THE IMPACT OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING ON ORGANIZATIONS CYBERSECURITY

by

Mustafa Abdulhussein

Dissertation

Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Liberty University, School of Business

February 2024

Abstract

As internet technology proliferate in volume and complexity, the ever-evolving landscape of malicious cyberattacks presents unprecedented security risks in cyberspace. Cybersecurity challenges have been further exacerbated by the continuous growth in the prevalence and sophistication of cyber-attacks. These threats have the capacity to disrupt business operations, erase critical data, and inflict reputational damage, constituting an existential threat to businesses, critical services, and infrastructure. The escalating threat is further compounded by the malicious use of artificial intelligence (AI) and machine learning (ML), which have increasingly become tools in the cybercriminal arsenal. In this dynamic landscape, the emergence of offensive AI introduces a new dimension to cyber threats. The current wave of attacks is surpassing human capabilities, incorporating AI to outsmart and outpace traditional, rule-based detection tools. The advent of "offensive AI" allows cybercriminals to execute targeted attacks with unprecedented speed and scale, operating stealthily and evading conventional security measures. As offensive AI looms on the horizon, organizations face the imperative to adopt new, more sophisticated defenses. Human-driven responses to cyber-attacks are struggling to match the speed and complexity of automated threats. In anticipation of this growing challenge, the implementation of advanced technologies, including AI-driven defenses, becomes crucial. This dissertation explored the profound impact of both AI and ML on cybersecurity in the United States. Through a qualitative, multiple case study, combining a comprehensive literature review with insights from cybersecurity experts, the research identified key trends, challenges, and opportunities for utilizing AI in cybersecurity.

Key words: artificial intelligence, cybersecurity, technology, cyber-attacks, automation, machine learning, IoT, cloud

THE IMPACT OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING ON ORGANIZATIONS CYBERSECURITY

by

Mustafa Abdulhussein

Dissertation

Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Liberty University, School of Business

February 2024

Approvals

_____	_____
Mustafa Abdulhussein, Doctoral Candidate	Date
_____	_____
Dr. Dennis Backherms, PhD, Dissertation Chair	Date
_____	_____
Dr. Mike Keprios, DBA, Committee Member	Date
_____	_____
Alexander Averin, PhD, MBA Chair, Doctoral Programs	Date

Dedication

I dedicate this dissertation to my family, advisors, mentors, participants, and all those who have supported me along the way. Without your support, this achievement would not have been possible. Thank you for being a part of my journey. To my beloved parents, I dedicate this dissertation to you. Your love and support have been my anchor during my academic journey. You have been there for me through the highs and lows, the successes, and failures, and have always encouraged me to pursue my dreams. I am grateful for the sacrifices you have made to ensure that I had the best opportunities in life. Your belief in me has been a source of inspiration, and I am forever indebted to you. To my research board and mentors, I would like to express my deepest gratitude for your guidance and support. Your expertise, encouragement, and constructive feedback have been invaluable throughout this journey. Your passion for your field and dedication to teaching have been inspiring, and I feel honored to have had the opportunity to learn from you. Your mentorship has helped shape me into the researcher and scholar that I am today. To the participants of my study, I would like to express my appreciation for your willingness to participate in my research. Your contributions have been critical to the success of this study, and I am grateful for your time and effort. I hope that the findings of this study will contribute to the advancement of knowledge in this field.

Acknowledgments

I would like to start by thanking parents. My mother has been a great source of support and encouragement throughout my academic journey, from the time I was a little child. Her belief in me, her patience, and her constant encouragement have been instrumental in helping me to overcome the many challenges and obstacles that I have faced along the way. I am also deeply grateful for all that my father has done to help me achieve my goals. Despite the challenging security situation in my home country during the war and the struggles of completing my final year in undergraduate school, I was on the brink of giving up. It was my father who persuaded me to persevere; he became my primary source of support during those tough times. He consistently reminded me that I was just a step away from reaching the finish line. Without his encouragement and guidance, making it through my undergraduate studies during such a difficult period would not have been possible.

I would like to express my deepest gratitude to my dissertation chair Dr. Dennis Backherms for his professional guidance and supervision throughout this entire research journey. Dr. Backherms' insightful feedback enlightened me on the appropriate approach to conducting academic research. He never hesitated to answer my questions, consistently offering support and proving to be a crucial factor in my success. I am also grateful to Dr. Kipreos and the members of my doctoral committee for their feedback and support throughout this process. Their expertise and insights have been critical in helping me to navigate the complex terrain of doctoral research, and I am deeply appreciative of their time and commitment.

