7-18-2024

Exploring Strategies Leaders Use for Enforcing Cybersecurity Policies to Protect Information Systems and Data

Ma'risa LaShawn Young
Walden University

Walden University

College of Management and Human Potential

This is to certify that the doctoral study by

Ma'risa Young

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. Alan Dawson, Committee Chairperson, Information Technology Faculty
Dr. Nawaz Khan, Committee Member, Information Technology Faculty

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

Walden University
2024

Abstract

Exploring Strategies Leaders Use for Enforcing Cybersecurity Policies to Protect Information Systems and Data

by

Ma'risa LaShawn Young

MS.IT, Walden University, 2022

MS, Western Governors University, 2019

BS, American Military University, 2018

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

July 2024

Abstract

Cybersecurity policies are critical for organizations to protect their digital assets and sensitive information. Leaders must explore and implement effective cybersecurity policies because the lack of effective strategies will lead to increased security risks. Grounded in the social cognitive theory, the purpose of this qualitative, pragmatic inquiry was to explore strategies cybersecurity leaders use to enforce cybersecurity policies in organizations to protect organizational information systems and data. The participants were cybersecurity leaders associated with cybersecurity policies and their implementation and enforcement in different organizations located in the Southeastern region of the United States. Data collection included semistructured interviews of five participating cybersecurity leaders and the analysis of fourteen publicly accessible documents. Four themes emerged from coding: user awareness and training, stakeholder buy-in (management support), baseline/risk assessment testing, and staying abreast with current trends/technologies/standards. A key recommendation is for leaders to establish a security culture where cybersecurity is seen as a value instead of another responsibility. The implications for positive social change include the potential for cybersecurity leaders to reduce the occurrence of breaches while enhancing people's perceptions and knowledge of cybercrime threats in their organizations creating a positive impact on social implications.

Exploring Strategies Leaders Use for Enforcing Cybersecurity Policies to Protect Information Systems and Data

by

Ma'risa LaShawn Young

MS.IT, Walden University, 2022

MS, Western Governors University, 2019

BS, American Military University, 2018

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

July 2024

Dedication

To The Love of My Life,

I dedicate this dissertation to you, Bre'Lon. I admire you more than words can say. You have always been the biggest blessing in my life and with your support and encouragement throughout my academic journey, I was able to complete this journey. Your love, patience, and understanding have been the pillars of my strength, and I could not have accomplished this childhood dream without you by my side. The way you believe in me, your willingness to listen to my endless thoughts, and your gentle nudges to keep me on track have been invaluable. The constant reassurance, even during the most challenging times, has helped me stay focused on my goals and has given me the courage to pursue all of my dreams. You know that this 3 year journey has not been a easy one and through it all, you have been my rock. I cannot thank you enough for all that you have done for me. I hope that you see this dissertation as a testament to the love, patience, and commitment that I have for you and our relationship, and that it brings us closer together as we continue to navigate this journey called life together.

Acknowledgments

I would like to thank God, for making it possible for me to complete this doctoral study. I want to thank my chair, Dr. Alan Dawson, for his mentoring, support, motivation, and guidance throughout writing my doctoral study. Without his support and motivation, I would not have understood and completed this study. Another thanks to my mentor, Dr. Tovi B. Williams. You have always been an inspiration to me and thank you for all of the long talks we have had in the 10 years of knowing each other. I am so proud to call you a friend.

Lastly, I would also like to acknowledge the support of all of my family and friends who have continuously encouraged me throughout this entire process. With the help of my husband, my kids, my parents, my best friends, and my DD 214 crew for their moral support and encouragement, it gave me the strength to keep on pushing until I had completed my study. I cannot thank you all enough.

Table of Contents

List of Tables

Section 1: Foundation of the Study

In this section, I will present the background of the problem, the problem statement, the purpose statement, and the nature of the study. I will explain the assumptions, limitations, and delimitations of the study. Lastly, I will present the study's research question, conceptual framework, and its significance.

Background of the Problem

The issue of cyber security remains a problem to many people (Aldawood & Skinner, 2019). Companies and organizations work diligently around the clock to ensure that they have working cybersecurity policies in place that help address and manage security problems that may arise, as well as implement different strategies to mitigate security risks. There are internal and external factors that are the causes of these security threats. Even though there are technical causes, people cause most cases through ignorance or negligence regarding data protection.

Cybersecurity policies are not necessarily the issue in this case. The lack of employee cybersecurity policy compliance is a substantial threat to companies and organizations. Liu et al. (2020) stated that organizations must have enhanced strategies to foster compliance with adopted information security strategies and policies. Because employees cause most security incidents, they are the weakest link in cybersecurity (Bauer et al., 2017). With the help of proper training and education on the subject, policy compliance may be enhanced, and the number of security incidents may come to a minimum. To reduce the risk, they pose harm to your company's security, consider

creative ways to engage and encourage employees to proactively contribute to your cyber security (Kemper, 2019).

Problem Statement

Maximizing the likelihood that employees comply with an organization's cybersecurity policy (internet use, passwords, antivirus software, BYOD (bring your own device), etc.) can reduce the risk of a costly and inconvenient data breach or network intrusion (Cram et al., 2020). Most organizations have an already implemented cybersecurity policy to promote secure behavior by employees, but over 50% of data breaches result from noncompliance with the cybersecurity policy. The general information technology (IT) problem is that employee noncompliance with organizational cybersecurity policies leads to increased security risks. The specific IT problem is the lack of strategies by cybersecurity leaders to enforce employee compliance with organizational cybersecurity policies, which can lead to increased security risks.

Purpose Statement

The purpose of this qualitative, pragmatic inquiry study is to explore the strategies that cybersecurity leaders use to enforce cybersecurity policies in an organization to protect organizational information systems and data. The study population of the study will be cybersecurity leaders associated with cybersecurity policies and the implementation and enforcement in eight large organizations located in the Southeastern United States. The cybersecurity leaders will include information system security officers (ISSO), cybersecurity managers, and chief information security officers (CISOs). The findings from this study may contribute to social change by improving the confidentiality

of data, reducing breaches, enhancing the integrity of personal information, continuous availability of services, and the safety of life through improved cybersecurity compliance and awareness.

Nature of the Study

My intent in this qualitative, pragmatic inquiry study is to explore the strategies that cybersecurity leaders use to enforce cybersecurity policies in an organization to protect organizational information systems and data. This approach is appropriate for this study because, as part of a pragmatic inquiry, one acknowledges that individuals within social settings (including organizations) experience action and change differently, and this enables them to be flexible in how they conduct investigations on increased security risk due to employee noncompliance of cybersecurity policies. Qualitative research is done with the intention of addressing questions concerned with developing an understanding of the meaning and experience dimensions of humans' lives and social worlds. This study is designed to provide a greater understanding of the tactics of cybersecurity awareness and training used to educate employees on practices to protect organizational information systems and data. Using the qualitative research method is the most suitable for this study because I am focusing on multiple organizations and their successful implementation of cybersecurity awareness and training programs. Qualitative research promotes the generation of detailed and rich responses to intricate subjects (Cope, 2014). This is the reason I am deciding not to collect numerical data to evaluate my research questions. When you conduct quantitative evaluations, numbers represent data. This ensures precise, specific, and concrete information (Aspers & Corte,

2019). Qualitative data captures the "lived experience." Instead of numbers, words represent the findings. Mixed methods research encompasses the incorporation of qualitative and quantitative methods and should only be utilized in the combination of methods better explains the research question than a single approach alone (Halcomb, 2019).

Research Question

What strategies do cybersecurity leaders use to enforce cybersecurity policies in an organization to protect organizational information systems and data?

Interview/Survey Questions

Demographic Questions

1. What is your current job role?
2. How long have you been in your current role?
3. What other job roles have you held in the field of cybersecurity?

Interview Questions

1. What aspects of cybersecurity interest you most?
2. What do you feel are the components of a good cybersecurity program?
3. What strategies would you use to promote the protection of information systems and data?
4. Can you describe your experience with developing and implementing cybersecurity policies?
5. How would you assess the effectiveness of cybersecurity policies once they have been implemented?

6. How would you collaborate with other departments or teams to ensure that cybersecurity policies are integrated into all aspects of the business operations?
7. How would you determine that employees have been adequately trained to protect information systems and data?
8. How do you ensure that cybersecurity policies are regularly updated and remain relevant in the face of evolving threats and technologies?
9. How do you stay informed about new trends, technologies, and best practices in cybersecurity to continuously improve policy implementation and security posture?

Theoretical or Conceptual Framework

The conceptual framework of this study is the social cognitive theory (SCT). In 1986, Albert Bandura developed this conceptual framework. SCT emphasizes the reciprocal interaction between individuals, their environment, and their cognitive processes. It posits that behavior is influenced by observational learning, self-efficacy beliefs, outcome expectations, and self-regulation. SCT uses a triadic model consisting of personal, behavioral, and environmental determinates, all of which interact with each other to shape human behavior (Bandura, 1989). Key constructs in SCT include self-efficacy (belief in one's ability to perform a behavior), observational learning (learning through observing others), outcome expectations (anticipated consequences of behavior), and self-regulation (the ability to set goals and regulate one's behavior). According to H.

N. Young et al. (2005), outcome expectancy and self-efficacy beliefs are constructs central to SCT.

Self-efficacy is the belief an individual has in themselves to accomplish something or overcome a challenge. Self-regulation refers to an individual being able to self-assess their actions (Benight et al., 2018). Social learning refers to the persuasions incurred from negative and positive social influences which impact an individual's learning (Lowry et al., 2017). Outcome expectancy is related to an individual's ability to assess the rewards versus consequences of taking action (Schoenfeld et al., 2017). Based on the SCT: (a) individuals' behavioral intentions are guided by outcome expectancies and self-efficacy, and (b) individuals' behaviors are influenced by behavioral intentions and sociostructural factors (Shahangian et al., 2021). Regarding outcome expectancy, people are motivated to perform a particular behavior if they feel driven, while self-efficacy deals with judgments of one's learning and performing actions when handling the prospective situation (Kursan Milaković, 2021; Schunk & Pajares, 2009; H. N. Young et al., 2005). SCT has been applied to various domains, including education, health, organizational behavior, and social psychology. It can be used to understand and promote behavior change, motivation, and learning processes.

The rationale behind choosing SCT as the conceptual framework because it aligned well with the implementation of cybersecurity awareness and training programs. The behavior and learning of an individual are based on intrinsic and extrinsic factors, as presented in the triadic model. Awareness and training programs in a corporate atmosphere may fail at teaching regular users' cybersecurity principles (Ricci et al.,

2018). Examining cybersecurity awareness and training strategies of IT leaders to improve user self-efficacy is important, and SCT is applicable. By relying on SCT as an interpretative framework, the study asserts that the determinants behind these perceptions and behaviors differ based on additional environmental and individual factors, such as how the general public perceives underperformance and over-performance in the context of cybersecurity preparedness. Successful cybersecurity programs require a mechanism to measure the success of objectives (Bozkus Kahyaoglu & Caliyurt, 2018) and applies to the goal-setting construct of SCT. Finally, social learning is a mechanism to deter the misuse of information systems by emphasizing the consequences of inappropriate actions (D'Arcy et al., 2009). For the reasons listed above, SCT is an appropriate theory to apply to the conceptual framework in examining cybersecurity awareness and training strategies in organizational use by IT leaders.

Definition of Terms

Cybersecurity training: Actions aimed to improve the skills and abilities of others (Beuran et al., 2018a).

Organizational cybersecurity leader: An individual that leads other IT/ Cybersecurity employees within the organization and manages the implementation of strategy, policy, and technology related to IT, such as a CEO, COO, CIO, CISO, IT director, IT manager, or general manager (Hickman & Akdere, 2018).

Policy generation: Policies that are generated based on associated labels with user-specific behaviors (AlQadheeb et al., 2022).

Sensitive data: Data that is considered sensitive or data in which sensitive details about an individual can be determined or extrapolated (Shabani & Borry, 2017).

Assumptions, Limitations, and Delimitations

Assumptions

Assumptions are concepts or facts imposed on the study that are accepted as true (Uprichard & Dawney, 2016). In this study, the assumption was made that S possess a strong understanding and knowledge of cybersecurity awareness and training programs. I also assumed that the participants responded truthfully, accurately, and honestly to the open-ended questions. I assumed that the use of a qualitative research methodology would be effective in providing the data needed to answer the research question. I constructed the interview questions in a manner to facilitate a discussion to acquire used cybersecurity practices used to enforce cybersecurity policies.

Limitations

Limitations of a study are potential weaknesses of a research study that may require future work to resolve or opportunities to perform additional research (Hall & Martin, 2019). There are a few limitations and challenges that may arise. The first limitation of this study is the geographic study location is in the Southeastern United States, which may produce results that may not be generalized nor transferable to other locations. The second limitation is cybersecurity leaders may not have much time for an interview due to their busy schedules. Another limitation includes getting participants to participate, and lastly, participants may not be truthful in their responses due to not wanting to give away "trade secrets".

Delimitations

Delimitations are constraints and boundaries that researchers impose in qualitative studies to scope the study (Alpi & Evans, 2019). First, participants of the study will include organizational cybersecurity leaders who possess the knowledge and/or experience of implementing cybersecurity awareness and training strategies at their organization. Second, the interviews will be open-ended to promote the open and transparent sharing of their experiences and observations about the implementation of cybersecurity awareness and training programs at their organization.

Significance of the Study

Contribution to Information Technology Practice

So many cybersecurity attacks have occurred to organizations throughout the world due to the nonexistence of a mature risk culture in the targeted organizations. This is the reason behind the need to enforce cybersecurity policies that will help reduce security risks and assist in preventing security breaches and improve cybersecurity compliance. This research study may contribute to the cybersecurity body of knowledge because it includes strategies for implementing cybersecurity policies. This research's findings may assist cybersecurity managers by providing them with strategies for implementing cybersecurity policies, overcoming the challenges that come with the process, understanding cybersecurity compliance better, and developing, enforcing, and implementing better cybersecurity policies. This study's findings may offer a comprehensive approach to the implementation of cybersecurity policies and fill in the gaps with existing literature.

One of the biggest gaps between the existing literature and current studies is the human behavior aspect. While there are studies that talk about human behavior and its effects on the workplace, there is limited research that ties SCT directly into employee compliance on cybersecurity with protecting and safeguarding its data and systems. This study helps to tie in the organizational culture, leadership support, training programs all to the overall cybersecurity climate. Most cybersecurity leaders have interventions in place such as training to improve compliance but their effectiveness is not studied. The study's findings may also help improve the cybersecurity culture by addressing the effectiveness of these different programs used to improve compliance in various organizations that require the recommended cybersecurity measures.

Implications for Social Change

This study is significant in that the findings from the research will contribute to a positive social change and impact on the public. Data breaches cause various impacts, including economic costs, to both business organizations and individual consumers (P. Wang et al., 2019). By utilizing the findings in this study, cybersecurity leaders can implement cybersecurity measures that could enhance the organization's and the public's confidence by assuring them of the safety of their personal information, the confidentiality of their data, the integrity of their data, and the availability of their services. The knowledge of how cybersecurity leaders execute these policies is of extreme essence as it contributes to the orderliness and security of organizational information systems (Blum, 2020). Aldawood and Skinner (2019) suggested that policies and procedures play a huge role in 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. This study's findings may help cybersecurity leaders learn how to implement cybersecurity policies that have the potential to reduce the occurrence of breaches while enhancing people's perceptions and knowledge of cybercrime threats in their organizations.

A Review of the Professional and Academic Literature

This qualitative, pragmatic inquiry study is to explore the strategies that cybersecurity leaders use to enforce cybersecurity policies in an organization to protect organizational information systems and data. The focus of the literature review was the research question: What strategies do cybersecurity leaders use to enforce cybersecurity policies in an organization to protect organizational information systems and data? I researched the background on the need for cybersecurity policies and how to encourage their adoption among staff. I then researched strategies on creating cybersecurity rules, employee cybersecurity policy compliance, and the origins of security assaults and tactics for enforcing cybersecurity policies

Keywords used for searching literature included: *Criminal violations, cyberattacks, data leakage, data compromise, secrecy, integrity, reliability, and non-repudiation, cybersecurity policies, social cognitive theory, human factor, cybersecurity education, data compromise, information security, pragmatic inquiry, qualitative methods, ransomware trojans, phishing, internet security, information technology,* and *social engineering*. were used to find relevant literature. I also used keyword

combinations to find correlations that may affect this study. These sites will present academic and industrial cybersecurity awareness and training perspectives on cybersecurity policies.

This literature review references several journals, publications, and conferences. The main research sources include Sage Journals, Google Scholar, ScienceDirect, IEEE Xplore Digital Library, ResearchGate, ProQuest Computing, and ProQuest Dissertations and Theses Global. I used Ulrich Web World Serials Directory verified peer-review. 117 (100%) of the 117 peer-reviewed articles I studied were published within five years of my predicted graduation.

The literature review focuses on a few areas: (a) SCT; (b) human aspects; (c) cybersecurity awareness, strategies, and the implementation of policies. The review of the four components and three determinants of SCT focused on the educating and awareness of human beings. The four constructs consist of self-efficacy, self-regulation, social learning, and outcome expectancy. The three determinants consist of personal, behavioral, and environmental factors. Finally, the research talks about cybersecurity awareness, strategies and the implementation and best practices of enforcing cybersecurity policies.

Choosing Social Cognitive Theory (SCT) as a framework

Behavioral psychology is a seminal school of thought which explores the impact of the environment on human behavior. In most instances, the discipline offers insight into how scholars and practitioners can use classical and operant conditioning to harness positive behavior. A key aspect of behavioral psychology is observational and social

learning which explores how people develop knowledge and beliefs by watching others. This aspect is predicated on the social cognitive theory coined by Albert Bandura in 1977. He drew inspiration from other behaviorists including Wastson and Thorndike. Initially, the practitioner used insight about social modelling on learning and imitation to base his assumptions. The insight allowed him to identify discrepancies and conduct research on the subject (Devi et al., 2022). Furthermore, he used the foundational knowledge to explore the principles of knowledge acquisition in the human social setting while incorporating them with cognitive psychology. The combination process was useful in generating a broader theory pertaining to human functioning based on individual thought and action.

The first conception of SCT was the social learning theory (SLT). The predecessor sought to describe the manner through which children learn from each other based on modeling, imitation, and observation. The guiding hypothesis was that the three processes work together to enhance knowledge acquisition and behavioral modification vis-à-vis normal interactions. Furthermore, the methodologies permit people to mimic desired behaviors of their peers and the surrounding environment. According to Bandura (2001), learning is influenced by cognitive and observational factors which define and predict behavior. SCT integrates various elements from the sociological and psychological fields to consider specific channels and methods used in the acquisition and sustenance of behavior (Devi et al., 2022). Nonetheless, the theoretical framework alludes to the role of self-beliefs in defining motivations, expectancies, and reinforcements.

Four Components of SCT

The basic idea behind SCT is that there is an intricate interplay between various processes and factors. The theory comes intact with four constructs, self-efficacy, self-regulation, social learning, and outcome expectancy. Self-efficacy is an individual understanding of ability and potential. Based on Bandura's experiment, people develop beliefs about their capabilities, allowing them to attain specific performance levels. These beliefs further influence specific events and variables that affect their lives (Code, 2020). They help determine how a person feels, thinks, motivates, and behaves. Nonetheless, self-efficacy allows an individual to engage in activities depending on their inherent sense of competence. Also, research shows that the person utilizes their previous experiences as a tool for motivation.

A common tenet in SCT is that self-efficacy equals control. In Layman’s terms, an influx in the former contributes to higher management or control of one’s behaviors, actions, and motivations. Such individuals exhibit an inherent belief that their actions are connected to the outcomes. However, scholars argue that a decline in self-efficacy contributes to feelings of helplessness (Devi et al., 2022). In light of this, a person witnesses low levels of motivation which hampers their ability to change behavior. It is critical to note that individual action depends on a conglomerate of motivational, cognitive, and affective processes. Bandura (2001) showed that these processes directly determine individual conviction of their self-efficacy. They work together or separately to enact action thereby generating desirable or nondesirable results from specific events.

