture
NIST Framework 800-18	
NIST Framework 800-30	x
NIST Framework 800-37	
NIST Framework 800-39	x
NIST Framework 800-53	
NIST Framework 800-53A	
NIST Framework 800-61	
NIST Framework 800-81	
NIST Framework 800-82	x
NIST Framework 800-137	
NIST Framework 800-161	x
NIST Framework 800-171	
NIST Risk Management Framework	x

Theme 4: Train End-users/Employees

Train end-users/employees frequently is the fourth theme of this study as a security awareness strategy to prevent cybercrimes based on collected data from multiple participants. PA1 reported that training end-users/employees are essential to prevent cybercrimes because people are the weakest links in the organization. That viewpoint reflects the opinion of other participants of this study. Security education and awareness training effectively reduce users' susceptibility to phishing attempts via the training material (Tschakert & Ngamsuriyaroj, 2019). Zwilling et al. (2020) estimated that organizations and educational institutions must develop adequate training programs by providing security awareness training courses that can comprehensively influence attitudes to information security management and improve cyber security awareness.

Miranda (2018) estimated that an organization and its users must be trained before you can test their abilities to detect and respond to cyberattacks, which should be initiated only with the expressed consent of the organization's leaders that is necessary to develop training exercise scenarios.

Those viewpoints converge with this study. Research revealed the importance to well training end-users/employees in the prevention of cybercrimes. The feedback of all the participants noted that organizations prefer spending quite some money every year to train their employees/end-users and prevent cyberattacks (Table 9), to protect against cyberattacks, training end-users/employees is very worthy, compared to the consequences of being cyber- attacked.

All the participants expressed their viewpoints about security awareness training used in their organizations to prevent cyberattacks. PA1 and PA2 reported that training end-users/employees should be done frequently to keep end-users/employees informed on new security threats and risks they face daily.

PA1 stated, “We have a pretty aggressive phishing training program, so employees understand the basics of identifying a phish and if there's any doubt whatsoever.” PA1 declared that his organization took the training of the end-users/employees very seriously and stated that security awareness is sometimes costly for organizations and indicated that he has a budget of 3 million US dollars yearly allocated in the training and prevention of cyberattacks within his organization. PA1 added that they have a phishing button embedded within outlook with a selected email, hook it with the fishing boating button and submit it to the Infosec desk. Then they will do the initial

triage or potential forensics to see if it is valid or not. If it is an actual phishing event, they will report it to their partners, whether Microsoft, McAfee, or other advanced industrial-based contractors or intelligence agencies. So, they hook that and send it. You know it is deleted from them.

PA2 stated, “We create the program that all our employees have a kind of training; let me say a quarterly or kind of awareness training quarterly that everybody participates from C-suite to janitorial because there is one thing we fail to do.” PA2 added that his organization provides security awareness training quarterly as part of its strategy to prevent cyberattacks. PA2 stated that people think that cyberattack is just for the top-ranking people in the company or the IT specialist but forget to think about these janitorial those that clean the company, those sectors that work on the computers. PA2 believed that the awareness in his organization embodies everybody to be aware of the risk and the threat out there in such a case that if the janitorial is working and somebody walks into the organization, he should know who this person is and what they are doing. Because that is a risk, and if that person is not aware of it, he will give access to that person to like getting anything he or she wants. That is why his organization conducts that action from top to bottom. PA3 stated,

> So usually, what we do here is we conduct like some failure detection. I call it a mock test, so those tests are like to try to mimic some type of attacks, let's say phishing and so on without even letting the end users know, without letting the employees know.

PA3 also reported that his organization leads security awareness training for their employees. His organization conducts a mock test at least twice a year and runs a phishing campaign or cyberattack campaign to see the number of people who will just fall under that category. Whoever will not follow the process will get caught. Then based on the number of those people, they decide what they increase more awareness when it comes to best practices. PA3 stated that by doing so, they could redefine again all the yearly training that should be done so they can reduce those risks due to the lack of knowledge and experience of some end-users toward those techniques. In addition, PA3 stated that more tests of the king are running along with some attacks exercise among teams and departments to see what kind of vulnerabilities and backdoor each team can find to agree on how they can better protect the organization.

PA4 stated: “To prevent cybercrimes, number one: hours of training. We train users/employees, so they are aware of cyber threats.” PA4 also declared that they have a defense in depth and defense in bread processes in place, which implements adequate security measures to prevent cybercrimes for the security controls. PA4 qualified a cybercrime as a threat, and the easy thing to do is reduce vulnerabilities because risks always exist. Therefore, there is a need to put security measures in place to reduce threats from exploiting vulnerabilities.

PA5 stated,” The first thing you want do is to educate yourself because you are like a model to the other people because when you educate yourself, you will know how to train others, so I keep myself current to my research.” PA5 acknowledged the importance of doing a lot of awareness training of other users, especially when

identifying different phishing campaign emails using tools such as KnowBe4, which is a tool they use to train users on how to identify a phishing email. PA5 also discussed the importance of ensuring they have a good system hardening, such as Firewall, access controls, IDS, IPS, and having monitoring tools such as SIEM tools like Splunk, Curator.

PA6 stated, “Most of the time during the onboarding process, we try to see how we can actually make sure all employees undergo security awareness training.” PA6 also stated that the mentioned process would help them to identify threats and avoid the system from being attacked. PA6 underlined that security awareness training is beneficial to ensure that employees comply with these norms before they gain access to the system. No organization would bring in criminals where you can be an insider, trading card information and sending it out there, but that can be prone to attacks. PA6 stated that it is vital to make sure the employees do their due diligence during the onboarding process and ensure that they go through the required standard process before gaining access to the system and ensuring their access is in line with the password policy chart.

PA7 stated,” The challenge that we use is to conduct a campaign by sending sometimes everyone month or every Friday malicious link to set up employees to see if any of them gonna fall for that so try to track how many people failed”. PA7 addressed the importance of testing security awareness in the work environment to see if employees are aware of the threats that they face when they receive a phishing email link. By clicking on it, employees demonstrate that there are not well aware and prepared to avoid any cyberattacks. PA6 said that they use such technique to score and rate his organization, which is audited by an outside organization that may be the one who sent

sometime those phishing campaigns, and not his security awareness team. PA7 stated that his organization carries cybersecurity chain and audit; how can they be exported? How can they prevent those types of cybersecurity chain? According to PA6, it is all about education as a culture where they get people every time about all this steps. They have URL set; they go for different vulnerabilities, Common Vulnerability Scoring (CVS) or Common Vulnerability Scoring System (CVSS). They use all these platforms in order to educate people. They search for the vulnerabilities instead of dealing with vulnerabilities. They look at the vulnerabilities. Sometimes they talk through the remediation plan that may use as a strategy to teach whatever employees how to avoid all these cyber-treats that are out there.

The theme of training of end-users/employees is aligned with the literature. Cybersecurity awareness programs must include adequate training aligned with the organization's objectives and long-term investment (Sabillon et al., 2019). The use of phishing emails by cybercriminals allows for personal and sensitive information, which are substantial online privacy concerns (Kumar et al., 2016). This approach is consistent with some of the techniques described by the study participants that cybercriminals use to gain access to an organization's network infrastructure.

The RAT framework supports the theme of training of end-users/employees. Argun and Dağlar (2016) stated that deviant behavior occurs in the presence of three elements: a suitable target, a lack of a suitable guardian, and a motivated offender. When those three elements are reunited, it can lead to cybercrime. Cybersecurity awareness programs, in this case, contribute to educate and train end-users/employees to detect

those elements so they can prevent cyberattacks. Chen et al. (2017) suggested that opening emails from unknown resources can lead users to access websites that are not safe and may see their computers infected with malicious codes. This fact is consistent with the approach of training end-users/employees in the prevention of cybercrimes.

NIST documents from the interviews also corroborate this theme, as shown in Table 13. The documents addressed specific aspects of the security awareness program and the importance for organizations to train their end-users/employees to become more aware of new security threats.

Table 13

NIST Documents to support the Theme 4 expressed by Participants

NIST Documents	Training of the End-users/Employees
NIST Framework 800-18	x
NIST Framework 800-30	
NIST Framework 800-37	x
NIST Framework 800-39	x
NIST Framework 800-53	x
NIST Framework 800-53A	x
NIST Framework 800-61	x
NIST Framework 800-81	
NIST Framework 800-82	x
NIST Framework 800-137	x
NIST Framework 800-161	x
NIST Framework 800-171	x
NIST Risk Management Framework	x

Applications to Professional Practice

This study aimed to address security awareness strategies used by information security officers to prevent cybercrimes by cybercriminals. The study's findings show

the relevance of security awareness strategy approaches to prevent cyberattacks from intruders. On the one hand, cybercrime cases have significantly increased over time and continue to cost organizations billions of US dollars each year regarding financial or/and intellectual property losses. However, on the other hand, organizations have recognized the importance of security awareness training for their employers as a "culture thing" so they can become more aware of cybercrimes in all its aspects by equipping them with adequate knowledge and tools that will help them to detect and prevent cyberattacks before it spreads within the organization, which could be very risky and costly for them for their activities when cyberattacks are not detected and escalated on time to quickly mitigate security incidences on the organization's resources and network infrastructure.

Based on the finding of this study, strong network infrastructure is not enough to protect organization for been cyber-attacked because cyber-attackers target mostly end-users/employees via phishing techniques in order to gain quick access to the organization network infrastructure and cause some harm.

The compliance to policies in place regarding cybersecurity is very useful in the prevention of cyberattacks within the organization and allows a better respect of the security procedures needed to minimize intrusions and cyberattacks.

The implementation of a strong cybersecurity response within the organization is an efficient measure to response on time to cyberattacks that face the organization in the daily bases and avoid disruption of service.

The development of a real cybersecurity culture within the organization is a positive way to aware the end-users/employees about the security risks and threats they face every day and make them part of the prevention of cyberattacks.

The training of end-users/employees frequently contributes in the prevention of cyberattacks within the organization in long run and increases their knowledge in that regard.

When all these mentioned measures are implemented efficiently within the organization, it becomes difficult for cyber-attackers to gain access to the organization network infrastructure and commit a cybercrime. Moreover, the mentioned elements contribute to ensure in long run the safety of the organization in terms of cyberattacks and allow the organization to save a lot of money in terms of business losses and ensure business continuity.

The study findings may enhance IT understanding of best learning and security practices relative to cybersecurity. They will improve the approach that IT professionals use to deal with threats and risks linked to cybercrimes. Information security officers may be inspired by the study's findings to improve the way they handle cybersecurity response and develop consistent cybersecurity policies and enhance the training of end-users/employees in the prevention of cyberattacks.