Table of Contents

List of Tables

List of Figures

Section 1: Foundation of the Study

In recent years, AI has emerged as an important means for augmenting the efforts of human information security teams. As of the current study, research has not paid close attention to malicious AI in cybersecurity and its threat to business operations. Instead, most of the research efforts have focused on using artificial intelligence (AI) and machine learning (ML) to improve security posture to include malware detection by learning patterns and behaviors. Zhang (2022) indicated that adversaries are also using AI as its subset, ML to mount more automated, aggressive, and coordinated attacks. In addition to using AI technology to automate attacks, hackers and cybercriminals have gotten smarter and more efficient utilizing AI tools to develop a deeper understanding of what companies use to prevent them from penetrating their environments; learning about companies' procedures and measures taken against cyber-attacks enable hackers to discover new gaps in the attack surface and predict companies' potential reaction against these attacks. With the unprecedented growth rate of AI capabilities in today's environment, it is more about using the right AI tools and technologies to fight intelligence with intelligence than using it to fight machines with machines (Zhang, 2022). Brundage et al. (2018) emphasized that while AI technologies have countless beneficial tools and applications, ranging from medical image analysis to machine translation, and applications are being developed and can be expected over the long term, many of these tools are in the hands of cybercriminals and malicious actors and less attention has historically been paid to the potential damages malicious AI can cause to cybersecurity field and very little has been understood about how hackers use AI technology to launch cyber-attacks.

Cybercriminals now leverage AI technologies to orchestrate automated attacks, social engineering campaigns and phishing scams. The development of unregulated AI models on the dark web adds more complexity to the threat. As AI continues to evolve, the need for cybersecurity

professionals and organizations to adapt and remain vigilant becomes a necessity. Automated cyber-attacks, with their scale and efficiency, pose significant risks, causing extensive and rapid damage compared to traditional methods. This research explored various AI and ML-powered cyber threats, ranging from continuous attacks to deep fakes and polymorphic malware. It explored the tools cybercriminals utilize to automate and enhance their activities such as generative pre-trained transformer (GPT) tools. The research addressed the financial impact of automated cyber-attacks in encompassing operational disruptions, legal penalties, reputational damage, and individual financial losses. While AI and ML offer advantages in cybersecurity, such as improved response times and threat detection, their implementation requires careful management to address ethical considerations and potential challenges. The research emphasizes the collaborative efforts of technology organizations, leveraging ML algorithms and AI to model attack patterns, automate responses, and enhance overall security measures. It addressed the decision-making in AI technology investments and cybersecurity is highlighted, involving collaboration, awareness, financial considerations, and adaptability to evolving threats. The governance and regulation of open-source AI-based tools present challenges as technology advances rapidly. Striking a balance between innovation, freedom, and security remains crucial. In the study, employee awareness and compliance emerged as critical factors in bolstering cybersecurity, necessitating regular training, testing, and accountability measures.

The purpose of this qualitative multiple case study is to discover the dark side of AI in the cybersecurity and defensive tactics that should be employed by organizations to reduce the risk of automated cyber-attacks. It emphasizes the necessity of leveraging AI as a core component of an organizations' cybersecurity. In addition to exploring the harmful side of AI and ML, this research study intends to identify the effectiveness of AI applications and cybersecurity in the war against

cybercrimes by identifying some business practices that help organizations prevent the risk of having to deal with the consequences of cyber-attacks. Lastly, the researcher felt the necessity to identify the best practices in research areas with more mature methods for addressing the negative impact of AI on cybersecurity. Section 1 consists of the background of the problem, problem statement, purpose statement, nature of the study, research questions, conceptual framework that includes two concepts and one theory, definitions of terms that reader might not be familiar with, assumptions, limitations, delimitations, the significance of the study, and a full review of the professional and academic literature.

Background of the Problem

The rapid development of AI and ML in technology drew the attention of information technology experts and even the U.S. government. Despite the advantage that AI adds to the cybersecurity field and the critical role ML plays in cybercrime detection and prevention. AI indeed has a dark side as it can enhance the capabilities of AI-powered cyberattacks. The usage of AI and ML technologies for cyber-attacks purposes has begun to appear in the United States. As AI increases the risk and effectiveness of cyber-attacks, technology organizations should prepare to counter the malicious AI that could cause severe damage to many businesses. Deploying AI and ML technologies to conduct cyber-attacks can create a practical business problem for the technology organizations that provide products and services to the most critical sectors in the United States.

According to Dixon and Eagan (2019), offensive AI's highly sophisticated and malicious attack code poses a threat to the technology field. It mutates itself, learns the environment, and then compromises systems with a small chance of detection. Paoli et al. (2018) indicated that cyber-attacks are becoming ubiquitous and recognized as one of the most strategically significant risks

facing the world today. These cyber/digital attacks targeted governments, critical infrastructure, private corporations, educational institutions, and non-profit organizations. That made experts realize that no sector or entity can be immune to these harmful attacks as the level of sophistication of AI-powered attacks is continually increasing (Dixon & Eagan, 2019). The use of AI-enabled cyber tools is not just limited to IT professionals; it is now available for use to state-sponsored actors, criminals, loan actors and even individuals. This availability has dramatically increased the risk of AI-powered cyberattacks. This study explored how technology companies can face serious business problems without taking the necessary measures and constantly evolving their security practices. It also focused on cybersecurity as one of the areas most affected by the technological advancement of AI and ML which represent a significant applied business problem to the technology organizations.