However, it is critical to note that self-efficacy is sourced from divergent sources. First, a person can develop confidence by mastering experiences. This level of mastery involves performing each task successfully which plays a role in enhancing individual confidence. Contrarily, failure is connected with a decline in self-efficacy since a person does not trust themselves. The second source is social modelling whereby people witness others completing or engaging in various activities. In most instances, observers raise the belief that they possess the necessary capabilities to master each task and succeed (Code, 2020). This stems from seeing others follow a similar protocol or guideline towards success. Source 3 revolves around social persuasion which entails the use of positive and encouraging statements. These statements work as incentive sand motivators thereby allowing a person to work towards goal attainment. Scholars allude that the provision of verbal encouragement allows individuals to overcome inherent self-doubt while focusing their best effort towards the task. Self-efficacy and the effectiveness of an organization's cybersecurity program are directly related to each other. The effectiveness of organizational cybersecurity program has a significant influence on self-efficacy, and self-efficacy has a significant influence on security compliance intent (Yoo et al., 2018). Senior management buy-in and organizational practices and policies related to cybersecurity awareness and training programs significantly influenced employee self-efficacy of cybersecurity principles (Cuganesan et al., 2017). Finally, self-efficacy can be harnessed via psychological responses to situations. A person's responses and emotional reactions impact how they feel about their personal abilities in various contexts.

Self-regulation is presented as a system which determines individual ability to direct their actions. The system is distinguished into three subfunctions including self-monitoring. This prong requires people to monitor their behavior and identify key influences, determinants, and direct effects. They use the monitoring process to judge and determine the nature of their behavioral tendencies. Subfunction 2 focuses on developing individual standards and evaluating them against moral or social guidelines. The guidelines enhance affective self-reaction (sb3) whereby a person becomes satisfied or dissatisfied with their behavior. They also facilitate self-sanction which curbs deviancy and improves positive behavior. SCT shows that the aspects and prongs are characterized by constant formulation of standards and referential comparisons.

The aforementioned system is also marked by reinforcement strategies. The first type is extrinsic which is offered by an external actor or standard. It helps support the development of desired actions while floating or presenting the likely consequences. On the other hand, intrinsic reinforcements are useful in harnessing self-efficacy and pride. The two feelings are guided by self-regulation which establishes a domain based on stable evaluative standards. Nonetheless, the domain contains varied and complex judgmental factors that help determine individual thoughts, emotions, and behavior. Therefore, the system is seminal in controlling disruptive impulses and emotions by setting a clear mode of operation and guidelines. It further emphasizes thinking before acting, thus reducing conflicting tendencies.

It is imperative to note that self-regulation occurs in various cyclical phases starting with forethought. This phase contributes to learning behavior and facilitates the

development of motivation which precedes effort to influence a person's preparation and willingness to engage in specific tendencies. The next stage is marked by performance-based actions that affect individual concentration and performance. The actions depend on the set objectives and a person's determination to become successful in their endeavors. Finally, self-regulation entails reflection with the participant reviewing their experiences to identify problem areas and opportunities for future success. The final phase generates feedback and influences considerations about the next activity.

Social/observational learning explores the processes involved in developing knowledge and behavior. SCT contends that learning occurs through continuous exposure to media or interpersonal displays of the same behavior. Therefore, peer modeling is lauded as a seminal strategy for influencing behavior. This is because individuals frequently imitate, especially when they perceive the models to be similar to themselves. An in-depth review of Bandura's arguments reveals they were radical compared to other behaviorists. The social learning component allows individuals to acquire information quickly by observing and mimicking environmental models. Nonetheless, Bandura built upon insights by Skinner by showing that social learning occurs in four steps (Devi et al., 2022). The first step revolves around attentional processes whereby individuals derive information from the milieu. They can choose to follow media examples or real-life models. The processes are often described as cognitive abilities that manage the sensory registration of modeled actions.

Step 2 focuses on retention mechanisms where they memorize the information in long-term memory (LTM). The mechanisms allow them to recall and recreate the

behavior in similar or differing circumstances. Retention techniques take transitory influences, converted into internal guides representing the memory. Step 3 entails motor production or reproduction, which moves component actions in the memory toward overt actions. The movement process is based on the apt nature of the environment or setting. However, SCT highlights that the observer might not perfectly reproduce the seen action. They might alter or modify the behavior to produce a version that is apt based on the situation (Manjarres-Posada et al., 2020). Furthermore, the theory denotes that the person must possess the ability and skills to reproduce each behavior. The lack of capabilities contributes to a decline in learning.

Motivational processes make up the final stage whereby they influence the emergence of behavior as overt action. SCT shows that the emergence process requires individuals to balance their behavioral tendencies on specific results and outcomes. It further contends that a person will likely repeat an action in the presence of a reward. They might however dismiss it when consequences are involved or probable. There are three sources involved when generating and harnessing motivation. The first source, expectancy, focuses on individual belief about behavioral success. It can be distinguished into situation-outcome which revolves around the connection between events. Outcome expectancies come in second as they pertain to the expected consequences and results. Finally, self-efficacy expectations help define individual mastery which affects the initiation and maintenance of coping behaviors (Alnoaim, 2022). Expectancy sources are complemented by value and affective reactions. The former highlights the significance of

a goal attained by specific actions. Comparatively, affective forms pertain to individual feelings and reactions.

Nonetheless, SCT shows that observational learning is connected with motives and punishment. Past reinforcement refers to a previous event where a person was rewarded for their efforts. It co-occurs with past punishment where they were admonished for going against the standards (Manjarres-Posada et al., 2020). Comparatively, promised reinforcements are those which a person can imagine. It is imperative to note that these forms tie with forethought whereby a person develops pictures or images of future rewards. The final type is vicarious wherein individuals see and recall the model being reinforced. However, the use of punishment does not contribute to positive responses as compared to reinforcement.

Outcome expectancy (OE) is a key component which involves gauging consequences based on benefits and demerits. It is subjective by nature while serving as a multiplicative function of motivation. Valence is a key dimension of OE which involves classifying consequences into positive or negative. Likewise, OE involves temporal proximity, which evaluates consequences based on the timeline. Specifically, this prong shows that people determine the outcomes in the short- or long-term. The former expectancies are more powerful in motivating behavior since they are often proximal to a person. Comparatively, the latter are deemed as distal, with people avoiding them due to the lack of certainty regarding their impact. However, individual differences exist regarding the consequences.

The final dimension is the area of consequences, which involves anticipating self-evaluative, social, and physical outcomes. The self-evaluative results are tied to emotional experiences after engaging in a specific activity or behavior. A person might be satisfied or feel ashamed based on their internal standards (Fasbender, 2019; Murphy, 2022). The standards tie back to the self-regulation (sub-function) system. Comparatively, social OE captures the likely environmental and external responses to a behavior. For instance, an employee might be cautious about being receiving a verbal counseling. On the other hand, physical OE examines individual experiences, which can be divided into positive/negative and short-/long-term.

However, there is a need to distinguish between the key concepts of self-efficacy including judgments and beliefs. The judgments refer to an outcome of process commonly contextualized in the present setting. They are often specific to a particular objective and do not extend past a person's inherent capabilities (Poluektova et al., 2023). The specificity is seminal in developing solutions to problems affecting the attainment of various objectives. The solutions combine myriad parallel verdicts to exert coping tendencies and apprise a person of their limitations. In contrast, the beliefs are often stable and general. This means that they extend towards the general domain of functioning that comprises various cognitive and mental structures. These structures work together to develop and distinguish knowledge that can be used when guiding individual processes or behavior. Nonetheless, the global cognitions harness a similar meaning and function pertaining to individual or collective successes.

Modes of Human Agency

A critical tenet in SCT is human agency, which refers to individual power to originate action. Bandura's theory denotes that individuals must be able to control and manage their behavior, motivation, and cognition. The control and management process relies on the development of self-efficacy and beliefs. These beliefs allow people to operate while considering mediative efforts and sociocultural environmental aspects.

Intentionality. The first feature, intention, revolves around a person's desire to act in a specific way depending on an existing idea and mental state. Code (2020) shows that the behavior can be accommodative or disruptive. Their respective nature is determined by the supposed value and consequence. Nonetheless, the element helps formulate proactive commitment with individuals relying on their personal interests and motivators. They distinguish the outcomes as consequences rather than agentive acts while actualizing key desires via goal setting and planning. The planning process hinges on rational and impulsive decisions that are largely situational (Alnoaim, 2022). In Layman's terms, a person selects the specific social and environmental settings which align with their goals, values, and strengths. Likewise, intentionality uses self-regulatory tools which increase individual commitment and coordination. These tools predicate on cognitive features to boost motivation and inherent desire to succeed.

Additionally, Bandura's SCT shows that the mode sets up a foundation for social cognition in divergent ways. It begins by unlocking the ontology of the mind due to its wide-ranging representation of basic mental categories. These categories are inclusive of awareness, belief, and desire. The awareness aspect is linked intermittently with self-regulation since a person is cognizant of their strengths and limitations. On the other

hand, belief revolves around self-efficacy as individuals develop a goal-oriented attitude depending on their capabilities. These capabilities push them towards an inherent desire to become the best at what they do.

Nonetheless, this mode of agency helps establish order and a structure to behavioral perceptions. In Layman's terms, SCT shows that intentionality allows a perceiver to identify the structure of their intentions and actions. They determine the likelihood of their behavior contributing to either positive or negative behavior. This determination enhances action-development and alleviates the risk of engaging in risky tendencies. It further extends towards coordinating social interaction since people are able to define their behaviors based on specific standards. In most cases, these explanations identify underlying mental causes behind various ideologies or processes.

To this end, Bandura (2001) indicated that the mode facilitates conscious thought and impacts both normal and automatic action control. Individuals with a heightened sense of agency are likely to develop self-affirming thoughts which form intention and mitigate counterfactuals. They constantly modify their conscious to overcome handicapping behavior marked by incessant sabotage of one's pursuit for achievement. The overcoming process mitigates a need for excuses for potential failure as a person holds themselves accountable depending on various standards. Also, intentionality formation occurs in a content specific route directed at the attainment of predefined goals. The route ensures that a person develops an attitude of success based on initial or past goal pursuits while outlining potential handicaps that might hamper their trajectory.

Forethought focuses on individual's ability to identify and evaluate outcomes. This mode of human agency moves past the normal futuristic planning with people setting goals and determining the prospective actions. Nonetheless, they formulate mitigation plans aimed at alleviating detrimental effects (Code, 2020). Through forethought, a person motivates themselves and develops a guiding framework while anticipating the future. SCT works in tandem with the self-determination theory to distinguish individual motivation into two forms, including intrinsic and extrinsic. Regardless of their differences, the two types are useful in developing a forethoughtful perspective that offers coherence, direction, and meaning (Bandura, 2001). Gradually, a person reorders their priorities and learns how to plan ahead. They further structure their lives based on their expectancies and the environment. The structuring phase relies on regulating individual behavior to achieve the pre-established goals.

However, Code (2020) shows that future events are not caused by current motivation and actions. This is because they lack actual existence. Comparatively, they are developed in the cognitive aspects, which allow people to convert each event into current behavioral regulators and motivators. The conversion then leads to the creation of anticipatory self-guidance, affective self-reactions, and sanctions. The self-reactions are also based on the construction of OE from observed conditional relationships between environmental events and associated outcomes.

Moving further, foresight–based behavior is a byproduct of the immediate environment. This environment influences a person's ability to transcend challenges and shape the present to fit the desired future. In light of this, people discard courses of action

that contribute to punishing outcomes and consequences (Manjarres-Posada et al., 2020). They develop considerable self-direction when faced with competing influences while adopting personal standards defined by self-evaluative results. Therefore, the results play a critical role in augmenting or overriding the influence of external outcomes.

The next mode, self-reactiveness, revolves around the development of choices as well as defining the best course of action. SCT presents self-reactiveness as individual capability to regulate their affect, action, and motivation. The regulation process hinges on the use of personal standards which set a foundation and offer a compass to a person. Specifically, the standards influence one's capability to take the necessary action especially when they deviate from their pre-planned goals. The action is often self-directed devoid of any external influences. It relies on the integration of thought and action with the individual shifting from a planner into a motivator. They develop strategies through forethought and utilize their past experiences/punishment to manage behavior.

Code (2020) alluded that the standards and reactiveness work together to enhance agentic behavior. Therefore, a person avoids sitting back and waiting for appropriate performances to occur through manifestation or nonaction. Instead, they use their inherent motivation and desire to execute each guideline. Likewise, self-reactiveness is inextricably linked to a set of self-referent sub functions including monitoring, guidance, and reactions. The sub-functions are useful in creating a singular framework which controls external variables. The framework facilitates the development of purposeful function whereby each individual exerts control over their thoughts, actions, and

motivations. The control process hinges on an internal locus governing which/what behavior are performance. Furthermore, it relies on knowledge pertaining to probable consequences and punishment.

Moving further, Alnoaim (2022) showed that motivational standards provide guidance through discrepancy reduction and production. The former involves making the necessary corrections to attain a goal. the latter focuses on developing an action plan and objectives which are then compared against personal accomplishments. Albeit different, they both work towards personality and behavioral modification. However, self-motivation is determined by three factors including self-efficacy. A person's belief in a given behavior directly influences their ability to perform it. If they feel capable, then they will work hard and avoid distractions. The next factor denotes that insight is useful in controlling or adjusting efforts towards specific levels of feasibility and reality. Finally, individuals have an anticipated time to goal attainment. This variable helps distinguish goals from proximal or distal. The proximal goals are more effective in enlisting motivation compared to the latter.

The motivational standards are complemented by social and moral guidelines. SCT indicates that people can only exercise moral agency if they establish a relationship between their thoughts and conduct. This relationship is defined by continuous self-reprimand and approval depending on the social standards. For instance, if a person believes that stealing is bad, they will engage in positive behavior to ensure that their conduct aligns with the social standard (Fasbender, 2019). The social guidelines are developed through direct instruction, behavioral feedback, and modeling. Direct

instruction often emanates from people with authority who inform a person on what they should do or avoid. Comparatively, behavioral feedback can be derived from colleagues, parents, or teachers. It apprises an individual about the associated consequences of their behavior. Finally, modeling outweighs verbal/direct instruction as it influences the internalization of standards and morals.

The final property, self-reflectiveness, enables individuals to evaluate their experiences and thought processes. The evaluation processes allow them to modify their action and harness self-efficacy. This form is central in SCT as it determines individual regulation and response to stimuli. According to the theory, people will formulate perceptions about their inherent characteristics and abilities. These lenses are useful in guiding their behavior by analyzing what the person intends to achieve. Likewise, their intention directly influences the level of effort exerted into each performance.

Bandura cited that people serve as self-examiners and agents of action. The two-pronged role is defined by their metacognitive capability to continuously reflect upon themselves. This ability allows them to gauge whether their thoughts and actions are concomitant with expected outcomes and expectancies (Bandura, 2001). The use of self-reflective methodologies enhances individual ability to motivation-based conflicts. For instance, they conduct cost-benefit analyses, allowing them to act in favor of one over another. The metacognitive activity is also linked with direct evaluation of operative and predictive thinking. The operative aspect entails determining how to attain each goal. The predictive tenet revolves around the expected outcomes and effects of other people's actions. Nonetheless, self-reflectiveness requires a person to change their agentive stance.

A causal structure is involved in the changing process aimed at defining the specific efficacy-related beliefs influencing individual adaptation. However, Nickerson (2023) cited that the modifications hinge on subjective motivators combining with ecological influences. The two work together to influence discrete development of either self-hindering or self-enhancing perspectives.

Triadic Reciprocal Determinism Model and Constructs

The SCT theory is based on the triadic reciprocal determinism model. This framework offers a vivid description of the correlation between environmental, personal, and behavioral factors. First, Schiavo et al. (2019) opined that the environmental factors revolve around the context where the behavior occurs. The milieu extends past the physical aspect and often depends on social variables that influence personal thoughts and tendencies depending on guidelines. Nonetheless, the social guidelines allow persons to engage in subjective assessments of their goals and work towards maintaining coherence (Schiavo et al., 2019; Woodcock & Tournaki, 2022).

The second construct is individual/personal, which includes characteristics rewarded in past experiences. This construct is marked by both personality and cognitive factors. The two work together to define individual behavior, expectations, and beliefs. The final construct is behavior, which can be reinforced or controlled in a given time or situation. The three constructs allow learning to occur through experience as a response to specific goals or interests (Yoon, 2019). Likewise, the environment plays a key role in harnessing or undermining motivation. They enjoy a bidirectional relationship that establishes a deterministic system accounting for each output and outcome.

Furthermore, the model supposes that the environment operates as either a facilitator or constraint. A person's ability to remain autonomous is influenced by the milieu. It often contains divergent stimuli which influence individual action and responses while allowing them to express or dismiss specific behavioral tendencies. Likewise, behavior operates as an outcome and driver behind the model. Most people rely on their tendencies to develop distinguishable characteristics which reflect their desires. The characteristics depend on cues and incentives with punishment helping curb deviancy.

Also, the constructs permit continuous engagement in agentic action. This action or behavior ensures that individuals can adapt flexibly based on the social, geographic, or climatic environments. The personal aspects of self-efficacy and regulation enable the circumvention of constraints. Also, confidence-based beliefs are used when redesigning and constructing the milieu to a particular standard. The reconstruction is then followed by new behaviors aimed at the attainment of desired outcomes. These tendencies are passed to others through social modeling. Furthermore, Bandura highlighted that most individuals use their knowledge to enhance power over the specific settings.

Regardless of its efficiency, scholars raise concerns about the determinism models. A common issue is that the three variables enjoy a complex and dynamic relationship. Therefore, the framework is subject to continuous changes which undermines the isolation and measurement of the specific impact of each variable. Also, the framework does not consider individual differences. The lack of consideration makes it challenging for professionals to generalize the impacts and effects. The final concern is

that Bandura's model has limited power when it comes to prediction. Therefore, social behaviorists and scholars cannot aptly forecast outcomes and behaviors.

Rationale for Using Social Cognitive Theory

The SCT seamless agreement with the study's primary goals provides a strong justification for using it as the foundation of this investigation. SCT's subtle emphasis on observational learning, the tenacity of self-efficacy beliefs, outcome projections, and the self-regulatory fabric provide a specialized framework to unravel the complexity of behavioral change in the context of cybersecurity awareness and training programs. SCT mimics the complex terrain of cybersecurity practices inside organizational settings by capturing the complex interplay between cognitive processes, contextual circumstances, and behavioral outcomes (M. D. Young et al., 2014). The effort to increase user self-efficacy, promote behavioral adaptability, and develop proactive cybersecurity practices resonates well with SCT's holistic viewpoint. The thorough framework of this theory is a useful tool for disentangling the confluence of personal preferences and environmental stimuli that influence cybersecurity behavior. In conclusion, the case for adopting SCT stems from its capacity to offer a thorough, flexible, and perceptive lens through which the dynamics of cybersecurity awareness and training tactics can be successfully investigated. (M. D. Young et al., 2014)

Comparison with Alternative Frameworks

Routine Activities Theory and Social Cognitive Theory

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. RAT

emphasizes that crime occurs when three elements converge: (a) a motivated offender, (b) a suitable target, and (c) the absence of a capable guardian. Over time, RAT was used to explain changes in criminal tendencies and prevent and reduce crimes. RAT has been used to explain Cybercrime at the individual level (Kigerl, 2012).