Participants of this study reported a significant reduction of cyberattacks within their organizations since they received frequent security awareness training on cybercrimes and observed security policies and guidelines implemented by their organizations in that regard. Therefore, the findings from this study can contribute to an

organization’s awareness about the effective security awareness strategies they can use to prevent cybercrimes in the long run and avoid business disruption in case of cyberattacks.

Implications for Social Change

The findings from this study may contribute to creating a culture of learning based on best security awareness practices used to prevent cyberattacks, which can also be used by organizations to improve the way they approach the fight against cybercrimes. Organizations are more preoccupied with the safety of their data and intellectual properties, representing important assets that contribute to meeting their daily goals and objectives and ensuring business continuity. The protection of the information/data within an organization is not solely the role of the system and network administrator but the involvement of all the stakeholders who use the organization's resources for business purposes. Moreover, a successful cyberattack may be very costly to an organization in terms of financial, material, data or/and intellectual property losses. That is the reason why organizations should involve their employees/end-users in the prevention of cyberattacks via frequent cybersecurity awareness training programs viewed as one of the efficient recipes for a better prevention against cybercrimes.

The implications for social change on people’s behaviors as they understand the cybercrime threats and risks in their communities, neighborhoods, organizations. They may become aware of the real threats they face daily and the impacts when exposed to cyber criminals via the Internet and social networks. The study will contribute to increase

people' vigilance and equip them to detect and prevent cyberattacks, which could transform their old behaviors and habits into a recurrent cyber-culture of awareness.

Recommendations for Action

The significant increase in cybercrimes every year demonstrates the importance of organizations focusing on the real causes of the problem rather than the solutions. The fundamental cause of the cybercrimes' phenomenon is linked to human behavior and its ability to use news and powerful technology tools and techniques to perpetrate their crime online. People and organizations also should acknowledge the inability of a machine to perpetrate a cybercrime on its own without the intervention or involvement of a human being. All this is to point the hand and participation of a human being behind any cyber-attacks. Cybercrimes will not disappear suddenly in our society as far as a human being is concerned and sophisticated technologies are developed in that regard.

Recommendations help further increase research coverage on the essential organizational stakeholder (Brauer & Wiersema, 2018). Based on the findings, my main recommendation is for organizations to focus their attention on the prevention aspect of the cybercrime phenomenon rather than the cure aspect. In that manner, the security awareness training approach appears to bring a quick and efficient way to prevent cybercrimes in the long run because it involves the participation of all the parties in the prevention of cyberattacks through the compliance of guidelines and policies implemented in the prevention of cybercrimes, which contributes to empower all the involved parties and make them part of the solution instead of being part of the problem.

IT professionals also have the responsibility to seek real solutions to prevent cybercrimes in the long run. Therefore, they should continue to work very closely with other IT professionals, experts, and engineers in the field to develop relevant approaches to preventing cybercrimes.

The findings of this study are made available to the public for educational purposes. This study is published in the academic database called ProQuest.

I also recommend that organizations follow the path of security awareness training programs; compliance with policies and guidelines in that regard; the implementation of a security response plan in case of a cyberattack, and the development of a culture of cybersecurity awareness as best practices to prevent cybercrimes in the long run. The previous recommendations are not very costly but very efficient compared to the cost they can spend to recover from a cyberattack on a large scale. The possibility of disruption of service may affect business continuity.

Recommendations for Further Study

The economic impact of cybercrimes on people, organizations, and government entities is enormous and costly. Therefore, my study has explored some aspects of the security awareness strategies to prevent cybercrimes by cybercriminals, which are very important in mitigating cyberattacks in the long run.

Further study needs to be done to extend my study analysis by focusing intensely on the social engineering aspects of the prevention that need to be considered when addressing security awareness strategies to prevent cybercrimes in the context of information security. Social engineering in information security can play a huge role in

addressing security threats that may face people in charge of ensuring data security and manipulating sensitive data within an organization. In social engineering attacks, intruders push individuals or enterprises to accomplish actions that benefit attackers or provide them with sensitive data such as social security numbers, health records, and passwords (Salahdine & Kaabouch, 2019). It is essential to acknowledge that security threats can also come from the inside than from the outside of the organization. So, it is vital to address that aspect to ensure that organizations have the right and trusted people at the right place regarding the access and the protection of their own IT data and assets.

Another limitation of this study is its geographical area which is limited to the Northeast coast of the United States. It would have been more interesting to explore other geographic regions to see what security awareness strategy approaches use other countries to prevent cybercrimes.

Reflections

Completing a DIT doctoral study is a challenging process that requires a lot of patience and perseverance. Certainly, it has the merit to test the doctoral student's ability in different aspects of the doctoral writing and research process until the finish line, which is graduation. The topic that I chose for this study allowed me to provide a deep analysis of relevant security awareness strategies to prevent cybercrime. My research findings will contribute to the edification of people and organizations in how they should view and prevent cybercrimes in the long run. I continue to say that cybercrime is not a matter of an organization, business, or government entity but a matter of everybody's responsibility. We should fight such phenomenon with our last energy by remaining

vigilant due to the negative impacts that such phenomenon has on people, businesses, organizations, and governments around the world in terms of economic, financial, and security consequences.

Summary and Study Conclusions

Cybercrimes are illegal and malicious activities that generate billions of U.S. dollars in financial losses for businesses, organizations, and governments worldwide every year. Such losses are due partly to the lack of understanding of such phenomena and the effective way of preventing them most efficiently. My research study that addresses security awareness strategies used to prevent cybercrimes by cybercriminals can be a recipe in preventing such phenomenon because it lays out the crucial aspects of preventing such phenomenon in the long run. Because people are often unaware of the phenomenon, cyber attackers exploit their weaknesses to cyberattack them by using new high-tech tools and techniques available in the market today. The study findings reveal the importance of following policies that provide a viable cybersecurity response plan in case of a cyberattack, to develop a cybersecurity culture within the organization, so it becomes part of their habits and to frequently train their employees/end-users on how to prevent against cybercrimes by making them a part of the solution in the prevention of such phenomenon instead of part of the problem. These approaches allow employees/end-users to learn best security practices that will help them quickly identify, detect, and make appropriate security decisions to mitigate cyberattacks.

My research study will offer strategies for businesses and organizations that face cybercrimes daily and contribute to establishing a culture of security awareness learning

and training best practices in the long run that will contribute to prevent more efficiently cybercrimes and allow them to meet their security awareness goals and objectives.

References

Abdalla, M. M., Oliveira, L. G. L., Azevedo, C. E. F., & Gonzalez, R. K. (2018). Quality in qualitative organizational research: Types of triangulation as a methodological alternative. *Administração: Ensino e Pesquisa*, *19*(1), 66-98. https://doi.org/10.13058/raep.2018.v19n1.578

Abernathy, J., Stefaniak, C., Wilkins, A., & Olson, J. (2017). Literature review and research opportunities on credibility of corporate social responsibility reporting. *American Journal of Business, 32*(1), 24-41. https://doi.org/ 10.1108/AJB-04-2016-0013

Adhabi, E., & Anozie, C. B. (2017). Literature review for the type of interview in qualitative research. *International Journal of Education, 9*(3), 86-97. https://doi.org/10.5296/ije.v9i3.11483

Agana, M. A., & Wario, R. (2018). A multi-level evidence-based cybercrime prosecution information system. *International Journal of Engineering & Technology*, *7*, 39-48. ResearchGate. https://www.researchgate.net/profile/Ruth_Wario/publication/326905155_A_Multi-level_Evidence-based_Cyber_Crime_Prosecution_Information_System/links/5b6b5781a6fdcc87df6dcce3/A-Multi-level-Evidence-based-Cyber-Crime-Prosecution-Information-System.pdf

Alase, A. (2017). The interpretative phenomenological analysis (IPA): A guide to a good qualitative research approach. *International Journal of Education and Literacy Studies*, *5*(2), 9-19. https://doi.org/10.7575/aiac.ijels.v.5n.2p.9

Al-Daeef, M. M., Basir, N., & Saudi, M. M. (2017, July). Security awareness training: A review. In *Proceedings of the World Congress on Engineering* (Vol. 1, pp. 5-7). AI2 Allen Institute for AI. https://pdfs.semanticscholar.org/f040/209717c34624dcb97ccd3ca8acc2e0d8ed93.pdf

Aldawood, H., & Skinner, G. (2019). Reviewing cybersecurity social engineering training and awareness programs—Pitfalls and Ongoing Issues. *Future Internet*, *11*(3), 73. https://doi.org/10.3390/fi11030073

Aldiabat, K. M., & Le Navenec, C. L. (2018). Data saturation: The mysterious step in grounded theory methodology. *Qualitative Report*, *23*(1), 245-261. https://nsuworks.nova.edu/tqr/vol23/iss1/18

Alex, M. E., & Kishore, R. (2017). Forensics framework for cloud computing. *Computers & Electrical Engineering*, *60*, 193-205. https://doi.org/10.1016/j.compeleceng.2017.02.006

Alohali, M., Clarke, N., Li, F., & Furnell, S. (2018). Identifying and predicting the factors affecting end-users' risk-taking behavior. *Information & Computer Security*. https://doi.org/10.1108/ICS-03-2018-0037

Alotaibi, F., Furnell, S., Stengel, I., & Papadaki, M. (2016). A review of using gaming technology for cyber-security awareness. *International Journal for Information Security Research (IJISR), 6*(2), 660-666. https://infonomics-society.org/wp-content/uploads/ijisr/published-papers/volume-6-2016/A-Review-of-Using-Gaming-Technology-for-Cyber-Security-Awareness.pdf

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security*, *98*, 102003. https://doi.org/10.1016/j.cose.2020.102003

Amankwaa, L. (2016). Creating protocols for trustworthiness in qualitative research. *Journal of Cultural Diversity*, *23*(3). National Library of Medicine. https://www.ncbi.nlm.nih.gov/pubmed/29694754

Anandarajan, M., & Malik, S. (2018). Protecting the Internet of medical things: A situational crime-prevention approach. *Cogent Medicine*, *5*(1), 1513349. https://doi.org/10.1080/2331205X.2018.1513349

Arachchilage, N. A. G., Love, S., & Beznosov, K. (2016). Phishing threat avoidance behaviour: An empirical investigation. *Computers in Human Behavior*, *60*, 185-197. https://doi.org//10.1016/j.chb.2016.02.065

Argun, U., & Dağlar, M. (2016). Examination of routine activities theory by the property crime. *Journal of Human Sciences*, *13*(1), 1188-1198. https://doi.org/10.14687/ijhs.v13i1.3665

Asiamah, N., Mensah, H. K., & Oteng-Abayie, E. F. (2017). General, target, and accessible population: Demystifying the concepts for effective sampling. *The Qualitative Report*, *22*(6), 1607-1621. https://nsuworks.nova.edu/tqr/vol22/iss6/9

Aspers, P., & Corte, U. (2019). What is qualitative in qualitative research. *Qualitative Sociology*, *42*(2), 139-160. https://doi.org/10.1007/s11133-019-9413-7