According to Carriço (2018), the greatest danger posed by AI is its ability for weaponization. Yamin et al. (2021) defined weaponized AI as malicious AI algorithms that can degrade the performance and disrupt the normal functions of benign AI algorithms while providing technological edge attack scenarios in cyberspace and physical spaces. Kaloudi and Li (2020) acknowledged that highly targeted and evasive attacks in simple and harmless carrier applications have demonstrated the intentional use of AI for harmful purposes. Social engineering attacks, phishing attacks, password attacks, distributed denial of service (DDoS) attacks, data manipulation, mutating malware attacks; all such attacks could be operationalized through simple applications the victims use on their devices. Therefore, the risk derived from the abuse of AI technology can strike targets far faster than humans can.

Current academic literature recognizes the practical business problem of AI-powered cyberattacks as a current concern and not a hypothetical future idea. The critical building blocks for

the use of offensive AI already exist, including highly sophisticated malware financially motivated cyber criminals willing to use all the available tools to break into systems and increase their financial profits (Dilek et al., 2015). Despite several studies on AI and security, researchers have not provided a clear explanation about the adversary's actions and how to develop proper defenses against AI-based cyber-attacks. Deficiencies in current information systems literature include an incomplete understanding of how an AI-enabled cyber-attack can be a critical threat with the advancement of technology. Whereas academic literature expansively addresses the benefits of AI-based technology on securing organizations' systems and how it contributes to improving these systems. The focus on the positive side of AI and the lack of the negative impact of AI in the field of information systems represents a gap in current literature.

Problem Statement

The general problem to be addressed is the use of AI and ML to conduct cyber-attacks against organizations resulting in the inability of organizations to effectively secure their networks from data breaches and malicious attacks (Shakeel, 2021). Brundage et al. (2018) indicated that using AI to automate tasks involved in conducting cyber-attacks may increase the risk associated with several types of cyber-attacks including labor-intensive cyber-attacks such as spear phishing, cyber-attacks that exploit human vulnerabilities such as the use of speech synthesis for impersonation, cyber-attacks that exploit software vulnerabilities such as automated hacking, or conduct adversarial examples and data poisoning exploiting the weakness of AI systems. Al-Moshaigeh et al. (2019) discussed how the growth of Al will trigger a wide range of cyber-attacks even more than before. It enables hackers to target organizations and businesses at a more rapid penetration rate, with more effective cyber-attack means. Olenick (2018) indicated that while AI-based technology becomes more widely used, an increase of cybersecurity threats and attacks is

becoming an ever-growing problem amongst the business industry all across the United States. Gao et al. (2020) emphasized that damage caused by data breaches could negatively affect an organization's finances and reputation. Cybercriminals capitalize on the growing AI technology to find more efficient offensive techniques that help them launch cyber-attacks on a vast scale with a higher effect (Shakeel, 2021). According to statistics, the United States breach incidents in 2017 hit a record high of 1,579 breaches. Paoli et al. (2018) predicted that the projected financial loss resulting from the continuous growth of cybercrime is expected to increase to reach $6 trillion annually by 2021. The specific problem to be addressed is the potential use of AI and ML to conduct cyberattacks against organizations within the technology industry in the United States, resulting in the inability of organizations to effectively secure their networks from data breaches and malicious attacks.

Purpose Statement

The purpose of this flexible design multiple case study is to explore how AI and ML-based technology can affect organizations' cybersecurity. The research sought to determine the threat AI can pose on organizations' assets and the tools used by adversaries and cybercriminals to conduct AI-powered cyberattacks, data breaches and malicious activities that can damage business assets and reputation. Since AI in cybersecurity is a two-edged sword, the research shed light on the benefit of AI to the cybersecurity field as well. Shakeel (2021) stated, "Intruders employ new methods and launch more comprehensive strategies based on AI to compromise systems. Similarly, organizations have started using robust defense systems that use AI (AI) to fight AI-powered cyberattacks." Therefore, this study examined the measures technology organizations in the United States can take to control such malicious attacks by answering the research questions that specifically seek to discover existing trends in AI-based cyber-attacks and cyber defenses.

Exploration of the problem occurs through an in-depth study of the negative impact technology businesses across the United States experienced as a result of cybersecurity threats in AI-based technology and the countermeasure taken to deter, mitigate or prevent them using the same type of technology. Cybercriminals employ AI to power cyber-attacks in several ways, including social engineering attacks by detecting patterns in behavior that they use to manipulate behaviors, gain access to sensitive information, and compromise networks. Human hackers can use AI to develop mutating malware to mutate software from detection; ML can help in data manipulation, which can have a devastating impact on technology business.