Although RAT has demonstrated its ability to explain victimization and criminal behavior, it cannot capture the proactive nature of cybersecurity readiness. With its roots in regular activities and criminal opportunities, RAT focuses mostly on the victim-offender dyad in criminal contexts. As a result, its perspective needs to be more coordinated with the proactive goal of improving cybersecurity policies.

Theory of Planned Behavior and Social Cognitive Theory

The theory of planned behavior (TPB) was developed by Icek Ajzen as an attempt to predict human behavior (Ajzen, 1991). The TPB posits that attitude toward the behavior, subjective norm, and perceived behavioral control influence behavioral intention (Asare, 2015). According to the TPB, human behavior is guided by three kinds of considerations: beliefs about the likely consequences of the behavior (*behavioral beliefs*), beliefs about the normative expectations of others (*normative beliefs*), and beliefs about the presence of factors that may facilitate or impede performance of the behavior (*control beliefs*) (Bosnjak et al., 2020).

Despite a long history of success in predicting behavior under a variety of conditions, the TPB was unable to fully capture the nuances required to comprehend the complex interplay of psychological and environmental factors in cybersecurity contexts. The TPB's emphasis on the need to anticipate behavior is an innovative idea, but it also

needs to take into account all the other facets of cybersecurity awareness and training. A more comprehensive paradigm was required due to the interaction of cognitive processes, behavioral regulation, and environmental influences (Anderson, 2014).

Experiential Learning Theory and Social Cognitive Theory. EL, developed by Kolb in 1984, is a paradigm for resolving the contradiction between how information is gathered and how it is used (Kong, 2021). The foundation of the ELT process is within an individual's environment and consists of an individual personally performing an activity, collecting data from the activity, and reflecting on what has occurred to ultimately create knowledge (Angstmann et al., 2019). This theory focuses on experience and a problem-based learning style. Within ELT, the self-reflective phase consists of personal reflection, and the forethought phase consists of goal setting, self-efficacy, and outcome expectancies to modify future performances (Nakabayashi, 2018). ELT also aligns well with the self-efficacy construct of SCT, and both theories theorize the importance of the atmosphere on the individual throughout the learning process.

The difference between ELT and SCT is that ELT does not explain how individuals learn through social observation, and that internal and behavioral factors contribute to the overall learning process. SCT accounts for demographics, personality, and outside influences, such as the organization and social pressures from peers to influence learning, which describes the organizational force and potential factors in exploring cybersecurity programs. SCT with its triadic model incorporating personal, behavioral, and environmental variables, was the most advantageous choice. SCT's emphasis on observational learning, self-efficacy beliefs, result expectations, and self-

regulation is in accord with the complex dynamics of cybersecurity behavior (Anderson, 2014). SCT offers a thorough perspective to investigate the intricate synthesis of unique cognitive processes, social elements, and environmental triggers, in contrast to RAT,TPB, and ELT revealing a more fundamental understanding of cybersecurity preparedness.

Human factors within the domain of cybersecurity

Nifakos et al. (2021) conducted a thorough literature analysis on the impact of human elements on medical cybersecurity. The research, which is qualitative in nature, examines previous research to ascertain how much of an effect human variables have on safety. In comparison, Pollini et al. (2021) took a holistic scientific strategy for cybersecurity by emphasizing the importance of human aspects. This study investigates the impact of human factors on cybersecurity events using a combination of surveys and in-depth interviews.

Nobles (2022) investigated the effects of human elements, including stress, burnout, and security weariness, on a group's security posture. The research gathers data regarding the incidence of these variables across cybersecurity specialists through a survey-based methodology. In contrast, Linkov et al. (2019) research focuses on human elements in automated vehicle cybersecurity that addresses emerging topics. A summary of the applicable literature is provided in this study, which is also qualitative. Although using different approaches, all four studies emphasize the vital significance of human elements in cybersecurity. Pollini et al. (2021) believed that an inclusive strategy that makes use of human factors may be highly effective in minimizing cybersecurity

incidents, whereas Nifakos et al. (2021) observed that human factors have an important influence on the effectiveness of cybersecurity operations. While Linkov et al. outlined major topics of study on the subject, Nobles highlighted the possible detrimental impact of stress, stress, and safety fatigue on cyberspace efforts.

Overall, the research offers important conclusions about the importance of human factors in security and emphasizes the significance of taking these variables into account when developing and implementing cybersecurity policies. Therefore, further study is required to understand the intricate relationship between human factors with cybersecurity as well as to create efficient methods for reducing the negative effects of these elements on cybersecurity efforts.

Impacts of the Human Factor on Cybersecurity

I studied and researched both quantitative and qualitative studies and both of them yielded the same results when it comes to the human factor in cybersecurity. Ani et al. (2019) focused on the industrial workforce, while Jeong et al. (2019) took a broader approach to understanding human factors in cybersecurity. Both studies employed a quantitative approach, using survey instruments to collect data. Ani et al. (2019) used a survey instrument to assess the cybersecurity capacity of the industrial workforce, while Jeong et al. (2019) used a survey to assess the cybersecurity awareness of employees. Ani et al. (2019) used descriptive statistics to analyze the data, while Jeong et al. (2019) used factor analysis and regression analysis to explore the relationships between variables.

Both Nifakos et al. (2021) and Alsharif et al. (2022) examined the effect of human weaknesses on privacy, but they did it from vastly different angles. Although Alsharif et

al. (2022) did a literature study to investigate the impact of human weaknesses on security, Nifakos et al. (2021) conducted a systematic review of the literature to investigate the impact of human elements on cybersecurity inside healthcare companies. Alsharif et al. (2022) had to use a quantitative technique, while Nifakos et al. (2021) used a qualitative approach. Whereas Alsharif et al. (2022) utilized descriptive statistics to assess the data, Nifakos et al. (2021) employed theme analysis.

All the research agreed that people are the most important part of cybersecurity. Ani et al. (2019) and Jeong et al. (2019) emphasized the significance of employee education and knowledge in averting cyber-attacks. Both Nifakos et al. (2021) and Alsharif et al. (2022) stressed the importance of taking an interdisciplinary strategy for tackling human weaknesses in cyber security. Although Nifakos et al. (2021) and Alsharif et al. (2022) dealt with human vulnerabilities, Ani et al. (2019) and Jeong et al. (2019) emphasized staff knowledge and cybercrime capability, respectively. Whereas Nifakos et al. (2021) and Alsharif et al. (2022) utilized a systematic review of the literature technique, Ani et al. (2019) and Jeong et al. (2019) employed survey tools to collect data. Whereas Alsharif et al. (2022) utilized a quantitative technique, Nifakos et al. (2021) had to use a qualitative methodology. In conclusion, these research studies emphasize the significance of the human element in cybersecurity. They both emphasized the importance of staff receiving education and awareness to prevent cyberattacks as well as the necessity of a multidisciplinary strategy to address human weaknesses in cybersecurity.

In order to better understand how human factors affect cybersecurity in healthcare providers, Nifakos et al. (2021) did a systematic study. Researchers looked at over twenty-one studies and produced eight distinct categories of human variables that affect cybersecurity. They came to the conclusion that education and awareness initiatives can assist in mitigating the risks associated with cybersecurity because human factors play such a significant part in the field.

Alsharif et al. (2022) conducted a qualitative study to look into how human weaknesses affect cybersecurity. They discovered that human flaws can dramatically raise the danger of assaults and developed a framework to address these flaws. To overcome human weaknesses, they emphasized the value of education and awareness campaigns.

To assess the cybersecurity skills of the business community, Ani et al. (2019) undertook a quantitative study. They observed that 208 workers from four different businesses had low information security and were inadequately trained. To increase the cybersecurity skills of the employee in the workplace, they developed a structure for information security. To better understand behavioral variables in cybersecurity, Jeong et al. (2019) conducted a quantitative research study. They polled 114 social media users and discovered that demographic factors, including age, ethnicity, and educational levels, have a major impact on users' attitudes and practices about online safety. To better comprehend the link between individual factors with cybersecurity, researchers created a model.

Cybersecurity policy implementation

Information security, privacy laws, and political developments in the implementation of computer systems in smart cities were the focus of a quantitative study by Habibzadeh et al. (2019). 127 experts in the field of smart cities from all over the globe were surveyed using an online questionnaire. Aldawood and Skinner (2019) provided a critical qualitative analysis of current social, technical solutions, measurements, strategies, tools, or applications in the field of cyber. The research by Habibzadeh et al. (2019), however, found that there are substantial obstacles to deploying computer networks in smart urban areas, including a shortage of cybersecurity and funds, in addition to the inadequacy of legislative framework and rules. On the opposite hand, Aldawood and Skinner (2019) conducted an extensive literature review that found that a more comprehensive and interdisciplinary strategy is necessary to effectively counter social engineering attempts. They also emphasized the significance of including human factors in security procedures and policy.

Eboibi (2020) provided a qualitative investigation of cybercrime worries in Southern Africa, Ghanaian, Ethiopia, and Nigeria and then examined the repercussions for the execution of cyberspace laws and institutional responsibility. The effect of information security knowledge on workers' security behavior was the subject of a quantitative study by Li et al. (2019). They employed regression analysis when analyzing the information, they gathered from 222 workers at various companies in China. Eboibi (2020) used a thematic analysis of existing literature to identify the challenges in addressing cybercrime in these countries, such as limited resources and inadequate legal frameworks. The author also emphasized the need for more effective policy measures and

institutional accountability to combat cybercrime (Eboibi, 2020). Li et al. (2019) results indicated that employees' cybersecurity policy awareness positively influences their cybersecurity behavior, and that the relationship is mediated by their perceived behavioral control and subjective norms.

Dedeke and Masterson (2019) conducted a comparative analysis of three cybersecurity implementation frameworks (CIF) from the United States, the United Kingdom, and Australia. They used a qualitative approach to analyze the frameworks and identified commonalities and differences in their approaches to cybersecurity implementation. They concluded that a more comprehensive approach, which considers the social, cultural, and organizational factors, is necessary for effective cybersecurity implementation. Habibzadeh et al. (2019) found that the lack of cybersecurity awareness and resources, as well as the absence of legal frameworks and policies, are significant challenges in deploying cyber-physical systems in smart cities. In contrast, Li et al. (2019) found that employees' cybersecurity policy awareness positively influences their cybersecurity behavior, suggesting that policies can be effective in promoting cybersecurity best practices among employees.

Aldawood and Skinner (2019) emphasized the need for a more holistic and multidisciplinary approach to address social engineering attacks effectively, while Dedeke and Masterson (2019) argued that a more comprehensive approach, which considers the social, cultural, and organizational factors, is necessary for effective cybersecurity implementation. These studies emphasize the significance of taking into account human elements in cybersecurity policies and procedures, implying that merely a

technical strategy might not be enough to effectively resolve cybersecurity concerns. Eboibi (2020) identified the challenges in addressing cybercrime in South Africa, Ghana, Ethiopia, and Nigeria, such as limited resources and inadequate legal frameworks. The author emphasized the need for more effective policy measures and institutional accountability to combat cybercrime, suggesting that a more comprehensive and coordinated approach is necessary to address this complex and evolving problem.

In summary, the studies reviewed here address various aspects of cybersecurity and highlight the challenges and opportunities in cybersecurity policy implementation and institutional accountability. While Habibzadeh et al. (2019) and Li et al. (2019) used quantitative methods to investigate specific aspects of cybersecurity, Aldawood and Skinner (2019), Eboibi (2020), and Dedeke and Masterson (2019) used qualitative approaches to provide critical appraisals and comparative analyses of cybersecurity measures, policies, and frameworks. Together, these studies provide valuable insights into the complex and multifaceted nature of cybersecurity and the need for multidisciplinary and holistic approaches to address it effectively.

Employee cybersecurity policy compliance

Employee cybersecurity policy compliance is essential for the success of any organization's cybersecurity strategy. Compliance ensures that employees follow the organization's cybersecurity policies and procedures to protect the organization's digital assets and sensitive information from cyber threats. The studies reviewed focus on employee cybersecurity compliance and explore numerous factors that influence employee attitudes and behaviors toward cybersecurity policies. These studies suggest

that promoting cybersecurity compliance requires a combination of organizational culture, training, communication, incentives, and user-centered approaches. While all studies address comparable topics, they employ different research methods and approaches to investigate these issues.

Cram et al. (2020) used a mixed-methods approach, trying to combine interviews and surveys to recognize the variables that lead to reduced adherence and recommend ways to boost adherence, whilst also Gundu (2019) used a quantitative research approach to determine what factors lead to the having to know disparity in worker information security conformance.

In order to better understand how cybersecurity and regulation knowledge affect employee adherence attitudes, Wong et al. (2022) used a case study methodology, focusing on the development of supply chain capacities. Reeves et al. (2021) used a qualitative methodology, combining focus group discussions and interviews, to investigate the difficulties of empowering employee satisfaction with information security, while Ameen et al. (2021) performed a cross-cultural study using a questionnaire to investigate information security adherence among Gen-Mobile working population. While all studies emphasize the importance of employee awareness, training, and motivation in promoting cybersecurity compliance, they differ in their focus and findings. For example, Cram et al. (2020) identified the lack of senior management support and inadequate training and communication as significant barriers to compliance, while Ameen et al. (2021) found that cultural differences, such as individualism and collectivism, can influence compliance behaviors. Furthermore, Reeves et al. (2021)

highlighted the issue of cyber fatigue, where employees may become disengaged and apathetic toward cybersecurity policies due to the overwhelming amount of information and training, they receive. The authors suggest that organizations should consider alternative approaches, such as gamification and social incentives, to encourage employee engagement and participation in cybersecurity initiatives.

Overall, the studies reviewed provide valuable insights into the complex issue of employee cybersecurity compliance and highlight the need for a multifaceted and tailored approach to address this problem. Organizations should also implement measures to monitor employee compliance, such as regular security assessments and audits. These measures can help identify potential vulnerabilities and ensure employees follow cybersecurity policies and procedures. While the studies use different research methods and approaches, they all emphasize the importance of employee awareness, training, motivation, organizational support, and culture in promoting cybersecurity compliance.

Gundu (2019), Cram et al. (2020), and Wong et al. (2022) all emphasize the importance of organizational culture, training, and communication in promoting cybersecurity compliance among employees. Gundu (2019) and Cram et al. (2020) use a quantitative and mixed-methods approach, respectively, to identify factors that contribute to low compliance rates, while Wong et al. (2022) use a case study approach to examine compliance attitudes and behaviors in a specific context. Ameen et al. (2021) take a cross-cultural approach to cybersecurity compliance, examining compliance behaviors among the Gen-Mobile workforce in diverse cultural contexts. The study highlights the significance of cultural norms and views toward protection, in addition to the significance

of perceived utility and convenience of use in driving compliance behaviors. The study uses a quantitative survey to identify differences in compliance behaviors across cultures. Reeves et al. (2021) focus on the issue of cyber fatigue, which refers to the exhaustion and apathy that can result from constantly dealing with cybersecurity threats. The study uses a qualitative approach to identify factors that contribute to cyber fatigue, including the complexity of security policies and the lack of perceived personal benefits from complying with policies. According to the findings, businesses should prioritize making security easier for end users by streamlining regulations and offering customized feedback and rewards.

In conclusion, employee cybersecurity policy compliance is essential for the success of an organization's cybersecurity strategy. By developing clear policies and procedures, providing regular training and education, monitoring compliance, and enforcing compliance, organizations can reduce the risk of cyber threats and protect their digital assets and sensitive information. The studies suggest that promoting cybersecurity compliance requires a combination of organizational culture, training, communication, incentives, and user-centered approaches. While some studies take a more quantitative or qualitative approach, they all emphasize the importance of addressing the complex social and cultural factors that can influence compliance behaviors.

Application to the applied IT problem

This literature review compiles numerous studies that center on different problems and difficulties associated with information technology (IT). In a quantitative analysis of the global IT project, Palvia et al. (2021) determined the top IT challenges and

issues faced by enterprises worldwide. In contrast, Sihombing (2019) conducted a qualitative examination of the legal framework of agricultural law institutions and investigated the major concerns connected to human capital and information technology. Filippova (2021) highlighted current security challenges in the information society, highlighting the need for an initiative-taking approach to security, Whereas Kaplan (2020) looked into the moral, legal, including social concerns and assessments of the use of telehealth and telemedicine even during COVID-19 pandemic.

In general, the studies are examples of several research paradigms that tackle various information technology problems. Palvia et al. (2021) and Filippova (2021) concentrated on the technical elements of information technology, whereas Sihombing (2019) and Kaplan (2020) investigated the legal, ethical, and social ramifications of information technology. Nonetheless, all of the studies agreed that it is essential to address the difficulties and problems related to IT to guarantee the technology's successful deployment and acceptance.

In addition, Palvia et al. (2021) and Filippova (2021) brought attention to the importance of taking a preventative and strategic approach to information technology security. On the other hand, Sihombing (2019) and Kaplan (2020) stressed the importance of having robust legal and ethical frameworks to oversee the use of information technology. Although the studies differed in the areas they focused on and the methods they used, they all agreed that IT problems are intricate and multifaceted and that it is necessary to take a comprehensive approach to solve them.

Palvia et al. (2021) conducted a quantitative analysis of the problems and issues that were caused by Information Technology (IT) in the context of the worldwide IT project. The authors conducted a survey that was distributed to IT workers in forty-three different countries in order to determine which obstacles and issues are the most significant in their line of work. According to the findings of the study, IT workers all over the world are particularly concerned about issues pertaining to cybersecurity, digital privacy, and big data analytics. Sihombing (2019), on the other hand, conducted a qualitative investigation of the legislative structures that control human capital and information technology in the Indonesian agricultural industry. According to the findings of the survey, some of the most significant obstacles that the industry is now facing include inadequate legal enforcement and restricted access to technology.

Filippova (2021) examined contemporary security challenges in the information society and provided an overview of the most significant risks to cybersecurity, including phishing, malware, and ransomware assaults. The need to have good cybersecurity policies and practices was underlined throughout the study to provide protection against these threats. Similarly, Kaplan (2020) investigated the moral, legal, and social problems that arose from the use of health information technology (HIT) and telemedicine during the COVID-19 epidemic. The research underlined the necessity for politicians to address issues such as privacy concerns, reimbursement for telemedicine, and the digital gap in order to guarantee equal access to healthcare.

The difficulties and problems related to the use of information technology are the primary subjects of all four of the studies mentioned above. Nonetheless, they are distinct

in terms of the precise study approaches and topics of inquiry that they focus on. While Sihombing and Kaplan investigate technology's moral and ethical ramifications in certain industries, Palvia et al. and Filippova is concerned with cybersecurity. While Filippova and Kaplan present overviews of contemporary concerns in their respective domains, Palvia et al. and Sihombing use quantitative and qualitative research methodologies, respectively.

Strategies used by cybersecurity leaders.

Cybersecurity leaders play a critical role in protecting their organization's digital assets and sensitive information from cyber threats. To be successful, these leaders must have a comprehensive understanding of cybersecurity and the ability to develop and implement effective cybersecurity strategies. Some themes that emerge from these studies are the importance of strategic leadership, effective cybersecurity strategies, and awareness in cybersecurity. Lehto and Limnéll (2020) discuss the case of Finland, where the government has taken an initiative-taking approach to cybersecurity by appointing a national cybersecurity coordinator and implementing a comprehensive national cybersecurity strategy. Similarly, Gearhart et al. (2019) emphasize the importance of leadership in higher education's cybersecurity, arguing that leaders need to prioritize cybersecurity and ensure they have the right resources and personnel to address cyber threats. Hepfer and Powell (2020) suggest that companies need to make cybersecurity a strategic asset rather than treating it as an afterthought or a technical issue.

Barosy (2019) explores successful operational cybersecurity strategies for small businesses, arguing that a multi-layered approach is necessary to address several types of

cyber threats. Goel et al. (2020) propose a strategic decision framework called PRISM for cybersecurity risk assessment, which takes into account factors such as threat probability, business impact, and risk appetite.