Awada, G. (2016). Effect of WhatsApp on critique writing proficiency and perceptions toward learning. *Cogent Education, 3*(1), 1264173. https://doi.org/10.1080/2331186X.2016.1264173

Babinski, A. (2015). State activities in the securing of cyberspace. *Internal Security, 7*(2), 217-235. https://doi.org/10.5604/20805268.1212124

Bai, J., Shi, Q., & Mu, S. (2019). A malware and variant detection method using Function call graph isomorphism. *Security and Communication Networks, 2019*. https://doi.org/10.1155/2019/1043794

Barlow, C. (2020, April). Human subjects protection and federal regulations of clinical trials. In *Seminars in Oncology Nursing* (p. 151001). WB Saunders. https://doi.org/10.1016/j.soncn.2020.151001

Barosy, W. (2019). Successful operational cybersecurity strategies for small businesses. Walden University. https://scholarworks.waldenu.edu/dissertations/6969/

Beck, A., & Hopkins, M. (2017). Scan and rob! Convenience shopping, crime opportunity and corporate social responsibility in a mobile world. *Security Journal*, *30*(4), 1080-1096. https://doi.org/10.1057/sj.2016.6

Bender, J. L., Cyr, A. B., Arbuckle, L., & Ferris, L. E. (2017). Ethics and privacy implications of using the internet and social media to recruit participants for health research: A privacy-by-design framework for online recruitment. *Journal of Medical Internet Research*, *19*(4), e104. https://doi.org/ 10.2196/jmir.7029

Bengtsson, M. (2016). How to plan and perform a qualitative study using content analysis. *NursingPlus Open*, *2*, 8-14. https://doi.org/ 10.1016/j.npls.2016.01.001

Bhatia-Lin, A., Boon-Dooley, A., Roberts, M. K., Pronai, C., Fisher, D., Parker, L., Engstrom, L., Ingraham, D., & Darnell, D. (2019). Ethical and regulatory considerations for using social media platforms to locate and track research participants. *The American Journal of Bioethics*, *19*(6), 47-61. https://doi.org/10.1080/15265161.2019.1602176

Birt, L., Scott, S., Cavers, D., Campbell, C., & Walter, F. (2016). Member checking: a tool to enhance trustworthiness or merely a nod to validation?. *Qualitative health research*, *26*(13), 1802-1811. https://doi.org/10.1177/1049732316654870

Blair, M. E., Le, M. D., & Sterling, E. J. (2017). Multidisciplinary studies of wildlife trade in primates: Challenges and priorities. *American journal of primatology*, *79*(11), e22710. https://doi.org/ 10.1002/ajp.22710

Boetig, B. P. (2006). The routine activity theory: A model for addressing specific crime issues. *FBI Law Enforcement Bulletin*, *75*, 12. HEINONLINE. https://heinonline.org/HOL/LandingPage?handle=hein.journals/fbileb75&div=59&id=&page=

Borrion, H., & Dehghanniri, H. (2019). Crime scripting: a systematic review. *European Journal of Criminology*. Cyber Technology Institute, De Montfort University, Department of Security and Crime Science, UCL-UK. https://discovery.ucl.ac.uk/id/eprint/10072755/3/Borrion%20crime%20scripting_submitted.pdf

Bouveret, A. (2019). Estimation of losses due to cyber risk for financial institutions. *Journal of Operational Risk, Forthcoming.* SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3391740

Brady, P. Q., Randa, R., & Reyns, B. W. (2016). From WWII to the world wide web: A research note on social changes, online "places," and a new online activity ratio for routine activity theory. *Journal of Contemporary Criminal Justice, 32*(2), 129. https://doi.org/10.1177/1043986215621377

Brauer, M., & Wiersema, M. (2018). Analyzing analyst research: A review of past coverage and recommendations for future research. *Journal of Management, 44*(1), 218-248. https://doi.org/10.1177/0149206317734900

Broman, K. W., & Woo, K. H. (2018). Data organization in spreadsheets. *The American Statistician, 72*(1), 2-10. https://doi.org/10.1080/00031305.2017.1375989

Bruce, A., Beuthin, R., Sheilds, L., Molzahn, A., & Schick-Makaroff, K. (2016). Narrative research evolving: Evolving through narrative research. *International Journal of Qualitative Methods, 15*(1). https://doi.org/10.1177/1609406916659292

Butt, U. J., Abbod, M. F., & Kumar, A. (2020). Cyber threat ransomware and marketing to networked consumers. In *Handbook of Research on Innovations in Technology and Marketing for the Connected Consumer*, 155-185. IGI Global. https://doi.org/ 10.4018/978-1-7998-0131-3.ch008

Caneppele, S., & Aebi, M. F. (2017). Crime drop or police recording flop? On the relationship between the decrease of offline crime and the increase of online and

hybrid crimes. *Policing: A Journal of Policy and Practice.* https://doi.org/10.1093/police/pax055

Carter, D. D., Robinson, K., Forbes, J., Walsh, J. C., & Hayes, S. (2019). Exploring the perspectives of stroke survivors and healthcare professionals on the use of mobile health to promote physical activity: A qualitative study protocol. *HRB Open Research*, *2*. https://doi.org/10.12688/hrbopenres.12910.1

Castillo-Montoya, M. (2016). Preparing for Interview Research: The Interview Protocol Refinement Framework. *The Qualitative Report, 21*(5), 811-831. https://nsuworks.nova.edu/tqr/vol21/iss5/2

Catota, F. E., Morgan, M. G., & Sicker, D. C. (2018). Cybersecurity incident response capabilities in the Ecuadorian financial sector. *Journal of Cybersecurity, 4*(1), tyy002. https://doi.org/10.1093/cybsec/tyy002

Chan, J., Ghose, A., & Seamans, R. (2016). The internet and racial hate crime: offline spillovers from online access. *MIS Quarterly*, *40*(2), 381-403. https://doi.org/10.2139/ssrn.2335637

Chastain, B., Qiu, F., & Piquero, A. R. (2016). Crime theory evaluation using simulation models of residential burglary. *American Journal of Criminal Justice*, *41*(4), 814-833. https://doi.org/10.1007/s12103-016-9336-8

Chaudhry, P. E. (2017). The looming shadow of illicit trade on the internet. *Business Horizons*, *60*(1), 77-89. https://doi.org/10.1016/j.bushor.2016.09.002

Chavez, N., & Bichler, G. (2019). Guarding against Cyber-Trespass and Theft: Routine Precautions from the Hacking Community. *International Journal of Cyber*

Criminology, *13*(1). http://www.cybercrimejournal.com/Chavez&Bichlervol13issue1IJCC2019.pdf

Chen, H., Beaudoin, C. E., & Hong, T. (2017). Securing online privacy: An empirical test on Internet scam victimization, online privacy concerns, and privacy protection behaviors. *Computers in Human Behavior*, 70, 291-302. https://doi.org/10.1177/1461444820902103

Cheng, X., Fu, S., & de Vreede, G. J. (2017). Understanding trust influencing factors in social media communication: A qualitative study. *International Journal of Information Management*, *37*(2), 25-35. https://doi.org/10.1016/j.ijinfomgt.2016.11.009

Chetty, K., Qigui, L., Gcora, N., Josie, J., Wenwei, L., & Fang, C. (2018). Bridging the digital divide: measuring digital literacy. *Economics: The Open-Access, Open-Assessment E-Journal*, *12*(2018-23), 1-20. https://doi.org/10419/177899

Cho, S., Hong, J. S., Espelage, D. L., & Choi, K. S. (2017). Applying the lifestyle routine activities theory to understand physical and nonphysical peer victimization. *Journal of Aggression, Maltreatment & Trauma, 26*(3), 297-315. https://doi.org/10.1080/10926771.2016.1264526

Choi, K., & Lee, J. R. (2017). Theoretical analysis of cyber-interpersonal violence victimization and offending using cyber-routine activities theory. *Computers in Human Behavior, 73,* 394-402. https://doi.org/10.1016/j.chb.2017.03.061

Choi, K., Cronin, S., & Correia, H. (2016a). The assessment of capable guardianship measures against bullying victimization in the school environment. *Police*

Practice and Research, *17*(2), 149-159. https://doi.org/10.1080/15614263.2015.1128161

Choi, K., Scott, T. M., & LeClair, D. P. (2016b). Ransomware against police: diagnosis of risk factors via application of cyber-routine activities theory. *International Journal of Forensic Science & Pathology.* Bridgewater State University. https://vc.bridgew.edu/cgi/viewcontent.cgi?article=1029&context=crim_fac

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, *44*(4), 588-608. https://doi.org/10.2307/2094589

Coker, Z., Widder, D. G., Le Goues, C., Bogart, C., & Sunshine, J. (2019). A qualitative study on framework debugging. In *2019 IEEE International Conference on Software Maintenance and Evolution (ICSME)* (pp. 568-579). IEEE. https://doi.org/10.1016/j.ienj.2019.01.005

Connelly, L. M. (2016). Trustworthiness in qualitative research. *Medsurg Nursing*, *25*(6), 435-437. Gale Academic Onefile. https://go.gale.com/ps/anonymous?id=GALE%7CA476729520&sid=googleScholar&v=2.1&it=r&linkaccess=abs&issn=10920811&p=AONE&sw=w

Corcoran, J., Zahnow, R., & Higgs, G. (2016). Using routine activity theory to inform a conceptual understanding of the geography of fire events. *Geoforum*, *75*, 180-185. https://doi.org/10.1016/j.geoforum.2016.07.015

Cruz, R. F., & Tantia, J. F. (2017). Reading and understanding qualitative research. *American Journal of Dance Therapy*, *39*(1), 79-92. https://doi.org/10.1007/s10465-016-9219-z

Cunningham, J. A., Menter, M., & Young, C. (2017). A review of qualitative case methods trends and themes used in technology transfer research. *The Journal of Technology Transfer*, *42*(4), 923-956. https://doi.org/10.1007/s10961-016-9491-6

Daniels, E., Arden-Close, E., & Mayers, A. (2020). Be quiet and man up: a qualitative questionnaire study into fathers who witnessed their Partner's birth trauma. *BMC Pregnancy and Childbirth*, *20*, 1-12. https://doi.org/10.1186/s12884-020-02902-2

Da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. *Computers & Security*, *92*, 101713. https://doi.org/10.1016/j.cose.2020.101713

Deighton-Smith, N., & Bell, B. T. (2018). Objectifying fitness: A content and thematic analysis of# fitspiration images on social media. *Psychology of Popular Media Culture*, *7*(4), 467. https://doi.org/10.1037/ppm0000143

DeJonckheere, M., & Vaughn, L. M. (2019). Semistructured interviewing in primary care research: a balance of relationship and rigour. *Family Medicine and Community Health*, *7*(2), e000057. https://doi.org/10.1136/fmch2018-000057