According to Munk (2022), adversaries take advantage of AI to identify network vulnerabilities. Fortunately, AI enables defense methods and services to detect and respond to cyber threats, which allows organizations to invest in ML technology to secure their networks and enhance their defenses against automated attacks, investing in robust cybersecurity systems that use the detection capabilities of AI and ML can form robust defense systems that are capable of detecting abnormal behaviors, automates identification and mitigation operations. The study intends to extend the current body of knowledge by identifying existing methods and techniques used to execute AI-based cyber-attacks.

Research Questions

RQ1 - How does the growth of AI contribute to the increase of cyberattacks and data breaches against organizations?

RQ1a - What are the negative effects of AI on cybersecurity?

RQ1b - What are some AI and ML tools Cybercriminals use to conduct cyber-attacks?

RQ1c - How do hackers take advantage of AI to conduct cybercrime- related activities?

RQ2 – How does AI contribute to enhance cybersecurity within organizations?

RQ2a - What are the positive effects of AI on cybersecurity?

RQ2b - What are some AI and ML tools organizations use to detect and counter cyber-attacks?

RQ2c - What can leaders do to avoid cyberattacks and secure their networks from data breaches and malicious activities.

RQ3 - How important is it for the high-tech industry in the United States to invest more in AI?

RQ3a -What are the challenges for businesses to build a reliable security system that cannot be compromised by hackers?

RQ4 - What are the financial impacts that organizations face as a result of cybersecurity threats?

RQ4a - What are the financial implications of cyber-attacks and data breaches on customers?

Nature of the Study

This study's proposed research method and design is a qualitative, flexible, multiple case study. The researcher selected pragmatism as the research paradigm representing the view of reality and truth for applied business research; the researcher explained how this worldview can guide the study. The nature of the study section described the research methodology by determining the design and method to study the problem at a very high level, as well as the rationale of the selected design and method. The researcher explained why choosing the qualitative research method and using multiple case study designs to conduct the research. Lastly, the researcher utilized triangulation to analyze results using different data collection methods to enhance validity and interrogate various means to better understand the research problem

(Kobayashi, 2019). The study supported the function of the selected research paradigm and methodology with multiple citations in order to emphasize their effectiveness to guide the study.

Discussion of Research Paradigm

The researcher's worldview is pragmatism. As indicated by Creswell (2017), pragmatism focuses on outcomes of the research rather than the antecedent condition and that it is not committed to any system of reality makes it suitable to the researcher's approach to the study and guided the research study. It allowed the researcher to choose methods and techniques of research that best meet the researcher's needs and purposes. Post-positivism offers a dynamic approach to research where the research problem drives the methodology. The way to investigate the problem is by using a diverse approach that includes qualitative data collection and analysis (Creswell & Poth, 2018). That said, understanding the connection between philosophical worldview and qualitative research methodology should give one's research a direction and provide the main structure of the research. Unlike pragmatism, post-positivism includes "hard science" researchers and those who take a cause-and-effect perspective (Creswell & Poth, 2018).

Post-positivists believe that a singular reality exists, but it cannot be known exactly. They tend to possess objective and unbiased values, not allowing personal views to interfere with their conclusions (Creswell & Poth, 2018). Everything that happens in the world happened due to another event, which does not align with the researcher's view. The constructivism philosophy focuses on one's interactions with the world around him and not so much intangible faith. Creswell and Poth (2018) stated, "In social constructivism, individuals seek understanding of the world in which they live and work" (p. 25). According to Creswell and Poth (2018), the goal of constructivism is to rely on the views of participants to understand a problem. Because it favors an inductive approach, it extrapolates the views of participants into theory. Constructivism is thus

typically qualitative and focuses on specific activities and the situations surrounding people's work to make meaning of how people see their functions.

Creswell and Poth (2018) explained how the four philosophical worldviews are all different but serve the same purpose of guiding a researcher's methods. The pragmatic method allows the researcher to find a balanced ground when researching a worldly situation. Bansal (2018) explained that the researcher can utilize open-ended questions to drive the research. Qualitative research promotes an approach that does not solely rely on data. Thus, the qualitative method and pragmatic framework work well together to solve a situation (Dodgson, 2019). According to Frey (2018), the pragmatic paradigm refers to a worldview that focuses on "what works" rather than what considered absolutely and objectively "true" or "real." Robson and McCartan (2016) indicated that a pragmatic view deals with things sensibly and realistically in a practical way rather than theoretically; they also explained that pragmatic researchers utilize a combination of research methods; thus, method and research diversity is essential. The qualitative methodology requires the researcher to ask questions like "how" and "why" (Dodgson, 2019). The philosophical worldviews allow the research to apply their worldview with a qualitative approach. Each philosophical framework would require researchers to take different research approaches. The pragmatic researcher utilized an approach that keeps a middle ground (Robson & McCartan, 2016, p. 27).