The study by Gearhart et al. (2019) focused on cybersecurity leadership issues and challenges in higher education. The study used a qualitative research design and conducted interviews with cybersecurity leaders in higher education to identify the leadership challenges and strategies for improving cybersecurity. The findings of the study revealed that the lack of cybersecurity awareness among employees and students, limited resources, and the complexity of the cybersecurity landscape were the main challenges faced by cybersecurity leaders in higher education. The study also highlighted the importance of leadership and communication skills for effective cybersecurity management in higher education. Cybersecurity leaders recognize that employees can be a significant vulnerability in an organization's cybersecurity strategy. To address this, they provide regular training and education to employees on best practices for cybersecurity, such as recognizing phishing frauds and avoiding risky online behavior.

In contrast, the study by Barosy (2019) aimed to identify successful operational cybersecurity strategies for small businesses. The study used a mixed-methods research design and collected data through surveys and interviews with small business owners and cybersecurity experts. The findings of the study revealed that small businesses face significant challenges in implementing effective cybersecurity strategies, such as a lack of resources, technical expertise, and awareness. The study also identified several

successful strategies for operational cybersecurity, including employee training and awareness, access control, and network segmentation.

The studies also highlight different challenges that cybersecurity leaders face. Gearhart et al. (2019) note that cybersecurity is a constantly evolving field, and leaders need to stay up to date with the latest trends and threats. Lehto and Limnéll (2020) discuss the challenge of balancing cybersecurity with other priorities, such as privacy and civil liberties. Hepfer and Powell (2020) argue that many companies struggle to attract and retain cybersecurity talent, and they suggest that organizations need to offer competitive salaries and benefits to address this issue. In terms of methodology, the studies use different approaches. Gearhart et al. (2019) and Barosy (2019) use a qualitative case study methodology to explore cybersecurity issues in higher education and small businesses, respectively. Lehto and Limnéll (2020) use a qualitative approach to examine strategic leadership in the context of cybersecurity, while Goel et al. (2020) use a quantitative approach to validate their PRISM framework. Hepfer and Powell (2020) use a combination of qualitative and quantitative methods to analyze data from a survey of cybersecurity professionals.

Overall, these studies highlight the importance of strategic leadership in addressing cybersecurity challenges. They also emphasize the need for effective cybersecurity strategies, which may vary depending on the organization and the specific threats it faces. The studies also highlight different challenges that cybersecurity leaders face, such as keeping up to date with the latest threats and attracting and retaining cybersecurity talent. The studies use different methodologies, with some focusing on case

studies and others using quantitative approaches. Taken together, these studies offer valuable insights into the strategies used by cybersecurity leaders and the challenges they face in today's rapidly evolving cybersecurity landscape.

Strategies that cybersecurity leaders use to enforce cybersecurity policies in an organization.

Yusif and Hafeez-Baig's (2021) study provides a conceptual model for cybersecurity governance. They highlight the importance of a comprehensive approach that encompasses technical, legal, and managerial aspects of cybersecurity governance. The study emphasizes that governance is essential for creating a culture of cybersecurity within an organization. In contrast, Huang and Pearlson's (2019) study is qualitative and presents a model for building a cybersecurity culture within an organization. The study proposes a six-element model that emphasizes the importance of leadership, communication, awareness, training, enforcement, and measurement in building a cybersecurity culture. The study emphasizes the importance of organizational culture in developing cybersecurity policies and inculcating them among employees.

Pöyhönen and Lehto's (2020) study focuses on trust-based architecture in the management of organization security. The study emphasizes the importance of trust-based relationships between employees and management, which can help to create an environment where employees are more willing to comply with cybersecurity policies. The authors suggest that trust can be established by providing employees with the necessary resources and training to implement cybersecurity policies effectively. The institutional strategies for cybersecurity in higher education institutions are the topic of

Cheng and Wang's (2022) study. The authors stress the importance of higher education institutions adopting a multi-layered strategy that incorporates policies, processes, and technologies to manage cybersecurity concerns.

Each of the four studies uses a unique set of research techniques to delve into a different facet of cybersecurity governance. In order to better understand how businesses may establish a cybersecurity culture, Huang and Pearlson (2019) employ a qualitative study approach. The trust-based architecture for managing organizational security is also investigated by Pöyhönen and Lehto (2020) using a qualitative method. A conceptual model for cybersecurity governance is proposed by Yusif and Hafeez-Baig (2021), and their research combines qualitative and quantitative techniques. Last but not least, Cheng and Wang (2022) use a quantitative approach to studying institutional cybersecurity initiatives in higher education institutions.

While using different approaches, all of these studies have the same overarching goal of enhancing corporate cybersecurity governance. The studies, however, focus on different areas of cybersecurity governance. Whereas Pöyhönen and Lehto (2020) concentrate on trust-based architecture, Huang and Pearlson (2019) concentrate on cybersecurity culture. A thorough model of cybersecurity governance, including policies, risk management, and leadership, is provided by Yusif and Hafeez-Baig (2021). Cheng and Wang (2022), on the other hand, focus solely on institutional cybersecurity strategies in higher education institutions.

Huang and Pearlson (2019) and Pöyhönen and Lehto (2020) used qualitative research methodologies to investigate various facets of cybersecurity governance.

Pöyhönen and Lehto look into the trust-based architecture for managing organizational security, whereas Huang and Pearlson concentrate on the creation of a cybersecurity culture. In-depth interviews with cybersecurity industry executives and experts are used in both projects to collect data.

A conceptual model for cybersecurity governance is provided by Yusif and Hafeez-Baig (2021), which encompasses several facets of cybersecurity governance, such as policy, risk management, and leadership. A survey and interviews with cybersecurity experts are included in the study's blend of qualitative and quantitative research techniques. Cheng and Wang (2022) explore organizational security strategies in educational institutions using a quantitative research methodology. IT experts in higher education institutions are surveyed to collect data.

In summary, the studies are focused on strengthening cybersecurity governance. They allow for better research to do so from a variety of perspectives and through a variety of methodologies. Researchers can now better understand the tactics and frameworks that cybersecurity leaders might employ to enforce cybersecurity policies in enterprises.

Literature-Based and Industry Document Validation

By adding both industry evidence and confirmation from the literature, the Social Cognitive Theory (SCT) chosen as the guiding framework is strengthened. Scholarly articles in a variety of domains, including education, health, organizational behavior, and social psychology, support the application of SCT. Furthermore, industry publications that deal with cybersecurity awareness and training corroborate the theory's validity in

the actual world of cybersecurity implementation. Publications, frameworks, and standards such as National Institute of Standards and Technology (NIST), ISO/IEC 27001, HITRUST, Federal Information Security Modernization Act (FISMA), Control Objectives for Information and Related Technologies (COBIT), and CIS Critical Security Controls (CIS Controls), act as a bridge between theoretical concepts and real-world applications, illustrating how SCT can be used to comprehend the intricacies of cybersecurity behavior. This method offers a solid foundation for investigating and putting into practice effective cybersecurity awareness and training strategies while strengthening the validity and applicability of the conceptual framework by fusing academic insights with corporate viewpoints (Anderson, 2014)

Cybersecurity awareness

This review's four research all examine distinct facets of cybersecurity awareness. While Quayyum et al. (2021) concentrated on security awareness for youngsters, Corallo et al. (2022) did a systematic literature study on security awareness within the setting of the industrial web of things (IIoT). Zwilling et al. (2020) did comparative research on information security, information, and behavior, while Zhang-Kennedy and Chiasson (2021) conducted a systematic review of multimedia technology for cybercrime education and awareness-raising.

Despite the fact that each study has a different focus, they all emphasize the significance of cybersecurity knowledge in various settings. Corallo et al. (2022) found that cybersecurity awareness is necessary in the IIoT to ensure security and safety, whereas Quayyum et al. (2021) stress the necessity of educating cybercrime to kids from

the beginning in order to promote secure and responsible use of technologies. Zhang-Kennedy and Chiasson (2021) looked at multimedia tools for cybersecurity awareness and education, while Corallo et al. (2022) focused on awareness and education in the setting of the industrial web of things (IIoT). Children's cyberspace understanding was studied by Quayyum et al. (2021), while cybersecurity attention, cognition, and behavior were compared across populations by Zwilling et al. (2020).

After doing a thorough literature search, Corallo et al. (2022) found twenty-eight studies that met their criteria. They discovered that IIoT cybersecurity knowledge should take into account not only technological but also institutional and psychological elements. According to the findings of the study, specialized awareness campaigns focusing on particular areas of IIoT are warranted. Zhang-Kennedy and Chiasson (2021) also conducted a systematic review and discovered thirty-seven papers that looked at multimedia technologies for cybersecurity awareness and education. The authors concluded that file management can be useful for raising cyber understanding, education, and behavior, but they also noted certain drawbacks, among them the necessity for frequent updates and the possibility of user fatigue. The importance of multimedia technologies in raising cybersecurity awareness, particularly in involving and educating users, is highlighted by Zhang-Kennedy and Chiasson (2021). Zwilling et al. (2020) came to a similar conclusion, seeing that training and instruction programs increased participants' understanding as well as conduct in regard to cybersecurity.

The research does show some divergent views on the efficacy of cybersecurity awareness campaigns, though. In spite of the increasing relevance of cybersecurity in the

IIoT, Corallo et al. (2022) discovered that there are few programs to raise information security awareness among industrial consumers. There is a dearth of studies on the efficacy of such initiatives, according to Quayyum et al. (2021), despite the fact that there is an increasing desire to promote cyber safety education for children.

Twenty-seven studies on children's information security were analyzed by Quayyum et al. (2021). The findings revealed that a number of characteristics, including age, gender, and prior exposure to computers, have an impact on children's information security. The research also emphasized the importance of providing children with a stimulating and interesting online education suitable for their age. Zwilling et al. (2020) compared information security, understanding, and behavior among three distinct groups: university graduates, working adults, and seniors. Significant disparities in cybersecurity awareness, understanding, and behavior were discovered between the groups, highlighting the necessity for targeted awareness initiatives.

Furthermore, while Zhang-Kennedy and Chiasson (2021) found multimedia tools to be effective in promoting cybersecurity awareness, they noted that there is still a lack of evaluation of the long-term effectiveness of such tools. Similarly, while Zwilling et al. (2020) found that training and education programs were effective in improving participants' knowledge and behavior, they also noted that there is a need for more comprehensive and personalized training programs to address individual differences in cybersecurity knowledge and behavior.

Overall, security awareness is an essential part of the fighting and prevention of cybercrimes. The studies listed above highlight the importance of cybersecurity

awareness in various contexts and the need for more effective and comprehensive initiatives to promote cybersecurity awareness and education. The need to increase cybersecurity capabilities and cooperation by investing in building safe, reliable, and persistent cyberspace decision-making platforms and frameworks and releasing cybersecurity leadership roles and commitment is essential to create cybersecurity and operating platform for all stakeholders that, include 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). The studies also highlight the potential effectiveness of different approaches, such as multimedia tools and personalized training programs, in promoting cybersecurity awareness.

Transition and Summary

The purpose of this qualitative, pragmatic inquiry study is to explore the strategies that cybersecurity leaders use to enforce cybersecurity policies in an organization. Section 1 comprises the introduction and foundation of my doctoral study. The section consists of the background, statement of the problem, statement of purpose, nature of the research, research question, questions for the interview, conceptual framework, definitions, and significance of the research. Furthermore, Section 1 comprises a discussion of the assumptions, limitations, and delimitations of the study and concludes with a review of the academic and professional literature.

Section 2 comprises detailed explanations of the research methodology chosen for this doctoral study. The section outlines the researcher's role, analysis of the participants, analysis of the various research methods and design approaches, the types selected for

this study, population sampling, ethical research, data collection, organization techniques, data analysis reliability, and validity.

Section 2: The Project

In this section, I will present a detailed explanation of the research methodology chosen for this doctoral study. The section outlines the researcher's role, analysis of the participants,analysis of the various research methods and design approaches, the types selected for this study, population sampling, ethical research, data collection, organization techniques, data analysis reliability, and validity.

Purpose Statement

The purpose of this qualitative, pragmatic inquiry study is to explore the approaches employed by cybersecurity leaders in implementing cybersecurity policies within an organization. The research focused on cybersecurity leaders who were involved in the development, implementation, and enforcement of cybersecurity policies within eight prominent organizations situated in the Southeastern region of the United States. The group of individuals who held positions of authority in the field of cybersecurity consisted of information system security officers (ISSO), cybersecurity managers, and chief information security officers (CISOs). The results of this study could potentially have an impact on society by enhancing the protection of data confidentiality, reducing the frequency of breaches, improving the reliability of personal information, ensuring uninterrupted access to services, and promoting safety through increased compliance and awareness of cybersecurity measures.

Role of the Researcher

I will be the primary instrument in this qualitative, pragmatic inquiry study. The role of the researcher involves activities such as providing expertise based on scientific

knowledge validated according to the norms of the respective discipline (Pohl et al., 2010). I have over 16 years of work experience and knowledge in IT and cybersecurity. I have filled many positions and roles such as IT manager, information assurance (IA) analyst, host analyst, information security support officer, database engineer, system engineer, SharePoint manager, and system administrator. My current position is risk management framework cybersecurity specialist (lead). I have worked for many government entities, such as the United States Navy, the Department of Defense (DoD), the Department of the Army, and some private organizations in relation to Information Technology. In all of those positions, I have had to deal with different entities of security awareness training as part of the requirements for all of those positions. As far as the participants are concerned, I do not have a relationship with them.

The researcher holds a pivotal role in ensuring the integrity and validity of data collection for the study. I followed the Belmont report for this study to ensure the respect of ethical research guidelines regarding the protection of human subjects by safeguarding the ethical rights and well-being of the participants; the researcher takes proactive measures to ensure the confidentiality and privacy of their personal information. The Belmont report is used in research and is related to protecting all research subjects or participants (Miracle, 2016). Throughout the research process, the researcher undertakes various responsibilities such as organizing, conducting, and overseeing the data collection stage, emphasizing meticulousness and precision. This role primarily focuses on establishing a collaborative rapport with the individuals involved, initiating meaningful dialogues to comprehend the study's objectives and scope, and securing their voluntary

participation. Cultivating a strong connection and gaining participants' trust is paramount in fostering candid and transparent responses. Additionally, creating a conducive environment that fosters comfort and promotes sharing firsthand experiences and perspectives holds great significance.

Ethical guidelines may influence decisions and behavior when communicated more efficiently (Hassan et al., 2020). Adhering to ethical guidelines, the researcher obtains informed consent from the participants. Participants are assured that their identities will remain confidential, and their responses will be treated with utmost sensitivity. This assurance is vital in encouraging participants to share truthful information without apprehensions regarding potential repercussions openly. They comprehensively explain the research, its objectives, and the potential benefits and risks associated with participation. In qualitative research, the researcher diligently strives to mitigate bias and approach data analysis reflexively. They conscientiously acknowledge and manage personal biases, employ consistent methods for data gathering, integrate diverse sources and perspectives to ensure accuracy, and adhere to a structured process for data examination. This commitment to impartiality and rigorous analysis enhances the reliability and validity of the research findings. In qualitative research involving interviews, an interview protocol establishes a framework and maintains uniformity. 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).

The reason for utilizing an interview protocol is to provide structure to the conversation and ensure that appropriate questions are posed to investigate the

experiences and viewpoints of the participants. The protocol enables thorough investigation while ensuring consistency across interviews, which enhances comprehension of the research subject. A researcher must back up each decision with up-to-date academic or influential sources. By citing appropriate scholarly sources, the researcher establishes a robust theoretical basis, increases the study's trustworthiness, and guarantees that the research is based on pre-existing knowledge. This helps to provide evidence for the validation of research methodologies, data analysis approaches, and interpretations of results while also placing the study within the broader scholarly framework. By meeting these obligations, the researcher intends to create a professional and ethical structure for the data collection process. This approach will guarantee the research's accuracy and consistency and promote a favorable and courteous atmosphere for participants to express their experiences and perspectives. In essence, the researcher's primary responsibility is to carry out the study morally and accountable, with a focus on safeguarding the welfare and entitlements of the participants.

Participants

This study centers on cybersecurity leaders tasked with formulating and implementing cybersecurity policies within eight prominent organizations in the Southeastern United States. Participants in qualitative research should meet the eligibility criteria to ensure that the data collected satisfy the research objectives (Roulston, 2017). The eligibility criteria for study participants encompass holding key positions such as information system security officers (ISSO), cybersecurity managers, or chief information security officers (CISOs) within their respective organizations. These

individuals are selected based on their expertise and practical experience in implementing cybersecurity policies. By utilizing purposive sampling, the researcher ensures that participants possess the requisite knowledge and background crucial for addressing the research inquiries effectively (Campbell et al., 2020; Etikan et al., 2016).

To establish contact with participants, researchers employ diverse strategies such as networking, cultivating professional relationships, and collaborating with organizational leaders and departments (Silvia, 2011). These approaches facilitate access to organizations and the identification and recruitment of potential participants (Gray, 2008). The researcher ensures transparent communication regarding the study's objectives, anticipated outcomes, and mechanisms for maintaining information confidentiality (Silvia, 2011). This creates an enabling environment for participants to openly share their perspectives and personal experiences (Gray, 2008). Ensuring that participants are aligned with the main research question is crucial to guarantee their pertinence to the study. The researcher makes sure that the chosen participants are actively involved in carrying out and enforcing cybersecurity policies, which directly corresponds to the research question. Once I identify potential participants, I will connect individually with each one of the selected participants by sending a brief introduction message about myself and my research study. 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.

All the participants were informed about the research study before the interview process to align with the overarching research question. I will develop a good working relationship with research participants that chose to participate in my research study by being transparent and trustworthy. Formal communication and the right interactions can promote transparency (Bamu et al., 2016). Data will be collected by using open-ended questions during the interview sessions and reviews of the organization's document. Participant-led research can advance health knowledge by challenging and complementing traditional research (Vayena et al., 2016).

Research Method and Design

I used qualitative research as the research method for this research study and used pragmatic inquiry design as the research method design. I will address in detail the reasons below for why quantitative methodologies will not be appropriate method for this research study. I will also address why phenomenological, ethnography, and narrative methodologies will not be appropriate designs for this study.

Method

My intent in this qualitative study is to explore the strategies that cybersecurity leaders use to enforce cybersecurity policies in an organization. The decision to use qualitative research was based on its ability to thoroughly investigate the approaches employed by cybersecurity leaders in implementing cybersecurity policies within organizations. Qualitative research promotes the generation of detailed and rich responses to intricate subjects (Cope, 2014). This study enhances comprehension regarding the

experiences, viewpoints, and actions of the individuals involved in cybersecurity compliance.

This study is particularly suitable for qualitative research because it emphasizes the collection of detailed and descriptive information through interviews. Unlike quantitative methodology, the use of qualitative methods may provide insights into the how and why of a phenomenon (Bush et al., 2019). Quantitative research focuses on collecting, manipulating, analyzing, and quantifying data and this is optional for the study. Quantitative research generally utilizes larger sample sizes and promotes generalize ability across a population, but it fails to gather deeper explanations and experiences (Rahman, 2017). Qualitative data consists of static and dynamic forms of rich data, such as static text within documents and descriptions of rich, dynamic experiences (Bansal et al., 2018). Furthermore, it entails the examination of the contextual elements and the subjective perspectives put forth by the individuals involved.