De Letter, J., van Rooij, T., & Van Looy, J. (2017). Determinants of harassment in online multiplayer games. In *67th Annual ICA Conference: Interventions:*

Communication Research and Practice. Universiteit Gent. https://biblio.ugent.be/publication/8510816

DeLiema, M. (2017). Elder fraud and financial exploitation: Application of routine activity theory. *Gerontologist*, *58*(4), 706-718. https://doi.org/10.1093/geront/gnw258

De Vries, B. (2018). Resonating with reflexive design: On participatory design, narrative research and crystallization. *EDeR. Educational Design Research*, *2*(1). https://doi.org/10.15460/eder.2.1.1184

De Waal, M. M., Christ, C., Dekker, J. J., Kikkert, M. J., Lommerse, N. M., van den Brink, W., & Goudriaan, A. E. (2018). Factors associated with victimization in dual diagnosis patients. *Journal of Substance Abuse Treatment*, *84*, 68-77. https://doi.org/10.1016/j.jsat.2017.11.001

Dijk, J. J. V. (1994). Understanding crime rates: on the interactions between the rational choices of victims and offenders. *British Journal of Criminology*, *34*(2), 105-121. https://doi.org/10.1093/oxfordjournals.bjc.a048398

Dimitriadis, A., Ivezic, N., Kulvatunyou, B., & Mavridis, I. (2020). D4I-Digital forensics framework for reviewing and investigating cyberattacks. *Array*, *5*, 100015. https://doi.org/10.1016/j.array.2019.100015

Dodel, M., & Mesch, G. (2017). Cyber-victimization preventive behavior: A health belief model approach. *Computers in Human Behavior*, *68*, 359-367. https://doi.org/10.1080/01639625.2016.1196985

Drawve, G., Thomas, S. A., & Hart, T. C. (2017). Routine activity theory and the likelihood of arrest: A replication and extension with conjunctive methods. *Journal of contemporary criminal justice*, *33*(2), 121-132. https://doi.org/10.1177/1043986216689747

Drew, J. M., & Farrell, L. (2018). Online victimization risk and self-protective strategies: Developing police-led cyber fraud prevention programs. *Police Practice and Research*, *19*(6), 537-549. https://doi.org/10.1080/15614263.2018.1507890

Drinkwater, K., Dagnall, N., Grogan, S., & Riley, V. (2017). Understanding the unknown: A thematic analysis of subjective paranormal experiences. *Australian Journal of Parapsychology*, *17*(1), 23-46. AIPR, Inc. http://eprints.staffs.ac.uk/3919/3/Drinkwater_Dagnall_Grogan_Riley_2017.pdf

Dwyer, A. J., & Chauveron, L. M. (2016). Wanting "something more": A review of marriage and meaning in Dollahite, Hawkins, and Parr (2012). *Marriage & Family Review*, *52*(4), 360-372. https://doi.org/10.1080/01494929.2015.1099588

Edwards, B., Hofmeyr, S., & Forrest, S. (2016). Hype and heavy tails: A closer look at data breaches. *Journal of Cybersecurity*, *2*(1), 3-14. https://doi.org/10.1093/cybsec/tyw003

Enigbokan, O. K., & Ajayi, N. (2017). Managing cybercrimes through the implementation of security measures. *Journal of Information Warfare, 16*(1), 112-129. Peregrine Technical Solutions, LLC. https://www.jinfowar.com/sites/default/files/u43/JIW_16.1.pdf#page=118

Erlingsson, C., & Brysiewicz, P. (2017). A hands-on guide to doing content analysis. *African Journal of Emergency Medicine*, *7*(3), 93-99.https://doi.org/10.1016/j.afjem.2017.08.001

Faraji, S. L., Ridgeway, G., & Wu, Y. (2018). Effect of emergency winter homeless shelters on property crime. *Journal of Experimental Criminology*, *14*(2), 129-140. https://doi.org/10.1007/s11292-017-9320-4.

Fletcher, A. J. (2017). Applying critical realism in qualitative research: methodology meets method. *International Journal of Social Research Methodology, 20*(2), 181-194. https://doi.org/10.1080/13645579.2016.1144401

Friesen, P., Kearns, L., Redman, B., & Caplan, A. L. (2017). Rethinking the Belmont report?. *The American Journal of Bioethics*, *17*(7), 15-21. https://doi.org/10.1080/15265161.2017.1329482

Fritz, R. L., & Vandermause, R. (2018). Data collection via in-depth email interviewing: Lessons from the field. *Qualitative health research, 28*(10), 1640-1649. https://doi.org/10.1177/1049732316689067

Fusch, P., Fusch, G. E., & Ness, L. R. (2018). Denzin's paradigm shift: Revisiting triangulation in qualitative research. *Journal of Social Change, 10*(1), 2. https://doi.org/10.5590/JOSC.2018.10.1.02

Gavin, J., & Rodham, K. (2017). From ethical rules to ethical puzzles: Research ethics in the digital age. *Psychology Review, 23*(1), 2-5. http://eprints.staffs.ac.uk/3798/4/PsychRev23_1_Rodham.pdf

Gcaza, N., Rossouw, v. S., Grobler, M. M., & Joey Jansen, v. V. (2017). A general morphological analysis: Delineating a cyber-security culture. *Information and Computer Security*, *25*(3), 259-278. https://doi.org/10.1108/ICS-12-2015-0046

Gcaza, N., & von Solms, R. (2017, May). Cybersecurity culture: an ill-defined problem. In *IFIP World Conference on Information Security Education* (pp. 98-109). Springer, Cham. https://hal.inria.fr/hal-01690975/document

Gelinas, L., Pierce, R., Winkler, S., Cohen, I. G., Lynch, H. F., & Bierer, B. E. (2017). Using social media as a research recruitment tool: ethical issues and recommendations. *The American Journal of Bioethics*, *17*(3), 3-14. https://doi.org/10.1080/15265161.2016.1276644

Genç, Z., Masalimova, A. R., Platonova, R. I., Sizova, Z., & Popova, O. V. (2019). Analysis of documents published in scopus database on special education learning through mobile learning: A content analysis. *International Journal of Emerging Technologies in Learning (iJET)*, *14*(22), 192-203. https://doi.org/10.3991/ijet.v14i22.11732

Gerring, J. (2017). Qualitative methods. *Annual Review of Political Science*, *20*, 15-36. https://doi.org/10.1146/annurev-polisci-092415-024158

Ghafir, I., Saleem, J., Hammoudeh, M., Faour, H., Prenosil, V., Jaf, S., Jabbar, S., & Baker, T. (2018). Security threats to critical infrastructure: the human factor. *The Journal of Supercomputing, 74*(10), 4986-5002. Springer Link. https://link.springer.com/article/10.1007/s11227-018-2337-2

Ghazvini, A., & Shukur, Z. (2018). A serious game for healthcare industry: Information security awareness training program for hospital Universiti Kebangsaan Malaysia. *International Journal of Advanced Computer Science and Applications*, *9*(9), 236-245. https://pdfs.semanticscholar.org/ef2d/097c3456967f7c694ce4d41f6316ad12b05f.pdf

Goertzen, M. J. (2017). Introduction to quantitative research and data. *Library Technology Reports*, *53*(4), 12-18. ALATechSource. https://journals.ala.org/index.php/ltr/article/view/6325/8274

Golafshani, N. (2003). Understanding reliability and validity in qualitative research. *The Qualitative Report*, 8(4), 597–607. http://www.nova.edu/ssss/QR/QR8-4/golafshani.pdf

Gordon, L. A., Loeb, M. P., & Zhou, L. (2020). Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model. *Journal of Cybersecurity*, *6*(1), tyaa005, Oxford Academy. https://doi.org/10.1093/cybsec/tyaa005

Gottschalk, P. (2017). Convenience in white-collar crime: Introducing a core concept. *Deviant Behavior*, *38*(5), 605-619. https://doi.org/10.1080/01639625.2016.1197585

Goyal, N., & Goyal, D. (2017). Cybercrime in the society: Security issues, preventions and challenges. *Research Journal of Engineering and Technology*, *8*(2), 73-80. https://doi.org/10.5958/2321-581X.2017.00012.5

Graham, R., & Triplett, R. (2017). Capable guardians in the digital environment: the role of digital literacy in reducing phishing victimization. *Deviant Behavior*, *38*(12), 1371-1382. https://doi.org/10.1080/01639625.2016.1254980

Graneheim, U. H., Lindgren, B. M., & Lundman, B. (2017). Methodological challenges in qualitative content analysis: A discussion paper. *Nurse education today*, *56*, 29-34. https://doi.org/10.1016/j.nedt.2017.06.002

Gupta, P., & Mata-Toledo, R. A. (2016). Cybercrime : in disguise crimes. *Journal of Information Systems & Operations Management*, *10*(1).

Hadi, M. A., & Closs, S. J. (2016). Ensuring rigour and trustworthiness of qualitative research in clinical pharmacy. *International journal of clinical pharmacy*, *38*(3), 641-646. https://doi.org/10.1111/jan.13031

Hamet, P., & Tremblay, J. (2017). Artificial intelligence in medicine. *Metabolism*, *69*, S36-S40. https://doi.org/10.1016/j.metabol.2017.01.011

Hammarberg, K., Kirkman, M., & de Lacey, S. (2016). Qualitative research methods: when to use them and how to judge them. *Human Reproduction*, *31*(3), 498-501. https://doi.org/10.1093/humrep/dev334

Hammersley, M. (2018). What is ethnography? Can it survive? Should it?. *Ethnography and Education*, *13*(1), 1-17. https://doi.org/10.1080/17457823.2017.1298458

Hancock, M. E., Amankwaa, L., Revell, M. A., & Mueller, D. (2016). Focus group data saturation: A new approach to data analysis. *The Qualitative Report*, *21*(11), 2124. http://nsuworks.nova.edu/tqr/vol21/iss11/13

Hanus, B., & Wu, Y. A. (2016). Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective. *Information Systems Management, 33*(1), 2-16. https://doi.org/10.1080/10580530.2015.1117842

Harriss, D. J., MacSween, A., & Atkinson, G. (2017). Standards for ethics in sport and exercise science research: 2018 update. *International journal of sports medicine, 38*(14), 1126-1131. https://doi.org/10.1055/s-0043-124001

Harrison, S., & Jürjens, J. (2017). Information security management and the human aspect in organizations. *Information and Computer Security, 25*(5), 494-534. https://doi.org/10.1108/ICS-07-2016-0054

Hassan, S., Pandey, S., & Pandey, S. K. (2020). Should Managers Provide General or Specific Ethical Guidelines to Employees: Insights from a Mixed Methods Study. *Journal of Business Ethics*, 1-18. https://doi.org/10.1007/s10551-020-04442-3