Pragmatists rejected the idea that social inquiry using a single scientific method could access truths regarding the real world. These pragmatists declared that truth is judged by its consequences. The pragmatic paradigm is useful for guiding research design, especially when a combination of different approaches is philosophically inconsistent (Frey, 2018). Goldkuhl (2012) indicated that pragmatism is concerned with action and change and the interplay between knowledge and action. This makes it appropriate as a basis for research approaches intervening in

the world and not merely observing the world. Creswell (2014) mentioned that the important aspect of research in pragmatism is the problem of the study and the questions asked about this problem instead of focusing on methods. Thus, the researcher finds it effective to use pragmatism to study cybersecurity related issues by focusing on the problem, understanding the real issue and finding out "what works" to solve it.

Discussion of Design

The research can be conducted using 3 methods: quantitative, qualitative, and mixed methods (Creswell, 2014). This study is conducted with a flexible design using qualitative method(s); specifically, a multiple case study design was used. The qualitative research design is appropriate for this study because the aim is to investigate a particular topic through exploring and understanding the research problem (Stake, 2010). The research method provided a better focus on objectivity and the permittance to generalize findings beyond a particular setting (Fletcher et al., 2016). Creswell and Poth (2018) indicated that qualitative research allows researchers to rely on the collection and analysis of data to explain and describe research findings. The qualitative research method provided the research with the tools to propose solutions to the research problem by better understanding how organizations respond to AI-related cyber threats and what effects cyber threats have on the technology business. The researcher decided not to select quantitative research designs due to the common weaknesses in capturing the subtleties and complexities of individual human behavior. In comparison, it is possible to capture it using a flexible design. In the study, the researcher has no intention to capture group aggregates which mainly involve fixed design.

According to Robson and McCartan (2016), "fixed designs are usually concerned with aggregates: with group properties and with general tendencies" (p. 103). Therefore, fixed designs present the danger of ecological fallacy. With fixed design, some problems come under the heading

of reliability. The unreliability of fixed design has various causes, including participant error, participant bias, observer error, observer bias, and types of validity (Robson & McCartan, 2016). In terms of multi-strategy design, the researcher avoided using the design due to the complexities and concerns that may produce disjointed and unfocused research. Regnault et al. (2018) identified some disadvantages in the mixed method, one of them is the application of multi-strategy design that can potentially raise practical concerns when integrating both qualitative and quantitative data as the integration process may require additional resources and time. There are also some uncertainties in mixing two differing paradigms in the same research study. “Some theoretical debate still exists on how - or even whether - quantitative and qualitative paradigms can be mixed” (Regnault et al., 2018). Mason (2006) indicated that multi- strategy design could severely test the capabilities of the researcher due to the complexity of its implementation. Mixed methods design may require more expertise to gather and analyze data and interpret the findings. In the real world, combining different methods requires extra resources and can establish certain constraints caused by practical, political, and resource issues (Mason, 2006). Therefore, the researcher focused on one method to ensure the ease of the data collection process.

Discussion of Method

The specific method for this study is a multiple case study. The design of this proposed flexible qualitative study aims to find answers to the research questions by determining the effects of AI-based technology on cybersecurity and how it affects business strategy and decision-making over time. The multiple case study seeks to understand the situation related to the problem through answering research questions and in-depth examinations of the different cases using archival data (Brown, 2020). It explored the events surrounding the problem by examining the interaction between different components that involve people, activities, and business policies. The research is

conducted on high-tech cybersecurity organizations that are investing in AI to overcome security threats. Stake (2010) stated that the multi-case study is a special effort to examine something having lots of cases, parts, or members. In the study, the researcher followed Stake's approach and defined multiple-case studies as being investigations of a particular phenomenon (or group of phenomena) at several different sites. This does not preclude a multi-case study from being conducted within one organization. Stewart (2012) identified three sequential processes or tracks of the multiple case study analysis. The first stage identifies themes in each of the cases, maintaining situational detail. The second track identifies factors, and the third track is the cross- case analysis, which involves generating a case-ordered descriptive matrix that establishes a basis for comparing the cases on a number of factors.

Qualitative research includes five design approaches narrative, phenomenological, ethnographic, grounded, and case study approaches (Creswell & Poth, 2018). After examining all the research methods and comparing them to each other, the researcher realized that the multi- case study is the most appropriate method for this study and made a choice not to use a single case study due to the significant potential difference between single and multi-case studies in terms of the range and reach of the multi-case study. Stewart (2012) indicated that unlike the single-case study, all cases in the multi-case studies are chosen for their similarities rather than their differences and that multi-case studies are essence comparative. As a multi-case researcher, the researcher is interested in using contrast or variance as a significant research tool for the case under study. Fitzgerald and Dopson (2009) denoted that the multi-case study researcher could examine the differences and similarities between cases within a specific context.