Research Design

In this study, I chose to use a pragmatic inquiry design. This approach is appropriate for this study because, as part of a pragmatic inquiry, one acknowledges that individuals within social settings (including organizations) experience action and change differently, and this enables them to be flexible in how they conduct investigations on increased security risk due to employee non-compliance of cybersecurity policies. The phenomenological approach offers educational researchers' fundamental empiricism, a flexible structure, and dialogical community support (Sohn et al., 2017). Phenomenological research design is not appropriate because I do not intend to

understand how shared experiences of a culture. Ethnography is not an appropriate research design for this study. According to Hammersley (2018), ethnography may be seen as an inefficient way of producing relevant findings. Lastly, narrative research was considered for conducting this study. Narrative research focuses on the stories presented by the participants about themselves or a particular event (Mohajan, 2018). The stories of participants are not solely constructed by facts, but by the meanings they interpret at the time, which influences the stories they construct (Shamir & Eilam, 2005).

Population and Sampling

A population is a complete set of people with a specialized set of characteristics, and a sample is a subset of the population (Banerjee & Chaudhury, 2010). It refers to the characteristics that determine who can participate in a study, such as the type of sample, how participants are chosen, where they are located, methods for reaching out to them, establishing a rapport, and ensuring that they are relevant to the main research question. The population targeted for investigation comprises cybersecurity leaders tasked with the development and implementation of cybersecurity policies within eight prominent organizations situated in the Southeastern United States. These organizations were specifically chosen based on predetermined criteria, including size, industry relevance, and the availability of cybersecurity leaders possessing the requisite knowledge and practical background essential for effective cybersecurity policy implementation.

This population selection aligns seamlessly with the overarching research question, which primarily centers on the exploration of strategies employed by cybersecurity leaders to enforce cybersecurity policies. Employing purposive sampling,

also referred to as purposeful sampling, is the chosen method for participant selection in this study. This method is substantiated by its capacity to specifically target individuals possessing the desired characteristics and expertise that directly align with the research topic (Creswell & Creswell, 2017). Purposive sampling enables a deliberate and focused participant selection, facilitating the acquisition of rich and in-depth insights from individuals who possess direct experience in implementing cybersecurity policies, such as information system security officers (ISSOs), cybersecurity managers, and chief information security officers (CISOs).

The rationale behind determining the sample size for this qualitative study is based on a power analysis that considers numerous factors including effect size, alpha level, and power level. Sample sizes for qualitative research studies are reached once data saturation hasbeen achieved (Sanders et al., 2017). The researcher applied the principle of data saturation for determining the required sample size. Achieving data saturation is an iterative process performed by the researcher in which the researcher identifies concepts during data collection and acquires additional participants to explore these presented concepts until no current information is produced (Hennink et al., 2016). The study uses a data saturation approach, a defining characteristic of qualitative research, to gauge the breadth and depth of its data collection. When no new themes or insights emerge from subsequent interviews, showing a complete comprehension of the topic under inquiry, data saturation is said to have been attained. In addition, a careful cross-referencing procedure supports response validation. Interview responses are methodically compared to findings from scholarly literature, public resources, and industry papers. This multi-

faceted validation technique ensures that the responses are consistent with wider viewpoints and supports the findings. The study strengthens the correctness and reliability of the data acquired by using data from several sources, which raises the credibility of the research findings. The study achieves a thorough understanding of the research area. It improves the reliability of the findings in the complex environment of cybersecurity awareness and training tactics by integrating data saturation and response validation (M. D. Young et al., 2014).

In the context of the sampling frame, the researcher utilizes a methodical strategy to choose participants from the designated organizations, with a specific emphasis on their respective roles and responsibilities in the execution of cybersecurity policies. The eligibility criteria require that participants (a) being over the age of 18 years old; (b) occupies an organizational hospitality IT leadership position for at least one year such as possess positions such as ISSOs, managers in the field of cybersecurity, or CISOs within their respective organizations; (c) volunteers to share their experiences; and (d) possesses knowledge or perceptions of cybersecurity awareness and training strategies to protect organizational information systems and data. This particular standard guarantees that individuals have the requisite expertise and hands-on expertise to offer meaningful perspectives on the implementation of cybersecurity regulations.

In light of the inherent strengths and weaknesses of purposive sampling, it is imperative to acknowledge that qualitative research places emphasis on comprehending specific contexts and producing comprehensive descriptions, rather than striving for generalizability. (Merriam, 2009). Purposive sampling is beneficial in situations in which

the researcherdoes not intend to generalize across a population (Fletcher & Friedel, 2018). Through purposive sampling, the researcher can access the expertise and knowledge of participants who possess considerable experience in implementing cybersecurity policies, thereby yielding comprehensive and intricate insights.

Interviews should be conducted at a time and location that is convenient for the participant with little to no disruptions (McGrath et al., 2018). The interview should be performed in a manner that promotes the comfort of the interviewee (Rosenthal, 2016). Protecting the respondent's privacy and maintaining the confidentiality of responses is a critical requirement of qualitative research (Fomby & Sastry, 2019). Interviewees locating a private setting to conduct interviews promote more accurate and detailed responses (Fomby & Sastry, 2019). Also, telephone interviews promote more open dialogue (Fomby & Sastry, 2019). I will conduct interviews with participants via face-to-face, video teleconference, or telephone. Conducting interviews over video teleconferencing is an alternative to face-to-face interviews, which promotes open dialogue and allows for the observation of nonverbal cues (Irani, 2018). Video teleconference interviews should also be conducted in a private location with little to no interruptions (Irani, 2018). The mode of the interview was decided upon by the interviewee to promote the comfort, privacy, and protection of the participant. The location of interviews will be conducted in a private location with little to no disruptions to either the researcher (interviewer) or participant (interviewee).

Ethical Research

Ensuring the safeguarding of participants' rights and well-being constitutes a fundamental tenet of ethical research. Within this particular section, an all-encompassing structure is formulated to ensure the protection and well-being of all individuals involved in the study. This framework adheres to a systematic and thorough approach to tackle fundamental ethical considerations.

To begin with, the informed consent process is given prominence, ensuring that participants are provided with comprehensive information regarding the study's objectives, methodologies, potential hazards, and advantages (Nusbaum et al., 2017). The incorporation of the Informed Consent Form promotes transparency and empowers participants to make well-informed choices. By implementing participant withdrawal procedures, the study upholds and safeguards the participants' autonomy, thereby enabling them to cease their engagement in the research without encountering any adverse consequences (Nusbaum et al., 2017). The outlined procedures can be found in the Informed Consent Form, which promotes a sense of intellectual ownership and autonomy.

Secondly, the utilization of incentives, if employed, is examined by the researcher. The purpose of incentives is to acknowledge participants' contributions and encourage their voluntary participation. However, it is crucial to ensure that incentives do not unduly influence participants or compromise the integrity of their involvement. By analytically assessing the role of incentives, the researcher upholds the ethical standards of the study and maintains the intellectual integrity of participants' engagement. Thirdly,

the protection of participants' confidentiality and privacy is addressed. Measures are implemented to anonymize participants' identities and the organizations involved, safeguarding their intellectual property, and ensuring confidentiality. A statement is included to convey the researcher's commitment to securely maintaining the data for five years, providing participants with a sense of intellectual security and trust.

Further ethical considerations focus on the assurance of ethical protection. The research design and procedures undergo thorough ethical review, obtaining approval from the Institutional Review Board (IRB) to ensure compliance with established ethical guidelines. By adhering to these intellectual standards, the researcher guarantees the ethical protection and well-being of participants, preserving the integrity of the study. The researcher emphasized the comprehensive inclusion of agreement documents. These documents enhance their accessibility and ensure their integration into the intellectual framework of the study. By analytically addressing the significance of agreement documents, the researcher demonstrated their commitment to transparency and accountability.

In summary, the Ethical Research subsection demonstrated the academic, analytical, and intellectual dimensions of the step-by-step process employed to protect participants' rights and ensure ethical standards throughout the study. Through the informed consent process, participant withdrawal procedures, examination of incentives, data confidentiality measures, assurance of ethical protection, and inclusion of agreement documents, the researcher upholds the academic integrity, analytical rigor, and intellectual accountability necessary for ethical research conduct.

.

Data Collection

Instruments

The Data Collection Instrumentation exemplifies a methodical approach to gather and analyze data. Careful selection and customization of specific instruments align them with the research objectives. Utilizing a semi-structured interview protocol as the primary data collection instrument facilitates obtaining detailed and comprehensive responses from participants about their experiences and perspectives on cybersecurity policy enforcement. Thoughtfully crafted questions within the protocol capture relevant concepts and dimensions crucial to the research objectives.

To ensure the data collection instrument's reliability and validity, multiple strategies have been employed. Implementing a member-checking process allows participants to review and validate response accuracy, bolstering the credibility of collected data (Motulsky, 2021). A thorough review of interview transcripts guarantees data accuracy and alignment with participants' intended meaning. Maintaining notes of participant responses and observations are critical components of data collection because it promotesthe gathering of rich data (Phillippi & Lauderdale, 2018). Following transcription, notes taken throughout data collection should be incorporated to add nonverbal content (Phillippi & Lauderdale, 2018). In addition, a pilot test will be conducted before the main study to address threats to validity and ensure consistency in data collection. This test involves administering the interview protocol to a select group

resembling the target population. Feedback and insights from participants refine the interview questions and ensure instrument effectiveness.

Emphasizing the use of semi-structured interviews as the primary data collection instrument, this study enables a flexible and nuanced exploration of participants' perspectives. The interview protocol proposed by Rivard et al. (2014) consists of five steps: building rapport, avoid asking leading questions, avoid interrupting the interviewee, allow for pauses between and during questions, and using follow-up questions to satisfy gaps in responses. Utilizing an interview protocol is a strategy that may improve reliability (Wixted et al., 2018). The open-ended nature of interviews encourages in-depth responses, facilitating a comprehensive understanding of the strategies employed by cybersecurity leaders in enforcing policies. In summary, this subsection demonstrated a rigorous and systematic approach to data collection, with the interview protocol as the foundation of the research methodology.

Data Collection Technique

The chosen approach for data collection in this dissertation is solely centered around semi-structured interviews that provide a flexible and dynamic approach for gathering data about the execution of cybersecurity policies. Moreover, they facilitate a comprehensive exploration of participants' viewpoints, thereby enabling the researcher to amass intricate and nuanced data.

Upon acquiring the requisite authorization from the Institutional Review Board (IRB), a preliminary investigation will be conducted to enhance the interview protocol and validate its effectiveness. The initial inquiry entails engaging in interviews with a

select cohort of individuals who exhibit resemblances to the primary group under scrutiny. The feedback obtained from the participants in the pilot study will undergo a comprehensive analysis to ascertain any necessary modifications or improvements to the interview questions and prompts.

To improve the trustworthiness and accuracy of the data collection process, we will use member checking (Motulsky, 2021). Member checking is a process where the analyzed interview transcripts are shared with the participants. This is done to make sure that the accuracy and interpretation of their responses are correct. This repetitive process guarantees that the viewpoints of the participants are faithfully portrayed and offers them a chance to validate or contribute further understandings. The interview questions and prompts will be included in the appendices for easy access and consultation. This enables readers to acquire a thorough comprehension of the process of gathering data and offers clarity in the methodology employed for research.

A thorough member verification procedure is incorporated into the approach in an effort to increase the rigor and reliability of the research. This entails working together with participants to review and validate the conclusions drawn from the interviews. Member checking promotes ownership and cocreation of information by allowing participants to consider the interpretations' precision and thoroughness (Y. Wang et al., 2021). It also creates a mutually beneficial relationship between the researcher and participants, strengthening the validity of the research findings. It resolves any potential misunderstandings or differences that can happen as a result of subtleties in communication or viewpoint. Through member checking, the study improves the results'

reliability and represents participants' experiences more accurately. The study's credibility in the field of cybersecurity awareness and training tactics is further enhanced by the practice's alignment with the values of openness, cooperation, and accountability (Y. Wang et al., 2021).

To summarize, the method used to gather data for this research study involves conducting semi-structured interviews. These interviews provide a thorough examination and comprehension of the experiences and viewpoints of cybersecurity leaders regarding the implementation of cybersecurity policies. The preliminary investigation and feedback from participants help strengthen the accuracy and reliability of gathering information. Including interview questions and prompts in the appendices allows for transparency and ease of understanding for readers.

Data Organization Techniques

The focus of this particular section within the research study pertains to the methodologies and procedures utilized to effectively manage and safeguard the acquired data. We will employ a diverse range of methodologies to ensure meticulous organization, robust security, and enduring preservation of the data. To guarantee the methodical recording of data and the cultivation of fresh perspectives, we shall uphold the practice of maintaining research logs and reflective journals. These instruments will serve as comprehensive documentation of the research endeavor, encompassing details regarding data acquisition, observations, reflections, and musings. The utilization of these records and diaries will facilitate the ongoing scrutiny and comprehension of the data.

Safeguarding the integrity of data constitutes a fundamental aspect of this research endeavor. Measures will be taken to guarantee confidentiality and safeguard the privacy of the individuals concerned. The entirety of the provided information shall be securely stored, with exclusive access granted solely to individuals possessing authorized permission. To safeguard the data from unauthorized access or breaches, we shall implement robust security measures such as access controls and encryption. The data will be retained for five years in adherence to ethical guidelines. This temporal window allows for the potentiality of conducting additional scrutiny, validation, and deliberation. Upon the completion of the designated period, the data shall be disposed of in a manner that upholds confidentiality and ensures the protection of the privacy of the individuals concerned. The meticulous process of data disposal will be comprehensively elucidated and meticulously documented, in strict adherence to both legal and ethical principles.

Data Analysis Technique

As the researcher, the focal point of data analysis in this study will be solely directed towards qualitative analysis methodologies. The objective is to amass significant data and discern recurring patterns from the data we have amassed. The researcher will subsequently employ this data to address our research inquiries and accomplish our goals. The assessment will be conducted utilizing a thematic analysis approach, enabling a systematic exploration and identification of noteworthy themes and patterns within the data. In commencing the analysis, the researcher will diligently transcribe the recorded interviews verbatim, ensuring the precise capture of participants' responses. The data will be transferred to the NVivo software, which will serve as a valuable tool for organizing,

classifying, and analyzing the qualitative data. NVivo enables efficient management of substantial volumes of data and facilitates the identification and categorization of emerging patterns.

The process of coding will require a thorough examination of the transcriptions, where we will identify common ideas, concepts, or patterns, and assign appropriate codes to represent them (Swain, 2018). The codes will be improved and modified repeatedly to accurately represent the subtleties and complexity of the data. As the process of coding advances, recurring patterns will become apparent, and relationships between various codes will be investigated. These themes will be carefully examined and improved to make sure they truly reflect the viewpoints and experiences of the participants (Swain, 2018).

During the analysis, the researcher will consistently compare and write down our thoughts to better comprehend the data and generate theoretical ideas. Memos are useful for researchers to reflect on their thoughts, interpretations, and possible connections between themes and the existing literature. The way we present, understand, and clarify the data will align with the research questions and the underlying theory. The results will be presented by including appropriate quotes and examples from the data. This will help explain and enhance the understanding of the phenomenon being studied. The researcher will carefully and openly follow established guidelines for qualitative research to ensure a thorough and transparent data analysis process. The ultimate examination will be extensively recorded, guaranteeing the ability to trace and rely on discoveries.

To summarize, as the researcher, the researcher will use a method called thematic analysis with the help of NVivo software to examine the qualitative data. The process will entail writing computer instructions, recognizing patterns, and making sense of the information to answer the research inquiries. By undertaking this process, my objective is to acquire a profound comprehension of the viewpoints of the participants and offer valuable observations regarding the research subject.

Reliability and Validity

Reliability

The reliability of this study is of utmost importance, as it guarantees the uniformity and steadfastness of the results. Firstly, the trustworthiness of the study itself pertains to the reliability and consistency of the research methods and procedures. To improve dependability, we will adhere to thorough procedures for gathering data, which involve using consistent methods for conducting interviews and carefully recording every step of the research. By ensuring that data collection and analysis are consistently carried out, the study's reliability is enhanced. Regarding the tools employed, the reliability of the semi-structured interview protocol will be determined by various assessments. Multiple researchers will independently analyze a subset of the interviews to ensure inter-rater reliability and compare their findings. This procedure will allow for the detection of any inconsistencies and improve the reliability of the analysis. Furthermore, we will implement a methodical approach to coding and theme development to maintain the uniformity of interpretations throughout the data.

Validity

This study will examine both internal and external validity. Internal validity is concerned with how accurately a study captures the relationship between the variables being investigated. To improve the accuracy of our findings, we will take measures to reduce any possible biases. This includes being aware of our perspectives as researchers and regularly discussing the analysis of data within our team. These actions will encourage a precise and impartial understanding of the information.

External validity refers to how applicable the findings of a study are to different situations or groups of people. Because the research is qualitative, the goal is not to attain statistical generalizability but rather to achieve theoretical generalizability. The study aims to make sure that the findings can be applied to similar situations by giving thorough explanations and specific details. This will help readers determine how relevant the findings are in other settings. To strengthen the validity of the study, the researcher will use member checking. Participants will be able to examine and confirm the explanations and discoveries, thus guaranteeing that their own experiences match up with the researcher's explanations. This procedure promotes a feeling of trust and cooperation between the researcher and participants, enhancing the accuracy of the study.

In essence, this study places significant importance on the dependability and accuracy of its findings. The study will be made reliable by using consistent procedures, and the instruments will be tested for reliability by comparing ratings from different people. Improving the study's accuracy will be achieved by reducing biases, and ensuring the reliability of the findings will be done by providing detailed explanations and seeking

confirmation from participants. By adhering to these principles, the study seeks to generate reliable and believable findings that add value to the domain of cybersecurity policy implementation.

Conformity and Credibility

The study uses a dual-pronged strategy to ensure compliance and increase credibility. The foundation of compliance is primarily a consistent dedication to meticulous research methods that are in line with the tenets of the selected Social Cognitive Theory (SCT). Internal consistency is promoted by this uncompromising adherence, which guarantees that the study stays loyal to its intended topic and theoretical framework. Second, triangulation, which combines data from various sources to validate conclusions, strengthens credibility. This compilation includes observations from interviews, business records, open sources, and academic literature (Y. Wang et al., 2021).

The study attempts to create a coherent narrative by cross-referencing many sources including the use of 13 IT industry publications (National Institute of Standards and Technology (NIST) 800-12 Revision 1/An Introduction to Information Technology, 800-30 revision 1/Guide for Conducting Risk Assessments, 800-53 Revision 4/ Security and Privacy Controls for Federal Information Systems and Organizations, 800-207/Zero Trust, 800-50/Building an Information Technology Security Awareness and Training Program, 800-92/Guide to Computer Security log Management, MITRE, ISO/IEC 27001, HITRUST, Federal Information Security Modernization Act (FISMA), Control Objectives for Information and Related Technologies (COBIT), System and Organization

Controls (SOC), and CIS Critical Security Controls (CIS Controls). These will help in confirming the research findings' validity and accuracy. The study's foundation within SCT is validated by this combination of conformance and credibility, which also serves as a quality control mechanism, guaranteeing that the conclusions are based on an extensive examination of cybersecurity awareness and training methodologies (Y. Wang et al., 2021).

Transition and Summary

In this section of the study, I presented a detailed explanation of the research methodology chosen for this doctoral study. The section outlines the researcher's role, analysis of the participants,analysis of the various research methods and design approaches, the types selected for this study, population sampling, ethical research, data collection, organization techniques, data analysis reliability, validity, conformity, and credibility. Section 3 will highlight an overview of the study, the study’s outcome, its application to the profession, social change implications, actionrecommendations, future research recommendations, reflections, and conclusion. Section 3 outlines the presentation of the findings, applications to professional practice, analysis of the participants, recommendations for actions, recommendations for further study, reflection, and summary and study conclusions.

Section 3: Application to Professional Practice and Implications for Change

Overview of Study

The purpose of this qualitative, pragmatic inquiry study is to explore the strategies that cybersecurity leaders use to enforce cybersecurity policies in an organization to protect organizational information systems and data.