Hawdon, J., Oksanen, A., & Räsänen, P. (2017). Exposure to online hate in four nations: A cross-national consideration. *Deviant behavior, 38*(3), 254-266. https://doi.org/10.1080/01639625.2016.1196985

Hayashi, P., Jr., Abib, G., & Hoppen, N. (2019). Validity in qualitative research: A processual approach. *The Qualitative Report, 24*(1), 98-112. https://nsuworks.nova.edu/tqr/vol24/iss1/8

Hershberger, P. E., & Kavanaugh, K. (2017). Comparing appropriateness and equivalence of email interviews to phone interviews in qualitative research on

reproductive decisions. *Applied Nursing Research*, *37*, 50-54. https://doi.org/10.1016/j.apnr.2017.07.005

Holmes, A. P., Grimwood, B. S., King, L. J., & The Lutsel K'e Dene First Nation. (2016). Creating an indigenized visitor code of conduct: The development of denesoline self-determination for sustainable tourism. *Journal of Sustainable Tourism*, *24*(8-9), 1177-1193. https://doi.org/10.1080/09669582.2016.1158828

Holt, T. J., van Wilsem, J., van de Weijer, S., & Leukfeldt, R. (2018). Testing an integrated self-control and routine activities framework to examine malware infection victimization. *Social Science Computer Review*.https://doi.org/10.1177/0894439318805067

Houghton, C., Murphy, K., Meehan, B., Thomas, J., Brooker, D., & Casey, D. (2017). From screening to synthesis: using nvivo to enhance transparency in qualitative evidence synthesis. *Journal of clinical nursing*, *26*(5-6), 873-881. https://doi.org/10.1111/jocn.13443

Howell, S. (2017). Two or three things I love about ethnography. *HAU: Journal of Ethnographic Theory*, *7*(1), 15-20. https://doi.org/10.14318/hau7.1.004

Hui, K. L., Kim, S. H., & Wang, Q. H. (2017). Cybercrime deterrence and international legislation: Evidence from distributed denial of service attacks. *Mis Quarterly*, *41*(2), 49. https://doi.org/10.25300/MISQ/2017/41.2.0

Ireland, L. (2020). Predicting Online Target Hardening Behaviors: An Extension of Routine Activity Theory for Privacy-Enhancing Technologies and

Techniques. *Deviant Behavior*, 1-17. https://doi.org/10.1080/01639625.2020.1760418

Jansen, J., & Leukfeldt, R. (2016). Phishing and malware attacks on online banking customers in the Netherlands: A qualitative analysis of factors leading to victimization. *International Journal of Cyber Criminology*, *10*(1), 79. http://cybercrimejournal.com/Jansen&Leukfeldtvol10issue1IJCC2016.pdf

Johnson, M., O'Hara, R., Hirst, E., Weyman, A., Turner, J., Mason, S., Quinn, T., Shewan, J., & Siriwardena, A. N. (2017). Multiple triangulation and collaborative research using qualitative methods to explore decision making in pre-hospital emergency care. *BMC medical research methodology*, *17*(1), 11. https://doi.org/10.1186/s12874-017-0290-z

Joslin, R., & Müller, R. (2016). Identifying interesting project phenomena using philosophical and methodological triangulation. International Journal of Project Management, 34(6), 1043-1056. https://doi.org/10.1016/j.ijproman.2016.05.005

Kakucha, W., & Buya, I. (2018). Information System Security Mechanisms in Financial Management. *Journal of Information and Technology*, *2*(1), 1-16. Stratford. https://stratfordjournals.org/journals/index.php/Journal-of-Information-and-Techn/article/view/115

Kallio, H., Pietilä, A. M., Johnson, M., & Kangasniemi, M. (2016). Systematic methodological review: developing a framework for a qualitative semi-structured interview guide. *Journal of advanced nursing*, *72*(12), 2954-2965. https://doi.org/10.1111/jan.13031

Kalu, M. E. (2019). Using Emphasis-Purposeful Sampling-Phenomenon of Interest–Context (EPPiC) Framework to Reflect on Two Qualitative Research Designs and Questions: A Reflective Process. *The Qualitative Report, 24*(10), 2524-2535. https://nsuworks.nova.edu/tqr/vol24/iss10/9

Kapoor, K. K., Tamilmani, K., Rana, N. P., Patil, P., Dwivedi, Y. K., & Nerur, S. (2018). Advances in social media research: Past, present and future. *Information Systems Frontiers, 20*(3), 531-558. https://doi.org/10.1007/s10796-017-9810-y

Kayser, C. S., Ellen Mastrorilli, M., & Cadigan, R. (2019). Preventing cybercrime: A framework for understanding the role of human vulnerabilities. *Cyber Security: A Peer-Reviewed Journal*, *3*(2), 159-174. Ingenta. https://www.ingentaconnect.com/content/hsp/jcs/2019/00000003/00000002/art00007

Khan, R., & Hasan, M. (2017). Network threats, attacks and security measures: a review. *International Journal of Advanced Research in Computer Science*, *8*(8), 119-120. ProQuest. https://search.proquest.com/openview/c8132c884935b6ce775af1cf2ccd1db7/1?pq-origsite=gscholar&cbl=1606379

Ki-Aries, D., & Faily, S. (2017). Persona-centered information security awareness. *computers & security, 70*, 663-674. https://doi.org/10.1016/j.cose.2017.08.001

Kigerl, A. (2012). Routine activity theory and the determinants of high cybercrime countries. *Social Science Computer Review*, *30*(4), 470-486. https://doi.org/10.1177/0894439311422689

Kocsis, R., & Palermo, G. (2016). Criminal profiling as expert witness evidence: The implications of the profiler validity research. *International journal of law and psychiatry*, *49*, 55-65. https://doi.org/10.1016/j.ijlp.2016.05.011

Korstjens, I., & Moser, A. (2018). Series: practical guidance to qualitative research. Part 4: trustworthiness and publishing. *European Journal of General Practice*, *24*(1), 120-124. https://doi.org/10.1080/13814788.2017.1375092

Krasznay, C., & Hámornik, B. P. (2018). Analysis of cyberattack patterns by user behavior analytics 1. *Academic and Applied Research in Military and Public Management Science*, *17*(3), 101-113. LUDOVIKA EGYETEMI KIADÓ. https://folyoirat.ludovika.hu/index.php/aarms/article/view/1069/391

Kumar, S., Kandasamy, S., & Deepa, K. (2016). On privacy and security in social media–A comprehensive study. *Procedia Computer Science*, *78*, 114-19. https://doi.org/10.1016/j.procs.2016.02.019

Lai, Y. L., Ren, L., & Greenleaf, R. (2017). Residence-based fear of crime: a routine activities approach. *International journal of offender therapy and comparative criminology*, *61*(9), 1011-1037. https://doi.org/10.1177/0306624X15625054

Lechner, N. H. (2017). An overview of cybersecurity regulations and standards for medical device software. *Central European Conference on Information and Intelligent Systems,* 237-249. Faculty of organization and informatics varazdin. http://archive.ceciis.foi.hr/app/public/conferences/2017/06/QSS-3.pdf

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*, *37*(3), 263-280. https://doi.org/10.1080/01639625.2015.1012409

Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2017). Cybercriminal networks, social ties and online forums: social ties versus digital ties within phishing and malware networks. *The British Journal of Criminology*, *57*(3), 704-722. https://doi.org/10.1093/bjc/azw009

Leung, X. Y., Yang, Y., & Dubin, E. A. (2018). What are guests scared of? Crime-related hotel experiences and fear of crime. *Journal of Travel & Tourism Marketing*, *35*(8), 1071-1086. https://doi.org/10.1080/10548408.2018.1473192

Levi, M. (2017). Assessing the trends, scale and nature of economic cybercrimes: overview and issues. *Crime, Law and Social Change*, *67*(1), 3-20.

Levitt, H. M., Bamberg, M., Creswell, J. W., Frost, D. M., Josselson, R., & Suárez-Orozco, C. (2018). Journal article reporting standards for qualitative primary, qualitative meta-analytic, and mixed methods research in psychology: The APA Publications and Communications Board task force report. *American Psychologist*, *73*(1), 26. https://psycnet.apa.org/fulltext/2018-00750-003.html

Liao, R., Balasinorwala, S., & Rao, H. R. (2017). Computer-assisted frauds: An examination of offender and offense characteristics in relation to arrests. *Information Systems Frontiers*, *19*(3), 443-455. https://doi.org/ 10.1007/s10796-017-9752-4

Litchfield, S., Formby, D., Rogers, J., Meliopoulos, S., & Beyah, R. (2016). Rethinking the honeypot for cyber-physical systems. *IEEE Internet Computing*, *20*(5), 9-17. https://doi.org/10.1109/MIC.2016.103

Maglaras, L., Ferrag, M. A., Derhab, A., Mukherjee, M., Janicke, H., & Rallis, S. (2019). Threats, protection and attribution of cyber attacks on critical infrastructures. *arXiv preprint arXiv:1901.03899*. https://arxiv.org/abs/1901.03899

Maguire, M., & Delahunt, B. (2017). Doing a thematic analysis: A practical, step-by-step guide for learning and teaching scholars. *AISHE-J: The All Ireland Journal of Teaching and Learning in Higher Education*, *9*(3). http://ojs.aishe.org/index.php/aishe-j/article/view/335/553

Malik, M. H., & Younis, N. (2016). Cybercrimes prevention and recovery strategies. *Science International*, *28*(3). Sci. Int (Lahore). http://www.sci-int.com/pdf/8190287451%201%20a%202489-2492%20Mazhar%20Hussain%20Malik%20-Cyber%20Crime%20Final%20Version--IT--MULTAN--2-1-15%20TR--London.pdf

Marcum, C. D. (2009). *Adolescent online victimization: A test of routine activities theory*. LFB Scholarly Publishing LLC. http://www.ncjrs.gov/App/publications/abstract.aspx?ID=252093

Marshall, C., & Rossman, G. (2016). *Designing qualitative research.* Thousand Oaks, CA: Sage.