Qualitative research aims to more fully understand the phenomenon studied contextually from the participants' perspective (Creswell, 2014; Creswell & Poth, 2018; Fletcher et al., 2016;

Stake, 2010). Creswell (2014), Creswell and Poth (2018), and Yin (2014) advised that the case study research design is most suitable for researchers to explore a given process within a specific context or bounded situation. A case study researcher's goal is to obtain descriptive content to better understand the phenomenon of interest (Creswell & Poth, 2018). Creswell (2016) suggested the case study design for the exploration of a specific issue. Yin (2014) shared that the use of multi-case studies can produce more robust and compelling results. Mumford et al. (2009) cautioned researchers on the single case study's limitation of generalizability. Therefore, the researcher chose a multi-case study methodology for this study to achieve data saturation and improve the generalizability and validity of the findings.

The phenomenological methodology is not appropriate for this research because participants do not encounter a unique event together, which presents the risk of expanding beyond the limited scope determined for this study. The researcher intends to stay focused on the intended study and within the scope by obtaining information from participants on the negative effect of AI on cybersecurity. According to Bondwe (2019), the phenomenological approach is appropriate to explore the lived experiences of the individuals of a phenomenon, which can be used to study how individuals interact when experiencing AI- related cyber-attacks. However, that is not the primary focus of the study, it is absolutely part of it, but the data collected using the phenomenological approach did not cover the intended topics the researcher intends to cover. Creswell (2007) acknowledged a common challenge of using the phenomenological method, which is the difficulty of bracketing personal experiences, which requires the researcher to decide how to introduce his personal understanding into the study.

Narrative research is an old research tradition. It illustrates individuals' life stories (Lewis, 2015; Morawski & Rottmann, 2016). Creswell and Poth (2018) mentioned that narrative research is

appropriate when studying a phenomenon involving a single person or a small group of individuals, typically two or three individuals. The individual provides his or her unique personal experience for the researcher, researcher record the story and experience of the participant. In this research, the researcher interviewed several individuals, not only a few and collected information from many participants in different businesses across the technology industry in the United States. The intent of this study is not to record a human's story chronologically nor to interview a single or a few individuals to collect data. Therefore, the narrative design is not a good fit for this study.

The ethnographic research method stems from anthropology and sociology, where the researcher explores shared patterns of behavior, language, and actions of a specific sample within the same cultural group over an extended period (Creswell, 2014). According to Creswell and Poth (2018), ethnography researchers conduct research in a "culture-sharing" environment. Ethnographers observe social behaviors and explore patterns of life surrounding a group of individuals (Ting-Toomey & Dorjee, 2018). Grey (2016) indicated that patterns of life include different activities within the cultural cycle. These cycles could be beliefs, dialects, festivities, or spiritual lifestyles. The ethnographic research method is inappropriate for this study because it is designed to examine in detail the cultural characteristics of the work environment, which cannot contribute to gaining a good understanding of the research problem in the case of this study. Therefore, the ethnographic approach to inquiry was ruled out.

The grounded theory research defers from all other approaches as it does not focus on individual/group stories nor highlights shared experiences. It instead aims to generate or uncover a theory (Creswell & Poth, 2018). Creswell and Poth (2018) described grounded theory as a process or action performed by a researcher who seeks to explain an emerging theory of a specific plan. In the grounded theory approach, the researcher grounds the theories that he or she develops in the

data that was collected from individuals or groups who had somehow experienced part of the process or action. Researchers then record and analyze data. Stake (2010) acknowledged that the grounded theory approach focuses on the generation or discovery of a theory. Investigators use memo writing techniques to shape the process and to record and analyze the gathered data (Johnson, 2016). The grounded theory method is appropriate to advance or identify a theory because it considers the perspectives of the research participants to explain a specific process, action, or interaction (Creswell & Poth, 2018). This study does not seek to develop emergent theories about the processes, actions, and interactions carried out by AI and cybersecurity professionals dealing with AI-related cyber-attacks. Therefore, the grounded theory design is not appropriate for this study.

Discussion of Triangulation

The researcher used multiple methods of qualitative data triangulation to address the research questions; in this study, the researcher intends to use triangulation as a research strategy to confirm and validate the quality results of the study (Carter et al., 2014). Robson and McCartan (2016) emphasized that triangulation is a valuable strategy that has many advantages to the study, triangulation enhances the rigor of the research and helps to counter all of the threat of validity. Triangulation achieved objectivity, truth, and validity (dependability and credibility) of research by using multiple sources instead of a single source, which provided the researcher with more insights and enable the researcher to recognize and remove inconsistencies (Fusch et al., 2018).