Presentation of the Findings

The research question I wanted to ask at the beginning of this study was: What strategies do cybersecurity leaders use to enforce cybersecurity policies to protect information systems and data? In order to get the answer to my question, I conducted semistructured interviews with a total of five participants. After conducting the semistructured interviews and reviewing fourtheen public accessible documents (Table 1), I then transcribed the interview recordings to text and sanitized the files to remove irrelevant interview discussions. The participant's names have been encrypted to mask their identities and they will be identified as Participant A, B, C, D, and E. NVivo was used for analysis and four themes were observed. The themes are (a) user awareness and training, (b) stakeholder buy in (management support), (c) baseline/risk assessment testing, and (d) staying abreast with current trends/technologies/standards. Once I found the themes, I begin searching publicly accessible documents (see Table 1) on the these themes and found the correlation which aided in the support of all four themes that surfaced from the interviews. In the following section, the four major themes that emerged during the data analysis phase are evaluated against the review of the literature,

publicly accessible documentation (see Table 1), and finally, examined through the lens of Albert Bandura's SCT, which served as the conceptual framework for this study.

Table 1

List of Documents Examined

Publicly Accessible Documents
NIST 800-12 Revision 1/An Introduction to Information Technology
NIST 800-30 revision 1/Guide for Conducting Risk Assessments
NIST 800-53 Revision 4/ Security and Privacy Controls for Federal Information Systems and Organizations
NIST 800-207/Zero Trust
NIST 800-50/Building an Information Technology Security Awareness and Training Program
NIST 800-92/Guide to Computer Security log Management
MITRE
ISO/IEC 27001
ISO/IEC 27002
HITRUST
Federal Information Security Modernization Act (FISMA)
Control Objectives for Information and Related Technologies (COBIT)
System and Organization Controls (SOC)
CIS Critical Security Controls (CIS Controls)

Theme 1: User Awareness and Training

The first theme that emerged was user awareness and training. Providing user awareness and training on the best cybersecurity best practices is crucial for enforcing cybersecurity policies and reducing human-related risks. This is because humans are

commonly cited as the biggest cybersecurity vulnerability. As noted by Mittal (2015), humans are globally recognized as the weakest link in cybersecurity and the biggest contributors to the vulnerability of businesses worldwide. For instance, employees can either deliberately or inadvertently jeopardize an organization's cybersecurity through weak passwords and clicking on malicious links. Other common attack vectors attackers can exploit to launch attacks on employees include social engineering or phishing, DDoS attacks, insider threats, ransomware, and accidental loss of hardware.

Table 2

Frequency of First Major Theme

	Participants		Documents	
Major theme references	Count	References	Count	References
User awareness and training	5	30	14	81

The participants described their methods, difficulties, and what approaches work. It was stressed that one of the best strategies was to have clear policy communication. The participants stressed the need for improved communication through simple but effective policies. It included training sessions, practical workshops, and media for regular policy updates. Participant A suggested: "Our mission is clear and consistent communication; yearly training sessions to provide updates on our cybersecurity policies are also a cornerstone of this approach." Assessing their threats and opportunities was also one of their methods. Cybersecurity representatives noted that the outlined policies should be generic and tailored to tackle the specific risks and needs of the organization. This consideration made the policies successful because the staff welcomed them.

Participant B said, "Analyzing only the routine risk assessment allows us to discover which locations we are the weakest. It also helps us change our policies to fit each site better. As a result, compliance there has greatly improved". One thing that they mentioned is that workers prefer to avoid using change to fix things. This called for specific communication, proper training, and, above all, the participation of organizational management. The employer's refusal is what makes this employee the most problematic. Just one prompt and training are enough to eradicate it.

By training employees on cybersecurity best practices, cybersecurity leaders can help this group comprehend the threats and risks associated with cyber-attacks by equipping them with the requisite knowledge and skills. This can significantly reduce the odds of suffering successful attacks. For instance, creating awareness of phishing attacks and training employees to identify phishing scams can prevent them from falling victim to such scams and avert possible information leaks (Jampen et al. (2020). Besides, cybersecurity leaders train their employees on best practices such as creating strong passwords that cannot be cracked easily and using secured mobile devices.

SCT framework results revealed that personal (attitudes, beliefs, perceived self-efficacy), behavioral (attitude, behavior, social support), and environmental factors (policy, support, regulations) were interacting in creating user awareness and training. The model stresses the dynamics related to the knowledge, attitudes, and efficacy of an individual, how the culture of an organization, and managers' support is also equally important. Clear employer communication and individualized training increase employees' efficacy in adhering to cybersecurity policy stipulations. Secondly, outcome

expectations, including confidence boosts and credits to employees, also contribute to enforcing adherence to policy. Self-regulation techniques include habitual approaches such as risk assessment and policy adaptation, allowing employees to check and control their conduct while simultaneously pursuing organizational targets.

Theme 2: Stakeholders Buy-In (Management Support)

Cybersecurity leaders bank on stakeholder buy-in, particularly management support, to enforce cybersecurity policies and protect information systems and data. Essentially, whenever the top-level executives in an organization prioritize cybersecurity and lead by example in its enforcement, the move underpins the significance of adhering to cybersecurity best practices and the firm's policies and procedures. As mentioned above, human error is responsible for the majority of electronic data breaches, with a 2014 IBM study reporting that 95% of all information security breaches result from human error (Amoresano & Yankson, 2023). Maintaining a resilient cybersecurity culture in an organization is thus vital to minimize the risks and threats posed by cybersecurity. That can only be realized with solid support and commitment from top-level executives and an organization's leadership.

Table 3

Frequency of Second Major Theme

	Participants		Documents	
Major theme references	Count	References	Count	References
Stakeholders Buy-In (Management Support)	5	19	14	50

Management support helps cybersecurity leaders spread the message to all other stakeholders regarding the importance of cybersecurity, the potential threats from cyber-attacks, and the risks of non-compliance. In an organization, every stakeholder, especially employees, should commit to keeping the organization safe from cyber-attacks. As noted by Reegård et al. (2019), given the constant evolution of cyber threats and the use of new technologies, maintaining an enterprise's cybersecurity is no longer the role of the IT department alone. Instead, the input of other stakeholders, such as the top-level executives and employees, is warranted. As such, with the buy-in of an executive team committed to spreading the importance of cybersecurity through regular security awareness and campaigns, cybersecurity leaders can foster a security-conscious culture, ultimately realizing the objective of keeping the organization safe from cyberattacks and security breaches. Besides, the management should be committed to allocating the appropriate resources, such as budget and staffing, to cybersecurity leaders to bolster the organization's cybersecurity posture.

The need for additional funds and human resource specialists was also challenging. The identified resource constraints prevented the policy from being implemented. Participants agreed there should be a boost in cybersecurity spending. Participant D stated that "limited budget and unskilled staff create hurdles in effective policymaking." Resource allocation is the key to this solution. Participant E said, "Cybersecurity laws cannot be properly enforced without the participation of the leaders and hence they are crucial." On the other hand, different individuals have varied views on what is more critical: external threats, organizational culture, and leadership support.

Participant F reported that “leadership support is important, but culture is the most crucial factor. Policies are ineffective if the organization doesn’t support cyber security”.

The results of the buy-in by stakeholders based on the Social Cognitive Theory Framework indicate that personal factors, environmental factors, and the behavioral aspect of an individual inter-relate together. The effectiveness of policy enforcement was observed to be dependent on the support of leadership and the environment (e.g., organizational culture). Leader's self-efficacy in policy enforcement, which, when paired with clearness of communication and allocation of resources, creates stakeholders' buy-in. In addition to this, outcome anticipations, including the likelihood of successful security outcomes and breaches, impact leadership's degree of policy enforcement. Leaders can reduce cybersecurity risk by employing self-regulation tools like prioritizing resources and emphasizing direct communication, enabling their behavior to comply with cybersecurity policies and match the organizational objectives.

Theme 3: Baseline/Risk Assessment Testing

Cybersecurity leaders also conduct baseline risk assessments and audits to bolster the overall cyber defense posture of their organizations. A baseline risk assessment is an evaluation performed on an organization’s cybersecurity posture to understand the cyber risks that may affect its operations (CISA.gov, 2021). The process may involve conducting vulnerability scans on the organization’s systems and interviewing key stakeholders to identify potential risks and vulnerabilities to the critical organizational data and systems. Essentially, before an organization attempts to improve its security posture, it is necessary to comprehend the threats and vulnerabilities such as cyber-

attacks, industry-specific risks, and operational risks imperiling its processes and procedures. Thus, a cybersecurity risk assessment is used to identify these threats and vulnerabilities. The risk assessment typically encompasses aspects like an organization's software applications, network infrastructure, and security procedures and policies.

The National Institute of Standards and Technology (NIST) maintains that risk assessments are integral to company-wide risk management efforts. According to the NIST Special Publication 800-30, organizations should conduct an ongoing risk assessment to inform their long-term cybersecurity strategy (Blank & Gallagher, 2012). Risk assessments inform an organization's decision-making across the risk management hierarchy, including advising the process of developing an information security architecture, designing security solutions for information systems, and modifying business processes, functions, and missions. Essentially, the information collected from the risk assessment process is used to guide an enterprise's day-to-day fixing of vulnerabilities and the cybersecurity strategy in the long run.

In addition to cybersecurity risk assessment, cybersecurity leaders bank on cybersecurity audits to ensure they meet specific compliance requirements and pertinent data protection standards. Essentially, cybersecurity leaders should evaluate the level to which their organizations comply with specific external regulations and standards. The process involves conducting a detailed review of the organization's policies and procedures to ensure compliance with the relevant regulatory requirements. Through cybersecurity audits, cybersecurity leaders can also ensure compliance with the organization's overall cybersecurity policies, internal controls, and risk management

processes (Slapničar et al., 2022). In addition, an internal control system or control framework should be in place to ensure an organization is compliant with the applicable regulations. One commonly used framework for IT governance is the Control Objectives for Information and related Technology (COBIT). The framework's recent version, COBIT 2019, helps cybersecurity managers enhance their organization's security posture and ensure that their cybersecurity measures align with the organization's objectives and compliance regulations (Sulistyowati et al., 2020). It realizes these by helping them to implement the appropriate controls and processes.

Table 4

Frequency of Third Major Theme

	Participants		Documents	
Major theme references	Count	References	Count	References
Baseline/Risk Assessment Testing	5	67	14	25

The study results illustrate various angles, difficulties, and leadership roles in the organization's cybercrime policy creation and control. The policy succeeded due to the establishment of effective communication and policy adaptation to meet the organization's requirements and with leadership support. Despite employee resistance and resource limitations, embraceable policy enforcement through proper planning and resolution from the top management is still possible. The work focused on the research will become the basis of policies related to cybersecurity in organizations and the protection of their data.

The SCT Frameworks highlighted the bidirectional relationship between personal behaviors and environmental factors in the baseline/risk assessment testing. Employee self-efficacy, determined by the degree of risk awareness and organizational support, is mostly expressed in policy compliance. Besides, expectation outcomes, including against cyber-attacks and possible recognition, motivate workers to align with cybersecurity policies. Self-regulation strategies are the key components of risk assessment and policy adaptation, which allow employees to keep track of and gauge their emotions in a way aligned with the organization's objectives.

Theme 4: Staying Abreast with Current Trends/Technologies/Standards

Cybersecurity leaders also protect an organization's information systems and data by keeping abreast of current trends, technologies, and standards. Essentially, the cybersecurity landscape is always changing. This has led to the emergence of new threats, vulnerabilities, and attack vectors. As a result of the increase in cybersecurity threats over the years and the recent evolution in the threat landscape, the efficacy of conventional protection systems, such as firewalls, in detecting sophisticated attacks has been severely jeopardized (Mallick & Nath, 2024). Therefore, cybersecurity leaders must stay up to date with the current trends and developments in cybersecurity. That ensures that these professionals can effectively anticipate and prepare for potential threats and thus implement proactive risk mitigation measures.

In addition, it is essential to note that cybersecurity technologies are rapidly advancing. Recently, the world has seen the increased use of technologies such as machine learning and artificial intelligence to counter cyber-attacks (Zeadally et al.,

2020). While these are effective cybersecurity solutions, a cybersecurity leader without an eye for the latest technologies would not effectively take advantage of the opportunities they present in cybersecurity. As such, this underscores the importance of staying abreast of the latest technologies in order to integrate them into security infrastructures and enhance the capability of information systems protection.

The study results illustrate various angles, difficulties, and leadership roles in the organization's cybercrime policy creation and control. The policy succeeded due to the establishment of effective communication and policy adaptation to meet the organization's requirements and with leadership support. Despite employee resistance and resource limitations, embraceable policy enforcement through proper planning and resolution from top management is still possible. The work focused on the research will become the basis of policies related to cybersecurity in organizations and the protection of their data.

Table 5

Frequency of Fourth Major Theme

	Participants		Documents	
Major theme references	Count	References	Count	References
Staying Abreast with Current Trends/Technologies/Standards	5	32	14	35

The results on the subject of "staying Abreast with the trends and technologies" aligned with the SCT Framework that dynamically specified the interaction of these three factors (i.e., personal, behavioral, and environmental). Employees' self-efficacy,

enhanced by practices such as knowledge acquisition and leadership support, creates an appetite for following technology standards policies. In addition to that, the expected results for instance strong security and the appraisals that come with it, computerize employees thereby keeping them up to date with the current trends. Through implementing self-regulated strategies like constant learning and technology adoption, workers can be brainwashed to reflect cybersecurity rules and organizational aims.

Applications to Professional Practice

Indeed, the findings of this project will be of great significance to IT professionals in terms of cybersecurity policy implementation. This particular segment further highlights the application of the findings to the betterment of IT practices. There is evidence from the study that effective policy communication is the key to successful professional practice. Cybersecurity managers need to develop unambiguous policies and develop good organizational communication. Continuous training and workshops and creating policy changes in various aspects have been very successful approaches. Organizations must replicate this model by guaranteeing that employees know and know the current cybersecurity policies. With a careful policy communication strategy, an organization is more likely to strengthen its cyber defenses against avoidable breaches occasioned by human error or ignorance (Yusif & Hafeez-Baig, 2021).

Cybersecurity leaders can leverage various strategies to enforce cybersecurity policies and protect information systems and data. As discussed above, these strategies include leveraging stakeholder buy-in, particularly the top management to spread the message on the importance of protecting information systems and data. Cybersecurity

leaders can also rely on baseline risk assessment testing to improve an organization's cybersecurity landscape. They can leverage risk assessment to understand threats and vulnerabilities such as cyber-attacks. Besides, providing user awareness and training on cybersecurity best practices can significantly reduce human-related cybersecurity risks.

In addition, the findings shed light on the need for a policy that only addresses the issues and threats of the organization. Developing cybersecurity policies should be driven by each organization's specific needs and goals (Uchendu et al., 2021). Risk assessment should be done periodically, and policies should be modified to suit the findings. In professional practice, companies should devote resources to unmask their weaknesses and find the most efficient ways to mitigate the risks. Through this personalized approach, the policies become realistic to the employees, making them compliant and reducing the number of security incidents. First, implementing cyber security policy provides a platform where I could work as a professional. We still have to deal with staff resistance to policy modifications in several organizations.

One of the tactics for managing this unwillingness is investing in communication, training, and engagement of organizational leadership. Resistance and policy compliance can be minimized if this approach is followed. This can be realized by enlisting the employees actively, rectifying their issues, and providing comprehensive training. Likewise, the limited resources, such as funding and competent staff, undermine the efficiency of the policy processes. Organizations must lobby for more money for cybersecurity to solve this problem. This could mean extending the budget and recruiting qualified staff responsible for implementing these policies.

The vital factor of policy enforcement turned out to be leadership support. Leadership engagement and resource allocation were crucial elements in making policies work. Organizations should treat cybersecurity as a professional responsibility, and top management should actively participate in cybersecurity efforts. Companies build a security culture through managerial support, where cybersecurity policies and practices are prioritized everywhere. In addition, empowering leadership is essential for getting the necessary resources to implement and enforce cybersecurity policies (Tagarev, 2020). Most participants pointed out that leadership support played the most crucial role, and a few others specified that the organizational culture and external threats were the factors to be considered. These would include leadership support, organizational culture, and external forces. Organizations can develop a better cyber security policy enforcement strategy by combining these factors with a comprehensive plan.

The study's findings have different impacts on IT professionals in terms of their practice. Through effective policy communication and policy adaptation to meet organization requirements, and with the support of leaders, the policy was a success. Companies could improve their cybersecurity posture and address such risks by addressing staff resistance and limited resources. The results of the presented study will be helpful for the organizational enhancement of security and data protection, which will benefit the broader IT community. This study has brought valuable lessons that can be used to develop and update cybersecurity standards and a safer and more secure digital world.

Implications for Social Change

Social change implications are presented through the betterment of individuals, groups, organizations, institutions, cultures, and communities. The findings of this research has carried enormous power in generating favorable social change in the process of cybersecurity policy application. This knowledge can be applied by individuals, communities, organizations, institutions, cultures, and society to support cybersecurity measures and avoid data loss due to cyber-attacks.

The research, on an individual basis, praises education and awareness of citizens' cybersecurity. With the growth of cybercrimes, people must be equipped with knowledge and skills to protect themselves and their companies (Rajasekharaiah et al., 2020). With the help of comprehensive and advanced cybersecurity training, companies can make their staff members proficient enough to recognize, protect, and handle cybersecurity threats. Besides, it not only protects the company but also individual data; therefore, it leads to a safer environment for all.

Local community cybersecurity report recommendations point to the collaborative work and joint responsibility of cybersecurity at the community level. Organizations, industry experts, and governments should cooperate in overcoming the cyber threat landscape, as this area has its specificity by its very nature (Pomerleau et al., 2020). By sharing know-how, resources, and information, communities may become more assiduous in cybersecurity and better protect themselves from cyber-attacks. This cooperative way of thinking helps create unity and strengthen a community's resilience to cyber threats, enabling it to withstand them.

It demonstrates the necessity of a proper cybersecurity culture at the organizational level. Organizations must pay more attention to the issue of cybersecurity and integrate it into their business values and everyday processes. Through developing a cybersecurity culture, companies can make cybersecurity policies to be implemented and followed by everyone within the organization. These proactive steps reduce the chance of data breaches and protect the company's image and financial status (Rajasekharaiah et al., 2020).

According to the research, institutional bodies share the need for policy development and resource allocation. Institutions ought to do the risk assessment and update their cybersecurity policies regularly. Efficient financial and technical resources can help institutions execute cybersecurity policies appropriately (Rajasekharaiah et al., 2020). Hence, when institutions do so, cybersecurity risks will be lessened. The audience is assured of privacy, stability of the institution, and integrity.

The study asserts that at the cultural level, a change of attitude and behaviors toward security is necessary. Cybersecurity culture based on security enlightens society about the importance of cybersecurity and encourages people to be proactive in cybersecurity protection (Marotta & Madnick, 2021). This cultural shift helps people stay vigilant against cyber threats, translating into a safe and secure digital environment for everyone. In a social context, the research results provide a ground for cybersecurity regulations and practices. The study will provide suggestions to help communities develop a good cybersecurity environment and prevent data leaks. This valuable information underlines macroeconomic stability, national defense, and international

cooperation. The collaboration of societies in the fight to overcome cyber threats creates a safe and secure digital future.

The social impacts of the study are immense and wide-ranging. Those insights could be of great value to individuals, communities, organizations, institutions, cultures, and societies in preventing cyber-attacks and data breaches, which could be achieved by building strong cybersecurity postures. This will bring about a safer and more secure digital environment that will, in the end, benefit the community as a whole.

Recommendations for Action

The recommendations would be based on the previous logical statement, which has steps that lead to beneficial actions. Moreover, the outlines should also indicate how the results will be disclosed. Given these results, organizations' cybersecurity training programs should be enhanced. This training has to be technical and tackles policies and their enforcement. The discipline should be taught to all company employees periodically to prevent cybersecurity attacks. Comprehensive cybersecurity training programs that address policy enforcement and will be compulsory for all employees will be developed and rolled out. The organization will, however, constantly be trained on cybersecurity to keep everyone knowledgeable and up to speed.