Martin, J., Dubé, C., & Coovert, M. D. (2018). Signal Detection Theory (SDT) is effective for modeling user behavior toward phishing and spear-phishing attacks. *Human factors*, *60*(8), 1179-1191. https://doi.org/10.1177/0018720818789818

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing*, *81*(1), 36-58. https://doi.org/10.1509/jm.15.0497

Mason, L., & Wronski, J. (2018). One tribe to bind them all: How our social group attachments strengthen partisanship. *Political Psychology*, *39*, 257-277. https://doi.org/10.1111/pops.12485

McGrath, C., Palmgren, P. J., & Liljedahl, M. (2019). Twelve tips for conducting qualitative research interviews. *Medical teacher*, *41*(9), 1002-1006. https://doi.org/10.1080/0142159X.2018.1497149

Miracle, V. A. (2016). The Belmont Report: The triple crown of research ethics. *Dimensions of Critical Care Nursing*, *35*(4), 223-228. https://doi.org/10.1097/DCC.0000000000000186

Miranda, M. J. (2018). Enhancing cybersecurity awareness training: A comprehensive phishing exercise approach. *International Management Review*, *14*(2), 5-10. http://www.imrjournal.org/uploads/1/4/2/8/14286482/imr-v14n2art1.pdf

Mittal, S., & Sharma, P. (2017). Enough law of horses and elephants debated… Let's discuss the cyber law seriously. *International Journal of Advanced Research in Computer Science, ISSN*, (0976-5697). https://doi.org/10.2139/ssrn.2977374

Moeller, K., Copes, H., & Hochstetler, A. (2016). Advancing restrictive deterrence: A qualitative meta-synthesis. *Journal of Criminal Justice, 46*, 82-93. https://doi.org/10.1016/j.jcrimjus.2016.03.004

Mohajan, H. K. (2017). Two criteria for good measurements in research: Validity and reliability. *Annals of Spiru Haret University. Economic Series*, *17*(4), 59-82. Central and Eastern European Online Library. https://www.ceeol.com/search/article-detail?id=673569

Mohajan, H. K. (2018). Qualitative research methodology in social sciences and related subjects. *Journal of Economic Development, Environment, and People*, *7*(1), 23-48. MPRA. https://mpra.ub.uni-muenchen.de/85654/1/MPRA_paper_85654.pdf

Moir, E., Hart, T. C., Reynald, D. M., & Stewart, A. (2018). Typologies of suburban guardians: Understanding the importance of responsibility, opportunities, and routine activities in facilitating surveillance. *Crime Prevention & Community Safety*. https://doi.org/ 10.1057/s41300-018-0057-4

Muller, S. R., & Lind, M. L. (2020). Factors in information assurance professionals' intentions to adhere to information security policies. *International Journal of Systems and Software Security and Protection (IJSSSP)*, *11*(1), 17-32. https://doi.org/10.4018/IJSSSP.2020010102

Mun, H. J., Hong, S., & Shin, J. (2018). A novel secure and efficient hash function with extra padding against rainbow table attacks. *Cluster Computing*, *21*(1), 1161-1173. https://doi.org/10.1007/s10586-017-0984-3

Munch, E. (2017). A user's guide to topological data analysis. *Journal of Learning Analytics*, *4*(2), 47-61. https://doi.org/10.18608/jla.2017.42.6

Nallaperumal, K. (2018, December). Cybersecurity analytics to combat cybercrimes. In *2018 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)* (pp. 1-4). IEEE. https://doi.org/10.1109/ICCIC.2018.8782430

Näsi, M., Räsänen, P., Kaakinen, M., Keipi, T., & Oksanen, A. (2017). Do routine activities help predict young adults' online harassment: A multination study. *Criminology & Criminal Justice*, *17*(4), 418-432. doi:10.1177/1748895816679866

Navarro, J. N., Clevenger, S., Beasley, M. E., & Jackson, L. K. (2017). One step forward, two steps back: Cyberbullying within social networking sites. *Security Journal, 30*(3), 844-858. https://doi.org/10.1057/sj.2015.19

Nawafleh, Y., Nawafleh, A., & Nawafleh, S. (2016). Cybercrimes: concept, forms, and their civil liabilities. *International Journal of Arts & Sciences, 9*(1), 211-234. ResearchGate. https://www.researchgate.net/profile/sahem_nawafleh/publication/323394145_cybercrimes_concept_forms_and_their_civil_liabilities/links/5a93dc99a6fdccecff05e4c8/cybercrimes-concept-forms-and-their-civil-liabilities.pdf

Nedelec, J. L. (2018). Individual differences and co-occurring victimization online and offline: The role of impulsivity. *Personality and Individual Differences, 133*, 77-84. https://doi.org/10.1016/j.paid.2016.11.028

Nelson, J. (2016). Using conceptual depth criteria: addressing the challenge of reaching saturation in qualitative research. *Qualitative research, 17*(5), 554-570. https://doi.org/10.1177/1468794116679873

Neubert, M. (2016). Significance of the speed of internationalization for born global firms-a multiple case study approach. *International Journal of Teaching and Case Studies*, *7*(1), 66-81. https://doi.org/10.1504/IJTCS.2016.076067

Neuner, S., Schmiedecker, M., & Weippl, E. (2016). Effectiveness of file-based deduplication in digital forensics. *Security and Communication Networks, 9*(15), 2876-2885. https://doi.org/10.1002/sec.1418

Ngo, F., & Jaishankar, K. (2017). Commemorating a decade in existence of the international journal of cyber criminology: A research agenda to advance the scholarship on cybercrime. *International Journal of Cyber Criminology, 11*(1), 1-9. https://doi.org/10.5281/zenodo.495762fngo

Nieles, M., Dempsey, K., & Pillitteri, V. (2017). *An Introduction to Information Security* (No. NIST Special Publication (SP) 800-12 Rev. 1 (Draft)). National Institute of Standards and Technology. CSRC. https://csrc.nist.gov/publications/detail/sp/800-12/rev-1/archive/2017-01-23

Oltmann, S. (2016, May). Qualitative interviews: A methodological discussion of the interviewer and respondent contexts. In *Forum Qualitative Sozialforschung/Forum: Qualitative Social Research*, 7(3). https://doi.org/10.17169/fqs-17.2.2551

Park, J., Cho, D., Lee, J. K., & Lee, B. (2019). The Economics of cybercrime: The role of broadband and socioeconomic status. *ACM Transactions on Management Information Systems (TMIS)*, *10*(4), 1-23. https://doi.org/10.1145/3351159

Paternoster, R., Jaynes, C. M., & Wilson, T. (2017). Rational choice theory and interest in the "Fortune of Others". *Journal of research in crime and delinquency*, *54*(6), 847-868. https://doi.org/10.1177/0022427817707240

Payne, B. K., Hawkins, B., & Xin, C. (2019). Using labeling theory as a guide to examine the patterns, characteristics, and sanctions given to cybercrimes. *American Journal of Criminal Justice*, *44*(2), 230-247. https://doi.org/10.1007/s12103-018-9457-3

Petrescu, M., Gironda, J. T., & Korgaonkar, P. K. (2018). Online piracy in the context of routine activities and subjective norms. *Journal of Marketing Management*, *34*(3-4), 314-346. https://doi.org/10.1080/0267257X.2018.1452278

Poster, W. R. (2018). Cybersecurity needs women. Nature. https://www.nature.com/articles/d41586-018-03327-w

Pothumani, S., & Anuradha, C. (2017). Decoy method on various environments-A survey. *International Journal of Pure and Applied Mathematics*, *116*(10), 197-200. http://acadpubl.eu/jsi/2017-116-8/articles/10/34.pdf

Pratt, T. C., & Turanovic, J. J. (2016). Lifestyle and routine activity theories revisited: The importance of "risk" to the study of victimization. *Victims & Offenders*, *11*(3), 335-354. https://doi.org/10.1080/15564886.2015.1057351

Prasanthi, B. V., Kanakam, P., & Hussain, S. M. (2017). Cyber Forensic Science to Diagnose Digital Crimes-A study. *International Journal of Scientific Research in Network Security and communication (IJSRNSC)*, *50*(2), 107-113. https://doi.org/10.14445/22312803/IJCTT-V50P119

Rahbek, O. (2018). What is assumption in research? *The quora*. https://www.quora.com/profile/Ali-M-Baker-Ph-D

Rahi, S. (2017). Research design and methods: A systematic review of research paradigms, sampling issues, and instrument development. *International Journal of Economics & Management Sciences*, *6*(2), 1-5.https://doi.org/10.4172/2162-6359.1000403

Räsänen, P., Hawdon, J., Holkeri, E., Keipi, T., Näsi, M., & Oksanen, A. (2016). Targets of online hate: Examining determinants of victimization among young Finnish Facebook users. *Violence and Victims*, *31*(4), 708-725. https://doi.org/10.1891/0886-6708.VV-D-14-00079

Reisig, M. D., & Holtfreter, K. (2018). The victim-offender overlap in late adulthood. *Journal of elder abuse & neglect*, *30*(2), 144-166. https://doi.org/10.1080/08946566.2018.1426512

Reyns, B. W., & Scherer, H. (2018). Stalking victimization among college students: The role of disability within a lifestyle-routine activity framework. *Crime & Delinquency*, *64*(5), 650-673. https://doi.org/10.1177/0011128717714794

Reyns, B. W., Fisher, B. S., Bossler, A. M., & Holt, T. J. (2019). Opportunity and self-control: Do they predict multiple forms of online victimization?. *American*

Journal of Criminal Justice, *44*(1), 63-82. https://doi.org/10.1007/s12103-018-9447-5

Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being pursued online: Applying cyber lifestyle–routine activities theory to cyberstalking victimization. *Criminal justice and behavior*, *38*(11), 1149-1169. https://doi.org/10.1177/0093854811421448

Reyns, B. W., Henson, B., & Fisher, B. S. (2016a). Guardians of the cyber galaxy: An empirical and theoretical analysis of the guardianship concept from routine activity theory as it applies to online forms of victimization. *Journal of Contemporary Criminal Justice*, *32*(2), 148-168. https://doi.org/10.1177/1043986215621378

Reyns, B. W., Henson, B., Fisher, B. S., Fox, K. A., & Nobles, M. R. (2016b). A gendered lifestyle-routine activity approach to explaining stalking victimization in Canada. *Journal of interpersonal violence*, *31*(9), 1719-1743. https://doi.org/10.1177/0886260515569066

Reyns, B. W., Randa, R., & Henson, B. (2016). Preventing crime online: Identifying determinants of online preventive behaviors using structural equation modeling and canonical correlation analysis. *Crime Prevention and Community Safety*, *18*(1), 38-59. https://doi.org/10.1057/cpcs.2015.21

Reynald, D. M., Moir, E., Cook, A., & Vakhitova, Z. (2018). Changing perspectives on guardianship against crime: an examination of the importance of micro-level factors. *Crime Prevention and Community Safety*, *20*(4), 268-283. https://doi.org/10.1057/s41300-018-0049-4

Riek, M., Bohme, R., & Moore, T. (2016). Measuring the influence of perceived cybercrime risk on online service avoidance. *IEEE Transactions on Dependable and Secure Computing, 13*(2), 261-273. https://doi.org/10.1109/TDSC.2015.2410795

Rosalina, R., & Jayanto, H. (2018). Maximal overlap discrete wavelet transform, graph theory and back propagation neural network in stock market forecasting. *IJNMT (International Journal of New Media Technology), 5*(1), 41-46. https://doi.org/10.31937/ijnmt.v5i1.679