To study this information systems business problem, the study overcame the weakness or intrinsic biases by applying a combination of several research methods and eliminate the problems caused by using a single method, observer, and theory studies. The researcher used semi structured interviews as a qualitative data collection method pertaining to the effects of AI-related cyber-

attacks on the technology organization in the United States. The results from the datasets collected during the interviews was analyzed independently then compared to each other to determine if results lead to the same conclusions. The use of qualitative data collection methods such as interviews and member checking eliminate bias in the research and is proven to yield accurate and concrete results and findings. According to Nightingale (2019), triangulation is used to enhance the validity of research findings, create a more in-depth picture of a research problem, and interrogate different ways of understanding a research problem. Nightingale (2019) suggested that researchers look for three types of data triangulation: convergence, complementarity, and divergence. Convergence refers to the degree of overlap and accuracy between the data sets collected using different methods.

The complementarity type clarifies the research results by allowing the results from different methods to inform each other. Divergence presents a different set of challenges within the methods. This study ensured that different methods and observers of the same phenomenon produce the same results. Williamson (2017) noted that there are four common forms of triangulation: Data source triangulation which involves using different sources of information to increase the validity of a study. Method triangulation which means the use of multiple methods in the same study to gather data, such as interviews, observations, questionnaires, and documents; theory triangulation involves using more than one theoretical scheme in the interpretation of the case (Guion, 2002). Investigator triangulation which uses or consults several different researchers, either interviewers or observers to provide multiple perspectives. In this study, the researcher used the methodological form of triangulation to develop a comprehensive understanding of the case. The researcher followed a data collection plan that uses multiple data sources to triangulate the qualitative study. Sources included interviews and member check in. The data collection plan

assisted the researcher in obtaining the extra data needed to support the interview findings and reach data saturation.

Summary of the Nature of the Study

After reviewing the research problem and questions, the researcher determined the research paradigm based on the researcher's worldview, the research methodology, and the data triangulation methods for this study. The researcher explored all the primary research paradigms and identified pragmatism as the worldview that constitutes truth, and knowledge which guide the researcher's thinking, beliefs, and assumptions about the study. The researcher determined the design for this study to be flexible design using qualitative method, the research is conducted using multiple case study method for data gathering that helped finding answers to the research questions. The researcher used the methodology to investigate the use of malicious AI to conduct cyber related attacks, the research methodology determined for this study helped exploring and understanding the research problem, it summarized the research process and determined how the research proceeds. The study used data triangulation to address the research questions, the researcher utilized multiple data collection methods for data triangulation, researcher conducted interviews and member checking to ensure the validity of the research results. The research approach determined for this study aimed on understanding the connection between philosophical worldview and research methodology which helped the researcher find better ways to go about investigating the topic. The study cited multiple sources to provide factual assertions for the research methodology, design, and triangulation functions.