Organizations must strive for a security culture where cybersecurity should be seen as a value instead of another responsibility. This means that cybersecurity regulations are in place and adhered to by all the organizational units. A security culture should be developed as cybersecurity is the primary value. Ensuring cybersecurity is in the mission statement and the institution's core values are essential. In addition, the

employees should be reminded about the importance of security via awareness campaigns. Organizations and institutions must regularly update and adjust their cybersecurity policies by considering new cyber threats. Frequent audits should be held to identify the gaps, and the policy should be updated based on the audit results and the most recent cyber threats. This involves introducing cybersecurity policies to all staff members. Viewing cybersecurity as a value rather than just a responsibility encourages all organizational units to comply with cybersecurity regulations (Onumo et al., 2021). The involvement of organizations, experts, and government agencies is essential to cope with dynamic cyber threats. Collaboration between organizations with field expertise and governmental entities should be promoted. Platforms and forums should be formed to distribute resources, best practices, and information. Public-private partnerships should be formed to intensify cybersecurity efforts (Reeder & Barnsby, 2020). Organizations should be ready to invest in technologies such as artificial intelligence (AI) and machine learning (ML) to improve their cybersecurity capacity. Encouraging investments into AI and ML cybersecurity technologies, implementing threat intelligence solutions capable of proactively detecting and responding to cyber threats, and providing IT infrastructure that can withstand emerging cyber risks are some of the proactive measures that should be taken.

Recommendations for Further Study

Impact of Cybersecurity Training on Employee Behavior

Another natural step is to evaluate the long-term effect of cybersecurity training on company staff behavior. Through knowledge and comprehension of the training's

impact on employee behavior over the long term, administrators of the security training programs might get an insight into the effectiveness of the training programs that improve cybersecurity skills (Kosutic & Pigni, 2022). Appraisal of the change in behavior post-cybersecurity training will provide an overall view of the maturation of culture in cybersecurity.

Evaluation of Emerging Cyber Threats

Future research should develop programs identifying emerging cyber threats and their effects on cyber policy frameworks. Identifying and analyzing emerging threats will enable organizations to develop and change cybersecurity policies in the future to deal with new problems more effectively (Hussain et al., 2020). A possible path for research can be to look at a few of the recent incidents of cybercrimes and guide organizations on how to make changes in their policies to cover those situations in the future.

Cross-Industry Comparative Analysis

A comparative analysis of a sector may help one identify policy enforcement practices, determine best practices, and make recommendations for cybersecurity for each industry (Atkins & Lawson, 2021). Collaboration among the industries enables practical training in regard to the most successful strategies and methods. It would be the best practice in research in the policy enforcement area in other sectors to apply cybersecurity for each industry.

Exploration of the Role of AI and ML in Cybersecurity

When developing cybersecurity policies, the role of enforcement in AI and ML should be considered. The investigations made in strengthening the policies will be

concluded by using AI and ML technology for existing cybersecurity infrastructure. The recognition of potential help from the said technology that will enhance the detection and remediation of cyber threats will offer organizations valuable tools for improving their cybersecurity procedures (Zeadally et al., 2020).

Longitudinal Study on Policy Effectiveness

As recommended by Sobb et al. (2020), conducting a long-term study to ascertain the effectiveness of the same on actual cybersecurity incidences would be long overdue. This would help an organization identify trends, difficulties, and likely areas for policy improvement by charting the development and impact of cybersecurity policy over time. These will possibly include regular assessments of policy effectiveness, which empower the policymaker to understand the data and make the right decisions to fine-tune cybersecurity functions from time to time.

Cultural Influences on Policy Compliance

Future research should be directed to the cultural aspects of compliance with organizational policies in cybersecurity. Research into cultural factors and how they lead to employees' compliance with cybersecurity policies is bound to give deep insights into implementing better policies. The organization best knows the kind of organization culture in policy compliance; therefore, it's best placed to develop a tailor-made approach to training and awareness in cybersecurity.

Evaluation of Policy Enforcement Technologies

Policy enforcement technology options must be assessed, and the best ones for the organizations must be chosen. Research can be done by studying and comparing different

types of technologies, including data-loss prevention (DLP) systems and endpoint security solutions. It will be helpful for organizations to be aware of the advantages and disadvantages of these technologies so that policies and tools suitable for implementing cybersecurity measures can be chosen.

Impact of Regulatory Frameworks on Policy Compliance

An extra investigation is needed to assess the impact of regulatory frameworks on compliance with cybersecurity policies. Examining the regulatory extent to which companies adopt policies can give insights regarding the methods of compliance (Abrahams et al., 2024). Research can be performed as a comparative review of companies operating under various regimes to pinpoint common problematic areas and best industry practices.

Reflections

Going through this DIT process has really been a lifechanging event for me. School has always came “easy” but this process has taught me such a great life lesson. Patience, diligence, and consistency are things that I need more of in my life. At one point, I told myself it just wasn’t meant to be because I didn’t finish 5 months ago. I had to continue to persevere despite all of the disappointments in the program as well as in my personal life. I am so proud to say that I am typing this reflection with a smile on my face because I saw this out to the very end. I have learned so much about myself. I have always heard that I was a strong and resilient person but getting to witness myself be the person everyone thinks I am made this experience one of the best things yet. As a first-

generation college student, I got to rewrite history for my family and pave a new way for my kids.

Policy has always been the end goal for me so that helped me to continue on with the research. This study opened my eyes to cybersecurity policy enforcement's technical and human aspects. Gradually, the process of self-examination allowed me to discover my prejudices, how they impact participants, and how I changed my perception. The main factor for the legitimacy of the research was to acknowledge personal prejudice and preconceived ideas. Among my goals is to acquire a more in-depth knowledge of cybersecurity enforcement policies and procedures through a keen curiosity. Eventually, I came to understand that there might be some discrimination, especially for a person with a computer science background. I was still critical of my presumptions. This awareness about self was what made the study credible and impart. Researching cybersecurity policies has changed my attitude toward cybersecurity policy compliance. After conversing with cybersecurity experts, I extended my understanding of security challenges and complexity as they spoke about their experiences and offered their opinions.

Summary and Study Conclusions

Protecting information and information systems from unwarranted access, use, disclosure, alteration, and destruction remains essential, given the ever-evolving cyber threat landscape. Information protection is vital to ensure data integrity, confidentiality, and availability. Cybersecurity leaders employ various strategies to enforce cybersecurity policies to protect information systems and data. Some common strategies cybersecurity

leaders employ include user awareness and training, stakeholder buy-in, risk assessment testing, and staying abreast with the current trends, technologies, and standards. Employees' compliance with organizational cybersecurity policies is positively influenced by effective strategies used by cybersecurity leaders that enhance self-efficacy beliefs, provide positive outcome expectations, facilitate self-regulation through training and awareness, and model desired cybersecurity behaviors. The results provide invaluable data for cybersecurity specialists, policymakers, and companies. By understanding the stories and viewpoints of cybersecurity leaders, companies can implement policy more efficiently. The consequences of social change illustrate opportunities to empower people, communities, organizations, institutions, cultures, or societies. This can be done by formulating an action plan based on the findings, which will help organizations increase their cybersecurity practices, thus improving the security of the digital world.

References

Abrahams, T. O., Ewuga, S. K., Kaggwa, S., Uwaoma, P. U., Hassan, A. O., & Dawodu, S. O. (2024). Mastering compliance: a comprehensive review of regulatory frameworks in accounting and cybersecurity. *Computer Science & IT Research Journal*, *5*(1), 120-140. https://doi.org/10.51594/csitrj.v5i1.709

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and HumanDecision Processes, 50*(2), 179-211. https://doi:10.1016/0749-5978(91)90020-T

Aldawood, H., & Skinner, G. (2019). Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues. *Future Internet*, *11*(3), 73. https://doi.org/10.3390/fi11030073

Alnoaim, J. A. (2022). Sociocultural and social cognitive theories: Historical and current practices for students with emotional and behavioural disorder (EBD). *Information Sciences Letters*, *11*(6), 1859–1870. https://doi.org/10.18576/isl/110601

Alpi, K. M., & Evans, J. J. (2019). Distinguishing case study as a research method from case reports as a publication type. *Journal of the Medical Library Association*, *107*(1). https://doi.org/10.5195/jmla.2019.615

AlQadheeb, A., Bhattacharyya, S., & Perl, S. (2022). Enhancing cybersecurity by generating user-specific security policy through the formal modelling of user behavior. *Array*, 100146. https://doi.org/10.1016/j.array.2022.100146

Alsharif, M., Mishra, S., & AlShehri, M. (2022). Impact of Human Vulnerabilities on Cybersecurity. *Computer Systems Science and Engineering*, *40*(3), 1153–1166. https://doi.org/10.32604/csse.2022.019938

Ameen, N., Tarhini, A., Shah, M. H., Madichie, N., Paul, J., & Choudrie, J. (2021). Keeping customers' data secure: A cross-cultural study of cybersecurity compliance among the Gen-Mobile workforce. *Computers in Human Behavior*, *114*, 106531. https://doi.org/10.1016/j.chb.2020.106531

Amoresano, K., & Yankson, B. (2023). Human Error-A Critical Contributing Factor to the Rise in Data Breaches: A Case Study of Higher Education. *HOLISTICA–Journal of Business and Public Administration*, *14*(1), 110-132. https://doi.org/10.2478/hjbpa-2023-0007

Anderson, J. F. (2014). *Criminological Theories: Understanding crime in America*. Jones & Bartlett Learning, LLC.

Angstmann, J. L., Rollings, A. J., Fore, G. A., & Sorge, B. H. (2019). A pedagogical framework for the design and utilization of place-based experiential learning curriculum on a campus farm. *Journal of Sustainability Education*, *20*, 1-14. Retrieved from http://www.susted.com/wordpress/content/a-pedagogical-framework-for-the-design-and-utilization-of-place-based-experiential-learning-curriculum-on-a-campus-farm_2019_04/

Ani, U. D., He, H., & Tiwari, A. (2019). Human factor security: evaluating the cybersecurity capacity of the industrial workforce. *Journal of Systems and Information Technology*, *21*(1), 2–35. https://doi.org/10.1108/jsit-02-2018-0028

Asare, M. (2015). Using the theory of planned behavior to determine the condom use behavior among college students. *American Journal of Health Studies*, *30*(1), 43–50. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4621079/#:~:text=The%20Theory%20of%20Planned%20Behavior%20(TPB)%20was%20developed%20by%20Icek

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

Atkins, S., & Lawson, C. (2021). An improvised patchwork: success and failure in cybersecurity policy for critical infrastructure. Public Administration Review, 81(5), 847-861. https://doi.org/10.1111/puar.13322

Bamu, B. N., Schauwer, E., & Hove, G. (2016). I can't say I wasn't anticipating it, but I didn't see it coming in this magnitude: A qualitative fieldwork experience in the northwest region of Cameroon. *The Qualitative Report, 21*(3), 571-583. Retrieved from https://nsuworks.nova.edu/tqr/

Bandura, A. (1989). Human agency in social cognitive theory. *American Psychologist*, *44*(9), 1175–1184. https://doi.org/10.1037//0003-066x.44.9.1175

Bandura, A. (2001). Social cognitive theory: an agentic perspective. *Annual Review of Psychology*, *52*(1), 1–26.

Banerjee, A., & Chaudhury, S. (2010). Statistics without tears: Populations and samples. *Industrial Psychiatry Journal*, *19*(1), 60–65. https://doi.org/10.4103/0972-6748.77642

Bansal, P. (Tima), Smith, W. K., & Vaara, E. (2018). New Ways of Seeing through Qualitative Research. *Academy of Management Journal*, *61*(4), 1189–1195. https://doi.org/10.5465/amj.2018.4004

Barosy, W. (2019). Successful Operational Cyber Security Strategies for Small Businesses. *Walden Dissertations and Doctoral Studies*. https://scholarworks.waldenu.edu/dissertations/6969/

Bauer, S., Bernroider, E. W. N., & Chudzikowski, K. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. *Computers & Security*, *68*, 145–159. https://doi.org/10.1016/j.cose.2017.04.009

Benight, C. C., Harwell, A., & Shoji, K. (2018). Self-Regulation Shift Theory: A Dynamic Personal Agency Approach to Recovery Capital and Methodological Suggestions. *Frontiers in Psychology*, *9*(1738). https://doi.org/10.3389/fpsyg.2018.01738

Beuran, R., Pham, C., Tang, D., Chinen, K., Tan, Y., & Shinoda, Y. (2018). Cybersecurity Education and Training Support System: CyRIS. *IEICE Transactions on Information and Systems*, *E101.D*(3), 740–749. https://doi.org/10.1587/transinf.2017edp7207

Blank, R., & Gallagher, P. (2012). Nist special publication 800-30 revision 1 guide for conducting risk assessments. *National Institute of Standards and Technology*. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

Blum, D. (2020). Rational Cybersecurity for Business: The Security Leaders' Guide to Business Alignment (p. 333). Springer Nature. https://doi.org/10.1007/978-1-4842-5952-8

Bosnjak, M., Ajzen, I., & Schmidt, P. (2020). The Theory of Planned behavior: Selected Recent Advances and Applications. *Europe's Journal of Psychology*, *16*(3), 352–356. NCBI. https://doi.org/10.5964/ejop.v16i3.3107

Bouveret, A. (2019, May 21). *Estimation of Losses Due to Cyber Risk for Financial Institutions*. Papers.ssrn.com. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3391740

Bozkus Kahyaoglu, S., & Caliyurt, K. (2018). Cyber security assurance process from the internal audit perspective. *Managerial Auditing Journal*, *33*(4), 360–376. https://doi.org/10.1108/maj-02-2018-1804

Bush, A. A., Amechi, M., & Persky, A. (2019). An Exploration of Pharmacy Education Researchers' Perceptions and Experiences Conducting Qualitative Research. *American Journal of Pharmaceutical Education*, *84*(3), ajpe7129. https://doi.org/10.5688/ajpe7129

Campbell, S., Greenwood, M., Prior, S., Shearer, T., Walkem, K., Young, S., Bywaters, D., & Walker, K. (2020). Purposive Sampling: Complex or Simple? Research Case Examples. *Journal of Research in Nursing*, *25*(8), 652–661. NCBI. https://doi.org/10.1177/1744987120927206

Cheng, E. C. K., & Wang, T. (2022). Institutional Strategies for Cybersecurity in Higher Education Institutions. *Information*, *13*(4), 192. https://doi.org/10.3390/info13040192

CISA.gov. (2021). SAFECOM- Guide to Getting Started with a Cybersecurity Risk Assessment. https://www.cisa.gov/sites/default/files/2024-01/22_1201_safecom_guide_to_cybersecurity_risk_assessment_508.pdf

Code, J. (2020). Agency for Learning: Intention, Motivation, Self-Efficacy and Self-Regulation. *Frontiers in Education*, *5*. https://doi.org/10.3389/feduc.2020.00019

Cope, D. G. (2014). Methods and Meanings: Credibility and Trustworthiness of Qualitative Research. *Oncology Nursing Forum*, *41*(1), 89–91.

Corallo, A., Lazoi, M., Lezzi, M., & Luperto, A. (2022). Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review. *Computers in Industry*, *137*, 103614. https://doi.org/10.1016/j.compind.2022.103614

Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2020). Maximizing Employee Compliance with Cybersecurity Policies. *MIS Quarterly Executive*, 183–198. https://doi.org/10.17705/2msqe.00032

Creswell, J. W., & Creswell, J. D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications.

Cuganesan, S., Steele, C., & Hart, A. (2017). How senior management and workplace norms influence information security attitudes and self-efficacy. *Behaviour &*

Information Technology, *37*(1), 50–65. https://doi.org/10.1080/0144929x.2017.1397193

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research*, *20*(1), 79–98. https://doi.org/10.1287/isre.1070.0160

Dedeke, A., & Masterson, K. (2019). Contrasting cybersecurity implementation frameworks (CIF) from three countries. *Information and Computer Security*. https://doi.org/10.1108/ics-10-2018-0122

Devi, B., Pradhan, S., Giri, D., & Baxodirovna, N. L. (2022). Concept of Social cognitive theory and its application in the field of Medical and Nursing education: framework to guide Research. *Journal of Positive School Psychology*, *6*(4), 5161–5168. https://journalppw.com/index.php/jpsp/article/view/4243/2794

Eboibi, F. E. (2020). Concerns of cyber criminality in South Africa, Ghana, Ethiopia and Nigeria: rethinking cybercrime policy implementation and institutional accountability. *Commonwealth Law Bulletin*, *46*(1), 78–109. https://doi.org/10.1080/03050718.2020.1748075

Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of Convenience Sampling and Purposive Sampling. *American Journal of Theoretical and Applied Statistics*, *5*(1), 1–4.

Fasbender, U. (2019). *(PDF) Outcome Expectancies*. ResearchGate. https://www.researchgate.net/publication/328638738_Outcome_Expectancies

Filippova, A. (2021). Current security issues in the information society. *SHS Web of Conferences*, *109*, 01014. https://doi.org/10.1051/shsconf/202110901014

Fletcher, J. A., & Friedel, J. N. (2018). Interrelationships between funding and state community college governance systems. *Journal of Applied Research in the Community College, 25*(1), 1-15. Retrieved from https://www.montezumapublishing.com/jarcc/issueabstracts/spring2018volume25issue1

Fomby, P., & Sastry, N. (2019). Data Collection on Sensitive Topics with Adolescents Using Interactive Voice Response Technology. *Methoden, Daten, Analysen*, *13*(1), 91–110. https://doi.org/10.12758/mda.2018.05

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

Gearhart, G. D., Abbiatti, M., & Miller, M. (2019). HIGHER EDUCATION'S CYBER SECURITY: LEADERSHIP ISSUES, CHALLENGES AND THE FUTURE. In *International Journal on New Trends in Education and Their Implications April* (pp. 11–18). http://www.ijonte.org/FileUpload/ks63207/File/02.g._david_gearhart.pdf

Goel, R., Kumar, A., & Haddow, J. (2020). PRISM: a strategic decision framework for cybersecurity risk assessment. *Information & Computer Security*, *ahead-of-print*(ahead-of-print). https://doi.org/10.1108/ics-11-2018-0131

Gray, B. (2008). Enhancing Transdisciplinary Research Through Collaborative Leadership. *American Journal of Preventive Medicine*, *35*(2), S124–S132. https://doi.org/10.1016/j.amepre.2008.03.037

Gundu, T. (2019, February). Acknowledging and reducing the knowing and doing gap in employee cybersecurity complaints. In *ICCWS 2019 14th International Conference on Cyber Warfare and Security* (pp. 94-102).