Rosenthal, M. (2016). Qualitative research methods: Why, when, and how to conduct interviews and focus groups in pharmacy research. *Currents in pharmacy teaching and learning*, *8*(4), 509-516. https://doi.org/10.1016/j.cptl.2016.03.021

Rutberg, S., & Bouikidis, C. D. (2018). Focusing on the fundamentals: A simplistic differentiation between qualitative and quantitative research. *Nephrology Nursing Journal*, *45*(2), 209-213. CNE. http://www.homeworkgain.com/wp-content/uploads/edd/2019/09/20181009143525article2.pdf

Sabillon, R., Serra-Ruiz, J., & Cavaller, V. (2019). An effective cybersecurity training model to support an organizational awareness program: The Cybersecurity Awareness TRAining Model (CATRAM). A Case Study in Canada. *Journal of Cases on Information Technology (JCIT), 21*(3), 26-39. https://doi.org/10.4018/JCIT.2019070102

Safa, N. S., Maple, C., Watson, T., & Von Solms, R. (2018). Motivation and opportunity based model to reduce information security insider threats in

organizations. *Journal of information security and applications*, *40*, 247-257. https://doi.org/10.1016/j.jisa.2017.11.001

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: a survey. *Future Internet*, *11*(4), 89. https://doi.org/10.3390/fi11040089

Salakhova, V. B., Bulgakov, A. V., Sokolovskaya, I. E., Khammatova, R. S., & Mikhaylovsky, M. N. (2016). Substantive (Content-Related) Characteristics of Deviant Behavior as a Social and Psychological Phenomenon. *International Journal of Environmental and Science Education*, *11*(17), 10609-10622. Look Academic Publishers. https://files.eric.ed.gov/fulltext/EJ1120216.pdf

Saridakis, G., Benson, V., Ezingeard, J. N., & Tennakoon, H. (2016). Individual information security, user behaviour, and cyber victimization: An empirical study of social networking users. *Technological Forecasting and Social Change*, *102*, 320-330. https://doi.org/10.1016/j.techfore.2015.08.012

Saunders, B., Sim, J., Kingstone, T., Baker, S., Waterfield, J., Bartlam, B., Burroughs, H., & Jinks, C. (2018). Saturation in qualitative research: exploring its conceptualization and operationalization. *Quality & quantity*, *52*(4), 1893-1907. https://doi.org/10.1007/s11135-017-0574-8

Schaefer, L., & Mazerolle, L. (2017). Putting process into routine activity theory: Variations in the control of crime opportunities. *Security Journal*, *30*(1), 266-289. https://doi.org/10.1057/sj.2015.39

Schreck, C. J. (2017). Routine Activity Theory. In *Preventing Crime and Violence*. 67-72. Springer, Cham. https://doi.org/10.1007/978-3-319-44124-5_7

Sedlander, E., Barboza, K. C., Jensen, A., Skursky, N., Bennett, K., Sherman, S., & Schwartz, M. (2018). Veterans' preferences for remote management of chronic conditions. *Telemedicine and e-Health*, *24*(3), 229-235. https://doi.org/10.1089/tmj.2017.0010

Seissa, I. G., Ibrahim, J., & Yahaya, N. (2017). Cyberterrorism definition patterns and mitigation strategies: A Literature Review. *International Journal of Science and Research (IJSR), 6*(1), 180-186. https://doi.org/10.21275/ART20163936

Shalhoub, J., Marshall, D. C., & Ippolito, K. (2017). Perspectives on procedure-based assessments: a thematic analysis of semistructured interviews with 10 UK surgical trainees. *BMJ Open, 7*(3), e013417.https://doi.org/10.1136/bmjopen-2016-013417

Shoaib, S., & Baruch, Y. (2019). Deviant behavior in a moderated-mediation framework of incentives, organizational justice perception, and reward expectancy. *Journal of Business Ethics, 157*(3), 617-633. https://doi.org/10.1007/s10551-017-3651-y

Siddiqui, M. Z., Yadav, S., & Husain, M. S. (2018). Application of artificial intelligence in fighting against cyber crimes: A review. *International Journal of Advanced Research in Computer Science, 9*(Special Issue 2), 118. https://doi.org/10.1109/CCCS.2018.8586801

Silva, L., Mondal, M., Correa, D., Benevenuto, F., & Weber, I. (2016, March). Analyzing the targets of hate in online social media. In *Tenth International AAAI Conference on Web and Social Media*. Cornell University. https://arxiv.org/pdf/1603.07709.pdf

Singh, M. M., & Bakar, A. A. (2019). A Systemic cybercrime stakeholders architectural model. *Procedia Computer Science*, *161,* 1147-1155. https://doi.org/10.1016/j.procs.2019.11.227

Simon, M. K., & Goes, J. (2013). Assumptions, limitations, delimitations, and scope of the study. http://dissertationrecipes.com/wp-content/uploads/2011/04/limitationscopedelimitation1.pdf

Simpson, S. S. (2019). Reimagining Sutherland 80 years after white-collar crime. *Criminology, 57*(2), 189-207. https://doi.org/ 10.1111/1745-9125.12206

Smith, B., & McGannon, K. R. (2018). Developing rigor in qualitative research: Problems and opportunities within sport and exercise psychology. *International review of sport and exercise psychology, 11*(1), 101-121. https://doi.org/10.1080/1750984X.2017.1317357

Smith, P. R. (2018). Collecting sufficient evidence when conducting a case study. *The Qualitative Report*, *23*(5), 1054-1048. https://nsuworks.nova.edu/tqr/vol23/iss5/2/

Sohn, B. K., Thomas, S. P., Greenberg, K. H., & Pollio, H. R. (2017). Hearing the voices of students and teachers: A phenomenological approach to educational research. *Qualitative Research in Education*, *6*(2), 121-148. https://doi.org/10.17583/qre.2017.2374

Spalek, B. (2016). *Crime victims: Theory, policy, and practice*. Macmillan international higher education. University of Derby. http://hdl.handle.net/10545/621209

Spaulding, S. (2015). Phenomenology of social cognition. *Erkenntnis, 80*(5), 1069-1089. https://doi.org/10.1007/s10670-014-9698-6

Srivastava, S. K., Das, S., Udo, G. J., & Bagchi, K. (2020). Determinants of cybercrime originating within a Nation: A Cross-country Study. *Journal of Global Information Technology Management*, 1-26. https://doi.org/10.1080/1097198X.2020.1752084

Stephan, U., Patterson, M., Kelly, C., & Mair, J. (2016). Organizations driving positive social change: A Review and an integrative framework of change processes. *Journal of Management*, *42*(5), 1250–1281. https://doi.org/10.1177/0149206316633268

Tambo, E., & Adama, K. (2017). Promoting Cybersecurity Awareness and Resilience Approaches Capabilities and Actions Plans against Cybercrimes and Frauds in Africa. *International Journal of Cyber-Security and Digital Forensics*, *6*(3), 126-138. https://doi.org/10.17781/P002278

Tankard, M. E., & Paluck, E. L. (2016). Norm perception as a vehicle for social change. *Social Issues and Policy Review*, *10*(1), 181-211. https://doi.org/10.1111/sipr.12022

Testa, A., Maimon, D., Sobesto, B., & Cukier, M. (2017). Illegal roaming and file manipulation on target computers: Assessing the effect of sanction threats on system trespassers' online behaviors. *Criminology & Public Policy*, *16*(3), 689-726. https://doi.org/10.1016/j.jisa.2017.11.001

Thomas, D. R. (2017). Feedback from research participants: are member checks useful in qualitative research?. *Qualitative Research in Psychology*, *14*(1), 23-41. https://doi.org/10.1080/14780887.2016.1219435

Thomas, K., Li, F., Zand, A., Barrett, J., Ranieri, J., Invernizzi, L., Markov, Y., Comanescu, O., Eranti, V., Moscicki, A., Margolis, D., Paxson, V., & Bursztein, E. (2017, October). Data breaches, phishing, or malware?: Understanding the risks of stolen credentials. In *Proceedings of the 2017 ACM SIGSAC conference on computer and communications security* (pp. 1421-1434). ACM. https://doi.org/10.1145/3133956.3134067

Tsai, A. C., Kohrt, B. A., Matthews, L. T., Betancourt, T. S., Lee, J. K., Papachristos, A. V., Weiser, S. D., & Dworkin, S. L. (2016). Promises and pitfalls of data sharing in qualitative research. *Social Science & Medicine, 169*, 191-198. https://doi.org/10.1016/j.socscimed.2016.08.004

Tschakert, K. F., & Ngamsuriyaroj, S. (2019). Effectiveness of and user preferences for security awareness training methodologies. *Heliyon, 5*(6), e02010. https://doi.org/10.1016/j.heliyon.2019.e02010

Tunley, M., Button, M., Shepherd, D., & Blackbourn, D. (2018). Preventing occupational corruption: utilising situational crime prevention techniques and theory to enhance organisational resilience. *Security Journal*, *31*(1), 21-52. Https://doi.org/10.1057/s41284-016-0087-5

Tyler, L. B. (2018). Exploring the implementation of cloud security to minimize electronic health records cyberattacks. Walden University. https://scholarworks.waldenu.edu/dissertations/5281/

Urquhart, L., & McAuley, D. (2018). Avoiding the internet of insecure industrial things. *Computer law & security review*, *34*(3), 450-466. https://doi.org/10.1016/j.clsr.2017.12.004

Vaismoradi, M., & Snelgrove, S. (2019, September). Theme in qualitative content analysis and thematic analysis. In *Forum Qualitative Sozialforschung/Forum: Qualitative Social Research* (Vol. 20, No. 3). https://doi.org/10.17169/fqs-20.3.3376

Vakhitova, Z. I., Reynald, D. M., & Townsley, M. (2016). Toward the adaptation of routine activity and lifestyle exposure theories to account for cyber abuse victimization. *Journal of Contemporary Criminal Justice*, *32*(2), 169-188. https://doi.org/10.1177/1043986215621379

Van Wegberg, R. S., Klievink, A. J., & Van Eeten, M. J. G. (2017). Discerning novel value chains in financial malware. *European Journal on Criminal Policy and Research*, *23*(4), 575-594. https://doi.org/10.1007/s10610-017-9336

Vasileiou, I., & Furnell, S. (2019). *Cybersecurity education for awareness and compliance*. IGI Global. https://kevincurran.org/papers/insiderthreats.pdf

Vayena, E., Brownsword, R., Edwards, S. J., Greshake, B., Kahn, J. P., Ladher, N., Montgomery, J., O'Connor, D., Richards, M. P., Rid, A., Sheehan, M., Wicks, P., & Tasioulas, J. (2016). Research led by participants: a new social contract for a

new kind of research. *Journal of Medical Ethics, 42*(4), 216-219. https://doi.org/10.1136/medethics-2015-102663