Habibzadeh, H., Nussbaum, B. H., Anjomshoa, F., Kantarci, B., & Soyata, T. (2019). A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities. *Sustainable Cities and Society*, *50*(101660), 101660. https://doi.org/10.1016/j.scs.2019.101660

Halcomb, E. J. (2019). Mixed methods research: The issues beyond combining methods. *Journal of Advanced Nursing*, *75*(3), 499–501. wiley. https://doi.org/10.1111/jan.13877

Hall, J., & Martin, B. R. (2019). Towards a taxonomy of research misconduct: The case of business school research. *Research Policy*, *48*(2), 414–427. https://doi.org/10.1016/j.respol.2018.03.006

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

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*. https://doi.org/10.1007/s10551-020-04442-3

Hennink, M. M., Kaiser, B. N., & Marconi, V. C. (2016). Code Saturation versus Meaning Saturation: How many Interviews are enough? *Qualitative Health Research*, *27*(4), 591–608. https://doi.org/10.1177/1049732316665344

Hepfer, M., & Powell, T. C. (2020). Make Cybersecurity a Strategic Asset. *MIT Sloan Management Review, 62*(1), 40-45. https://www.proquest.com/scholarly-journals/make-cybersecurity-strategic-asset/docview/2450655586/se-2

Hickman, L., & Akdere, M. (2018). Effective leadership development in information technology: building transformational and emergent leaders. *Industrial and Commercial Training*, *50*(1), 1–9. https://doi.org/10.1108/ict-06-2017-0039

Huang, K., & Pearlson, K. (2019). *For What Technology Can't Fix: Building a Model of Organizational Cybersecurity Culture For What Technology Can't Fix: Building a Model of Organizational Cybersecurity Culture*. https://web.mit.edu/smadnick/www/wp/2019-02.pdf

Hussain, A., Mohamed, A., & Razali, S. (2020, March). A review on cybersecurity: Challenges & emerging threats. In Proceedings of the 3rd International Conference on Networking, Information Systems & Security (pp. 1-7). https://doi.org/10.1145/3386723.3387847

Irani, E. (2018). The Use of Videoconferencing for Qualitative Interviewing: Opportunities, Challenges, and Considerations. *Clinical Nursing Research*, *28*(1), 3–8. Sagepub. https://doi.org/10.1177/1054773818803170

Jampen, D., Gür, G., Sutter, T., & Tellenbach, B. (2020). Don't click: towards an effective anti-phishing training. A comparative literature review. *Human-centric*

Computing and Information Sciences, *10*(1), 33. https://doi.org/10.1186/s13673-020-00237-7

Jeong, J., Mihelcic, J., Oliver, G., & Rudolph, C. (2019). Towards an Improved Understanding of Human Factors in Cybersecurity. *2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC)*. https://doi.org/10.1109/cic48465.2019.00047

Kaplan, B. (2020). Revisiting Health Information Technology Ethical, Legal, and Social Issues and Evaluation: Telehealth/Telemedicine and COVID-19. *International Journal of Medical Informatics*, *143*(1), 104239. https://doi.org/10.1016/j.ijmedinf.2020.104239

Kaspersky. (2017). *The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within | Kaspersky official blog*. Kaspersky. https://www.kaspersky.com/blog/the-human-factor-in-it-security/

Kemper, G. (2019). Improving employees' cyber security awareness. *Computer Fraud & Security*, *2019*(8), 11–14. https://doi.org/10.1016/s1361-3723(19)30085-5

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

Kong, Y. (2021). The Role of Experiential Learning on Students' Motivation and Classroom Engagement. *Frontiers in Psychology*, *12*(1). https://doi.org/10.3389/fpsyg.2021.771272

Kosutic, D., & Pigni, F. (2022). Cybersecurity: investing for competitive outcomes. Journal of Business Strategy, 43(1), 28-36. https://doi.org/10.1108/JBS-06-2020-0116

Kursan Milaković, I. (2021). Purchase experience during the COVID-19 pandemic and social cognitive theory: The relevance of consumer vulnerability, resilience, and adaptability for purchase satisfaction and repurchase. *International Journal of Consumer Studies*, *45*(6). https://doi.org/10.1111/ijcs.12672

Lehto, M., & Limnéll, J. (2020). Strategic leadership in cyber security, case Finland. *Information Security Journal: A Global Perspective*, *30*(3), 1–10. https://doi.org/10.1080/19393555.2020.1813851

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, *45*(45), 13–24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Linkov, V., Zámečník, P., Havlíčková, D., & Pai, C.-W. (2019). Human Factors in the Cybersecurity of Autonomous Vehicles: Trends in Current Research. *Frontiers in Psychology*, *10*. https://doi.org/10.3389/fpsyg.2019.00995

Liu, C., Wang, N., & Liang, H. (2020). Motivating information security policy compliance: The critical role of supervisor-subordinate guanxi and organizational commitment. *International Journal of Information Management*, *54*, 102152. https://doi.org/10.1016/j.ijinfomgt.2020.102152

Lowry, P. B., Zhang, J., & Wu, T. (2017). Nature or nurture? A meta-analysis of the factors that maximize the prediction of digital piracy by using social cognitive theory as a framework. *Computers in Human Behavior*, *68*, 104–120. https://doi.org/10.1016/j.chb.2016.11.015

Mallick, M. A. I., & Nath, R. (2024). Navigating the Cyber Security Landscape: A Comprehensive Review of Cyber-Attacks, Emerging Trends, and Recent Developments. *World Scientific News*, *190*(1), 1-69. https://www.researchgate.net/profile/Md-Mallick/publication/378343830_Navigating_the_Cyber_security_Landscape_A_Comprehensive_Review_of_Cyber-Attacks_Emerging_Trends_and_Recent_Developments/links/65d5dc11adf2362b634a53ff/Navigating-the-Cyber-security-Landscape-A-Comprehensive-Review-of-Cyber-Attacks-Emerging-Trends-and-Recent-Developments.pdf

Manjarres-Posada, N. I., Onofre-Rodríguez, D. J., & Benavides-Torres, R. A. (2020). Social Cognitive Theory and Health Care: Analysis and Evaluation. *International Journal of Social Science Studies*, *8*(4), 132. https://doi.org/10.11114/ijsss.v8i4.4870

Marotta, A., & Madnick, S. (2021). Convergence and divergence of regulatory compliance and cybersecurity. Issues in Information Systems, 22(1). https://doi.org/10.48009/1_iis_2021_10-50

McGrath, C., Palmgren, P. J., & Liljedahl, M. (2018). Twelve tips for conducting qualitative research interviews. *Medical Teacher*, *41*(9), 1–5. Tandfonline. https://doi.org/10.1080/0142159X.2018.1497149

Merriam, S. B. (2009). *Qualitative research : a guide to design and implementation*. Jossey-Bass.

Miracle, V. A. (2016). The Belmont Report. *Dimensions of Critical Care Nursing*, *35*(4), 223–228. https://doi.org/10.1097/dcc.0000000000000186

Mittal, S. (2015). Understanding the human dimension of cyber security. *Indian Journal of Criminology & Criminalistics (ISSN 0970–4345)*, *34*(1), 141-152. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2975924

Mohajan, H. K. (2018). Qualitative Research Methodology in Social Sciences and Related Subjects. *Journal of Economic Development, Environment and People*, *7*(1), 23–48. https://mpra.ub.uni-muenchen.de/85654/1/mpra_paper_85654.pdf

Motulsky, S. L. (2021). Is member checking the gold standard of quality in qualitative research? *Qualitative Psychology*, *8*(3), 389–406. https://doi.org/10.1037/qup0000215

Murphy, T. F. (2022, August 25). *Outcome Expectancies*. Psychology Fanatic. https://psychologyfanatic.com/outcome-expectancies/#:~:text=Bandura%20explains%20that%20%E2%80%9Cin%20this

Nakabayashi, K. (2018). Course design investigation and trial on the subject of self-regulated learning using video content and online report submission. *Interactive*

Technology and Smart Education, *15*(2), 104–118. https://doi.org/10.1108/itse-10-2017-0050

Nickerson, C. (2024, February 2). *Albert Bandura's Social Cognitive Theory: Definition & Examples*. Simply Psychology. https://www.simplypsychology.org/social-cognitive-theory.html

Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review. *Sensors*, *21*(15), 5119. https://doi.org/10.3390/s21155119

Nobles, C. (2022). Stress, Burnout, and Security Fatigue in Cybersecurity: A Human Factors Problem. *HOLISTICA – Journal of Business and Public Administration*, *13*(1), 49–72. https://doi.org/10.2478/hjbpa-2022-0003

Nusbaum, L., Douglas, B., Damus, K., Paasche-Orlow, M., & Estrella-Luna, N. (2017). Communicating Risks and Benefits in Informed Consent for Research: a Qualitative Study. *Global Qualitative Nursing Research*, *4*(1), 233339361773201. https://doi.org/10.1177/2333393617732017

Onumo, A., Ullah-Awan, I., & Cullen, A. (2021). Assessing the moderating effect of security technologies on employees compliance with cybersecurity control procedures. ACM Transactions on Management Information Systems (TMIS), 12(2), 1-29. https://doi.org/10.1145/3424282

Palvia, P., Ghosh, J., Jacks, T., & Serenko, A. (2021). Information technology issues and challenges of the globe: the world IT project. *Information & Management*, *58*(8), 103545. https://doi.org/10.1016/j.im.2021.103545

Phillippi, J., & Lauderdale, J. (2018). A Guide to Field Notes for Qualitative Research: Context and Conversation. *Qualitative Health Research*, *28*(3), 381–388. https://doi.org/10.1177/1049732317697102

Pohl, C., Rist, S., Zimmermann, A., Fry, P., Gurung, G. S., Schneider, F., Speranza, C. I., Kiteme, B., Boillat, S., Serrano, E., Hadorn, G. H., & Wiesmann, U. (2010). Researchers' roles in knowledge co-production: experience from sustainability research in Kenya, Switzerland, Bolivia and Nepal. *Science and Public Policy*, *37*(4), 267–281. https://doi.org/10.3152/030234210x496628

Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2021). Leveraging human factors in cybersecurity: an integrated methodological approach. *Cognition, Technology & Work*, *24*(2). https://doi.org/10.1007/s10111-021-00683-y

Poluektova, O., Kappas, A., & Smith, C. A. (2023). Using Bandura's Self-Efficacy Theory to Explain Individual Differences in the Appraisal of Problem-Focused Coping Potential. *Emotion Review*, *15*(4), 175407392311643. https://doi.org/10.1177/17540739231164367

Pomerleau, P. L., Lowery, D. L., Pomerleau, P. L., & Lowery, D. L. (2020). Major Themes in the Literature of Cybersecurity and Public–Private Partnerships; A Focus on Financial Institutions. Countering Cyber Threats to Financial

Institutions: A Private and Public Partnership Approach to Critical Infrastructure Protection, 87-122. https://doi.org/10.1007/978-3-030-54054-8_5

Pöyhönen, J., & Lehto, M. (2020). Cyber security : Trust based architecture in the management of an organization‘s security. In T. Eze, L. Speakman, & C. Onwubiko (Eds.), *ECCWS 2020 : Proceedings of the 19th European Conference on Cyber Warfare and Security* (pp. 304-313). Academic Conferences International. Proceedings of the European conference on information warfare and security. doi.org/10.34190/EWS.20.090

Quayyum, F., Cruzes, D. S., & Jaccheri, L. (2021). Cybersecurity awareness for children: A systematic literature review. *International Journal of Child-Computer Interaction*, *30*, 100343. https://doi.org/10.1016/j.ijcci.2021.100343

Rahman, S. (2017). The Advantages and Disadvantages of Using Qualitative and Quantitative Approaches and Methods in Language “Testing and Assessment” Research: a Literature Review. *Journal of Education and Learning*, *6*(1), 102–112. https://doi.org/10.5539/jel.v6n1p102

Rajasekharaiah, K. M., Dule, C. S., & Sudarshan, E. (2020, December). Cyber security challenges and its emerging trends on latest technologies. In IOP Conference Series: Materials Science and Engineering (Vol. 981, No. 2, p. 022062). IOP Publishing. https://doi.org/10.1088/1757-899X/981/2/022062

Reeder, J. R., & Barnsby, R. E. (2020). A Legal Framework for Enhancing Cybersecurity through Public-Private Partnership. The Cyber Defense Review, 5(3), 31-44. https://www.jstor.org/stable/26954871

Reegård, K., Blackett, C., & Katta, V. (2019). The concept of cybersecurity culture. In *29th European Safety and Reliability Conference* (pp. 4036-4043). https://doi.org/10.3850/978-981-11-2724-3_0761-cd

Reeves, A., Delfabbro, P., & Calic, D. (2021). Encouraging Employee Engagement With Cybersecurity: How to Tackle Cyber Fatigue. *SAGE Open*, *11*(1), 215824402110000. https://doi.org/10.1177/21582440211000049

Ricci, J., Breitinger, F., & Baggili, I. (2018). Survey results on adults and cybersecurity education. *Education and Information Technologies*, *24*(1), 231–249. https://doi.org/10.1007/s10639-018-9765-8

Rivard, J. R., Fisher, R. P., Robertson, B., & Hirn Mueller, D. (2014). Testing the Cognitive Interview with Professional Interviewers: Enhancing Recall of Specific Details of Recurring Events. *Applied Cognitive Psychology*, *28*(6), 917–925. https://doi.org/10.1002/acp.3026

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.

Roulston, K. (2017). Qualitative interviewing and epistemics. *Qualitative Research*, *18*(3), 322–341. https://doi.org/10.1177/1468794117721738

Sanders, S., Stensland, M., & Juraco, K. (2017). Agency behind bars: Advance care planning with aging and dying offenders. *Death Studies*, *42*(1), 45–51. https://doi.org/10.1080/07481187.2017.1303552

Schiavo, M., Prinari, B., Saito, I., Shoji, K., & Benight, C. C. (2019). A dynamical systems approach to triadic reciprocal determinism of social cognitive theory. *Mathematics and Computers in Simulation*, *159*, 18–38. https://doi.org/10.1016/j.matcom.2018.10.006

Schoenfeld, J., Segal, G., & Borgia, D. (2017). Social cognitive career theory and the goal of becoming a certified public accountant. *Accounting Education*, *26*(2), 109–126. https://doi.org/10.1080/09639284.2016.1274909

Schunk, D. H., & Pajares, F. (2009). Self-efficacy theory. In K. R. Wentzel & A. Wigfield (Eds.), *Handbook of motivation at school* (pp. 35–53)

Shabani, M., & Borry, P. (2017). Rules for processing genetic data for research purposes in view of the new EU General Data Protection Regulation. *European Journal of Human Genetics*, *26*(2), 149–156. https://doi.org/10.1038/s41431-017-0045-7

Shahangian, S. A., Tabesh, M., & Yazdanpanah, M. (2021). Psychosocial determinants of household adoption of water-efficiency behaviors in Tehran capital, Iran: Application of the social cognitive theory. *Urban Climate*, *39*, 100935. https://doi.org/10.1016/j.uclim.2021.100935

Shamir, B., & Eilam, G. (2005). "What's Your Story?" A Life-stories Approach to Authentic Leadership Development. *The Leadership Quarterly*, *16*(3), 395–417. https://doi.org/10.1016/j.leaqua.2005.03.005

Sihombing, B. F. (2019). Contemporary Issues of Agrarian Law Institutions: Critical Analysis of Legal Structure on Human Capital and Information Technology. *Journal of Legal, Ethical and Regulatory Issues*, *22*(2), 1–315.

https://www.abacademies.org/articles/contemporary-issues-of-agrarian-law-institutions-critical-analysis-of-legal-structure-on-human-capital-and-information-technology-8168.html

Silvia, C. (2011). Collaborative Governance Concepts for Successful Network Leadership. *State and Local Government Review*, *43*(1), 66–71. https://doi.org/10.1177/0160323x11400211

Slapničar, S., Vuko, T., Čular, M., & Drašček, M. (2022). Effectiveness of cybersecurity audit. *International Journal of Accounting Information Systems*, *44*, 100548. https://doi.org/10.1016/j.accinf.2021.100548

Sobb, T., Turnbull, B., & Moustafa, N. (2020). Supply chain 4.0: A survey of cyber security challenges, solutions and future directions. Electronics, 9(11), 1864. https://doi.org/10.3390/electronics9111864

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. https://doi.org/10.17583/qre.2017.2374

Sulistyowati, D., Handayani, F., & Suryanto, Y. (2020). Comparative analysis and design of cybersecurity maturity assessment methodology using nist csf, cobit, iso/iec 27002, and pci dss. *JOIV: International Journal on Informatics Visualization*, *4*(4), 225-230. http://dx.doi.org/10.30630/joiv.4.4.482

Swain, J. (2018). A Hybrid Approach to Thematic Analysis in Qualitative Research: Using a Practical Example. *Sage Research Methods*. https://doi.org/10.4135/9781526435477

Tagarev, T. (2020). Towards the design of a collaborative cybersecurity networked organisation: Identification and prioritisation of governance needs and objectives. Future Internet, 12(4), 62. https://doi.org/10.3390/fi12040062

Uchendu, B., Nurse, J. R., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. Computers & Security, 109, 102387. https://doi.org/10.1016/j.cose.2021.102387

Uprichard, E., & Dawney, L. (2016). Data Diffraction: Challenging Data Integration in Mixed Methods Research. *Journal of Mixed Methods Research*, *13*(1), 19–32. https://doi.org/10.1177/1558689816674650

Vayena, E., Brownsword, R., Edwards, S. J., Greshake, B., Kahn, J. P., Ladher, N., Montgomery, J., O'Connor, D., O'Neill, O., 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

Wang, P., Morris, R., & Wood, D. F. (2019). ECONOMIC COSTS AND IMPACTS OF BUSINESS DATA BREACHES. *Issues in Information Systems*, *20*(2), 162–171. https://iacis.org/iis/2019/2_iis_2019_162-171.pdf

Wang, Y., Shen, C., Bartsch, K., & Zuo, J. (2021). Exploring the trade-off between benefit and risk perception of NIMBY facility: A social cognitive theory model.

Environmental Impact Assessment Review, *87*, 106555. https://doi.org/10.1016/j.eiar.2021.106555

Wixted, J. T., Mickes, L., & Fisher, R. P. (2018). Rethinking the Reliability of Eyewitness Memory. *Perspectives on Psychological Science*, *13*(3), 324–335. https://doi.org/10.1177/1745691617734878

Wong, L.-W., Lee, V.-H., Tan, G. W.-H., Ooi, K.-B., & Sohal, A. (2022). The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities. *International Journal of Information Management*, *66*, 102520. https://doi.org/10.1016/j.ijinfomgt.2022.102520

Woodcock, S., & Tournaki, N. (2022). Bandura's triadic reciprocal determinism model and teacher self-efficacy scales: A revisit. *Teacher Development*, *27*(1), 1–17. https://doi.org/10.1080/13664530.2022.2150285

Yoo, C. W., Sanders, G. L., & Cerveny, R. P. (2018). Exploring the influence of flow and psychological ownership on security education, training and awareness effectiveness and security compliance. *Decision Support Systems*, *108*, 107–118. https://doi.org/10.1016/j.dss.2018.02.009

Yoon, H. J. (2019). Toward Agentic HRD: A Translational Model of Albert Bandura's Human Agency Theory. *Advances in Developing Human Resources*, *21*(3), 335–351. https://doi.org/10.1177/1523422319851437

Young, H. N., Lipowski, E. E., & Cline, R. J. W. (2005). Using social cognitive theory to explain consumers' behavioral intentions in response to direct-to-consumer

prescription drug advertising. *Research in Social and Administrative Pharmacy*, *1*(2), 270–288. https://doi.org/10.1016/j.sapharm.2005.03.011

Young, M. D., Plotnikoff, R. C., Collins, C. E., Callister, R., & Morgan, P. J. (2014). Social cognitive theory and physical activity: a systematic review and meta-analysis. *Obesity Reviews*, *15*(12), 983–995. https://doi.org/10.1111/obr.12225

Yusif, S., & Hafeez-Baig, A. (2021). A Conceptual Model for Cybersecurity Governance. *Journal of Applied Security Research*, *16*(4), 1–24. https://doi.org/10.1080/19361610.2021.1918995

Zeadally, S., Adi, E., Baig, Z., & Khan, I. A. (2020). Harnessing artificial intelligence capabilities to improve cybersecurity. *IEEE Access*, *8*, 23817-23837. https://doi.org/10.1109/ACCESS.2020.2968045.

Zhang-Kennedy, L., & Chiasson, S. (2021). A Systematic Review of Multimedia Tools for Cybersecurity Awareness and Education. *ACM Computing Surveys*, *54*(1), 1–39. https://doi.org/10.1145/3427920

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*, *62*(1), 1–16. https://doi.org/10.1080/08874417.202