Wachs, S., Michelsen, A., Wright, M. F., Gámez-Guadix, M., Almendros, C., Kwon, Y., Na, E., Sittichai, R., Singh, R., Biswal, R., Görzig, A., & Yanagida, T. (2020). A routine activity approach to understand cyber grooming victimization among adolescents from six countries. *Cyberpsychology, Behavior, and Social Networking.* https://doi.org/10.1089/cyber.2019.0426

Weller, S. C., Vickers, B., Bernard, H. R., Blackburn, A. M., Borgatti, S., Gravlee, C. C., & Johnson, J. C. (2018). Open-ended interview questions and saturation. *PloS one, 13*(6), e0198606. https://doi.org/10.1371/journal.pone.0198606

Whitaker, C., Stevelink, S., & Fear, N. (2017). The use of Facebook in recruiting participants for health research purposes: a systematic review. *Journal of Medical Internet Research, 19*(8), e290. https://www.jmir.org/2017/8/e290/

Whitehead, D., & Whitehead, L. (2016). Sampling data and data collection in qualitative research. ECU, Research Online Institutional Repository. https://ro.ecu.edu.au/ecuworkspost2013/1555/

Whitmarsh, L., & Corner, A. (2017). Tools for a new climate conversation: A mixed-methods study of language for public engagement across the political spectrum. *Global Environmental Change, 42,* 122-135. https://doi.org/10.1016/j.gloenvcha.2016.12.008

Whitty, M. T. (2019). Predicting susceptibility to cyber-fraud victimhood. *Journal of Financial Crime, 26*(1), 277-292. https://doi.org/10.1108/JFC-10-2017-0095

Wick, S. E., Nagoshi, C., Basham, R., Jordan, C., Kim, Y. K., Nguyen, A. P., & Lehmann, P. (2017). Patterns of cyber harassment and perpetration among college students in the United States: A test of routine activities theory. *International Journal of Cyber Criminology*, *11*(1). https://doi.org/10.5281/zenodo.495770

Wilcox, P., & Cullen, F. T. (2018). Situational opportunity theories of crime. *Annual Review of Criminology*, *1*, 123-148. https://doi.org/10.1146/annurev-criminol-032317-092421

Wiley, A., McCormac, A., & Calic, D. (2020). More than the individual: Examining the relationship between culture and Information Security Awareness. *Computers & Security*, *88*, 101640. https://doi.org/10.1016/j.cose.2019.101640

Williams, M. L., Levi, M., Burnap, P., & Gundur, R. V. (2019). Under the corporate radar: Examining insider business cybercrime victimization through an application of routine activities theory. *Deviant Behavior*, *40*(9), 1119-1131. https://doi.org/10.1080/01639625.2018.1461786

Woods, M., Paulus, T., Atkins, D. P., & Macklin, R. (2016). Advancing qualitative research using qualitative data analysis software (QDAS)? Reviewing potential versus practice in published studies using ATLAS. ti and NVivo, 1994–2013. *Social Science Computer Review*, 34(5), 597-617. https://doi.org/10.1177/0894439315596311

Woodward, E., & Marrfurra McTaggart, P. (2016). Transforming cross-cultural water research through trust, participation and place. *Geographical Research*, *54*(2), 129-142. https://doi.org/10.1111/1745-5871.12136

Wong, J. (2016). *U.S. Patent No. 9,294,483*. Washington, DC: U.S. Patent and Trademark Office. Google Patents. https://patents.google.com/patent/US9294483B2/en

Wong, S., & Cooper, P. (2016). Reliability and validity of the explanatory sequential design of mixed methods adopted to explore the influences on online learning in Hong Kong bilingual cyber higher education. *International Journal of Cyber Society and Education*, *9*(2), 45-64. https://doi.org/10.7903/ijcse.1475

Yaokumah, W., Walker, D. O., & Kumah, P. (2019). SETA and security behavior: Mediating role of employee relations, monitoring, and accountability. *Journal of Global Information Management (JGIM)*, *27*(2), 102-121. https://doi.org/10.4018/JGIM.2019040106

Yapıcıoğlu, A. E., & Kaptan, F. (2017). A mixed-method research study on the effectiveness of socioscientific issue-based instruction. *Egitim Ve Bilim*, *42*(192). https://doi.org/10.15390/eb.2017.6600

Yar, M. (2005). The novelty of 'cybercrime' an assessment in light of routine activity theory. *European Journal of Criminology*, *2*(4), 407-427. https://doi.org/10.1177/147737080556056

Yeboah-ofori, A., Abdulai, J. D., & Katsriku, F. (2018). Cybercrime and risks for cyber-physical systems: A review. https://doi.org/ 10.20944/preprints201804.0066.v1

Yeong, M. L., Ismail, R., Ismail, N. H., & Hamzah, M. (2018). Interview protocol refinement: Fine-tuning qualitative research interview questions for multi-racial

populations in Malaysia. *The Qualitative Report, 23*(11), 2700-2713. https://nsuworks.nova.edu/tqr/vol23/iss11/7/

Zabyelina, Y. G. (2017). Can criminals create opportunities for crime? Malvertising and illegal online medicine trade. *Global Crime, 18*(1), 31-48. https://doi.org/10.1080/17440572.2016.1197124

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2020). Cyber security awareness, knowledge and behavior: a comparative study. *Journal of Computer Information Systems*, 1-16. https://doi.org/10.1080/08874417.2020.1712269

Appendix A: The National Institute of Health (NIH) Certificate of Completion

Certificate of Completion

The National Institutes of Health (NIH) Office of Extramural Research certifies that **PASCAL POUANI TIENTCHEU** successfully completed the NIH Web-based training course "Protecting Human Research Participants".

Date of completion: 05/18/2017.

Certification Number: 2398160.

Appendix B: The Interview Protocol the Interview Protocol

Location of the Interview:	**Date and Time of the Interview:**	**ID Number:**	**Name of the Participant:**

My name is Pascal Pouani Tientcheu and I will be conducting this interview. The goal of this interview is to have your opinion regarding my research topic, which is the following:" Security awareness strategies used in the prevention of cybercrimes by cybercriminals". The interview will last 30 minutes.

Your opinion is very relevant for my research findings and will contribute to preventing cybercrimes through the use of best security awareness strategies practices.

You are among the 10 participants that I selected to participate in this interview and all of you are located in the Washington DC area.

10 open-ended questions will be asked in order and the entire interview will be recorded accordingly. You are free to stop me anytime during the interview process if you need more clarification on any questions.

Your selection is based on the fact that you met all the criteria needed for this study, which is tied specifically to your IT position about cybersecurity and your geographic location.

One invitation letter (Appendix D) and two consent forms were sent to you before the today interview via your email address (one to sign and return and one to keep for the personal record).

Do you have any change to bring to one signed copy of the consent form?

Do you have any questions in that regard?

Let start with the first question if you do not have any inquiry.

1. Please tell me more about your responsibility.
    a. How long have you been working as an information security officer (ISO)?
    b. How many people you are supporting in your organization?
    c. Tell me more what you do when your organization is cyber-attacked.
    d. What is your first response to any cyberattack?
    e. How you address cyberattack issues within your organization?
2. Could you tell me more about what policies/procedures do you have to avoid a cyberattack?
3. Tell me more what strategies does your organization use for security awareness?
4. Could you tell me what strategies do you use to prevent cybercrimes?
5. Could you tell me who within your organization is more exposed to cyberattacks and why?
6. Tell me what types of cyberattack do employees of your organization face daily?
7. Tell me what are the frequencies of cyberattacks in your organization?
8. Tell me what are the economic impacts of cybercrimes on your organization?
9. Could you tell me what categories of information are targeted by cybercriminals?
10. Could you tell me what sensitive information is more targeted by cybercriminals?

Thank you for taking the time to answers all my questions and for your participation in this interview.

You will receive by mail or email within two weeks a full transcript of this interview.

Thank you again for your contribution to this research study.

Appendix C: Participant Consent Form in the Research Interview

Research Topic: "Security awareness strategies used in the prevention of cybercrimes by cybercriminals"

#	Closures	Remark
1	I understand that my participation is voluntary and could last less than an hour for a face-to-face, Skype or Zoom interview under my consent.	
2	I understand that a gift card will be provided to me for my participation in this research study.	
3	I understand that Walden University is aware of this research topic and have approved it. You may contact Walden University at 1-800-925-3368	
4	I understand that I will receive within two weeks after the completion of the interview, a copy of the interview transcript by mail or email.	
5	I understand that the interview process will be recorded under my consent.	
6	I understand that the researcher will keep secured the interview record for 5 years, which will be destroyed after the 5 years limitation period.	
7	I understand that the interview will not violate any ethical rules and will conform to the National Institute of Health (NIH) rules.	
8	I understand that any sensitive or classified information will not be discussed or provided during the interview.	
9	I understand that I will prevent the researcher by email or mail if I decide to withdraw from this study.	
10	I understand that there will not any penalty if I withdraw from the study.	
11	I understand the reason for my participation in this research study.	
12	I understand that the researcher will allow the participant to review information about the study for a 2-week periods before any given consent.	
13	I understand that the participant should keep a copy of this consent form for his/her personal record.	
14	I understand that the participant may contact the researcher for any questions concerning this research study.	
15	I understand that by signing this consent form, I acknowledge all the mentioned closures, and will be contacted by the researcher regarding data collection process, member checking related to this study.	

Participant's Signature:	**Date:**	**Researcher's Signature :**	**Date:**
Participant's Name:	**ID Number:**		
Participant's Email or Mail Address:			

Appendix D : Participant Invitation Letter

Dear Participant,

My name is Pascal Pouani Tientcheu; I'm a doctoral candidate in Information Technology at Walden University.

I am conducting a doctoral study to address security awareness strategies used by Information Security Manager in the prevention of cybercrimes by cybercriminals and I solicit your participation in this research study.

You have been approached for this study because you have the required skills, knowledge, and experience in cybersecurity and your participation will be very useful in the finding of strategies that will contribute to the prevention of cybercrimes.

I have attached a consent form to this invitation letter. Please feel free to reach out to me by email at pascal.pouanitientcheu@waldenu.edu or via my mobile phone at 202-XXX-XXXX if you need additional information in that regard.

Your participation is a voluntary act and will be compensated with a gift card for your participation in this study. Besides, you are free to accept the invitation or withdraw at any time without any penalty.

I would appreciate any positive feedback in terms of your participation and thanks to you in advance for your time and consideration.

Best regards,

Pascal Pouani Tientcheu

Appendix E: Information Security Officer (ISO) Responsibilities

Here are some of the responsibilities of an ISO:

- Monitor the organization's IT system to look for threats to security.
- Monitor network usage to ensure compliance with security policies.
- Establish protocols to identify and reduce the effect of threats and maintain updated anti-virus software to block threats.
- Keep up to date with developments in IT security standards and threats.
- Perform penetration tests to find any flaws.
- Collaborate with management and the IT department to improve security.