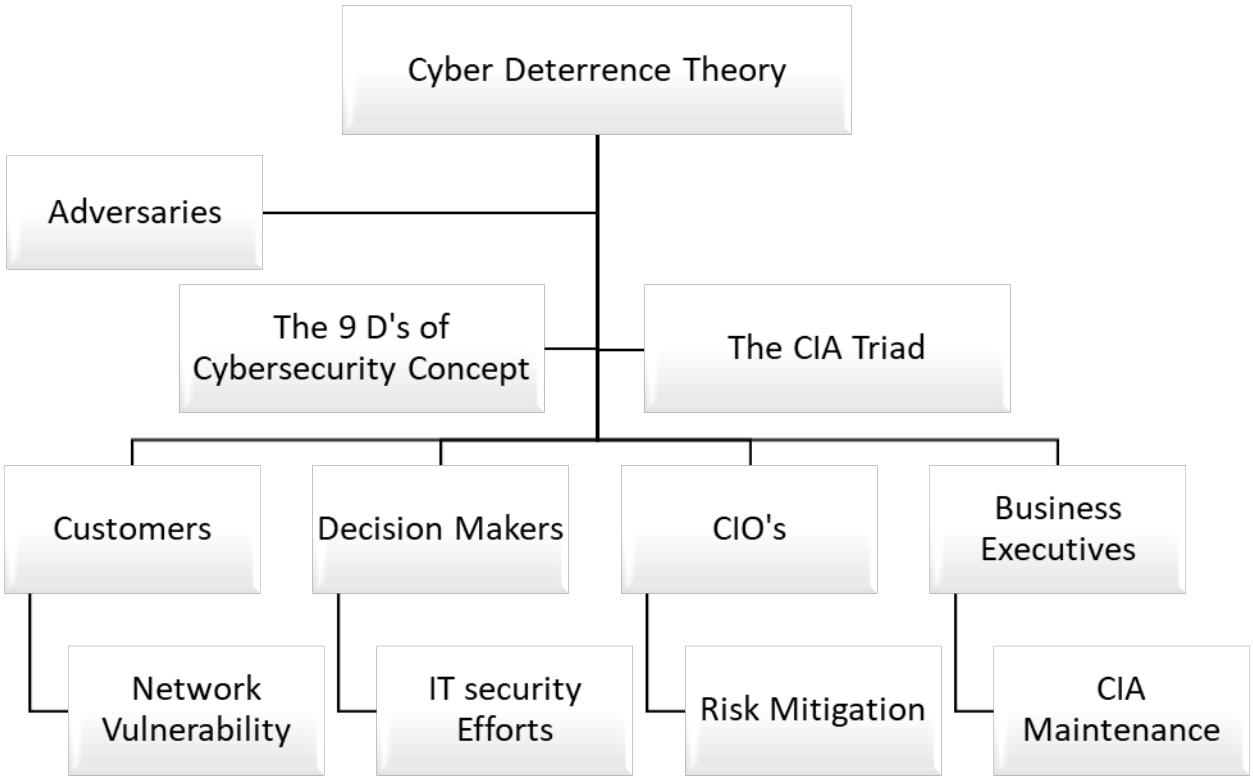
Conceptual Framework

The research framework for this study addressed the aspects of the specific problem statement. It examined the relationships between elements and clarified the conditions surrounding

the problem. This qualitative research framework consists of two core concepts, a theory, several actors, and research constructs. Chen et al. (2014) characterized a research conceptual framework as a visual or written explanation that illustrates either graphically or in narrative form. The major parts that the conceptual framework addresses are the key factors, concepts, or constructs and their presumed relationships. Figure 1. shows the relationships between concepts and flow of action, information, and influence between actors and constructs.

Figure 1

Relationships between concepts.



Concepts

The Confidentiality, Integrity, and Availability (CIA) Triad Concept

For the purpose of this study, the CIA triad is considered the core concept of information

security and is central to the research problem that helped explore the cybersecurity challenges within the technology industry in the United States. The CIA triad consists of three primary concepts in information security, maintaining confidentiality, integrity, and availability of the data is necessary to achieve the cybersecurity goal of protecting information from unauthorized access, unauthorized modification, and unauthorized deletion (Gao et al., 2020).

The confidentiality, integrity, and availability of the data are vital in cybersecurity as it provides essential security features; implementing the CIA triad helps organizations avoid compliance issues, ensures business continuity, and prevents reputational damage. According to Kar Yee and Zolkipli (2021), the purpose of data security and protection is to preserve data integrity and availability for necessary use while maintaining user privacy through confidentiality. The triad achieves the objectives of information security to ensure data protection (Alkhudhayr et al., 2019). The CIA triad is a widely used cybersecurity model that can guide an organization's efforts and policies to keep its data secure (Alhassan & Adjei-Quaye, 2017). The initials stand for the triad on which information security rests.

Confidentiality. Confidentiality is a necessary component of privacy. Technology organizations take user privacy seriously and focus on providing secure services to their customers. Achieving confidentiality ensures that only authorized users and processes can access or modify data. Khidzir et al. (2018) defined confidentiality as the restrictions on using and storing various data types. Confidentiality protects sensitive information from unauthorized disclosure while in transit over a network (Andress, 2014). The concept considers a set of rules and restrictions that limit access to certain types of information and supports the user data as secret, private, and not viewed even by the cloud service provider. Common methods of ensuring confidentiality are data encryption, user identity documents (IDs), passwords, cards, retina scans, voice recognition,

fingerprints, security tokens, and key fobs tokens (Tchernykh et al., 2019).

Integrity. Data integrity involves maintaining the consistency, accuracy, and trustworthiness of information to prevent unauthorized people from changing, altering, deleting, or illegally accessing the data. It ensures that no entity can modify or change the information other than the owner during the creation, transmission, and storage processes. Integrity supports a complete data structure as a fundamental concept of information security (Tchernykh et al., 2019). Measures to ensure integrity include file permissions and user access control are the measures controlling the data breaches in an organization. Common attacks that compromise data integrity include attacks that penetrate the webserver, Man-In-the-Middle (MITM) attacks, salami attacks, trust relationship attacks, session hijacking attacks, and malicious code attacks (Weaver et al., 2013).

Availability. The final leg of the CIA triad is availability; service availability depends on the robustness of the hardware, hardware repairs and maintaining a correctly functioning operating system environment, system upgrades, preventing the occurrence of bottlenecks, etc. (Tchernykh et al., 2019). The term "availability" refers to enabling the authorized users' access to the related assets and information when needed. It is a security service that ensures the constant availability of resources and services to only authorized parties in a timely manner (Khidzir et al., 2018). As Andress (2014) indicated, loss of availability causes several breaks anywhere in the chain that allow users access to their data. Loss of availability can result from different incidents such as power loss, application problems, operating system issues, network attacks, compromise of a system, or other related problems.

The Nine Ds of Cybersecurity Risk Management Concept

Cybersecurity risk management is a tool used by cybersecurity professionals to prioritize

cybersecurity defensive measures based on the potential adverse impact of the threats they are designed to address (Frank et al., 2019). The Nine D's concept is inspired by the department of defense's three tenets of cybersecurity. It is one of the four cybersecurity concepts that enable the evaluation of protection systems, including analyzing defeats by known exploits and predicting likely vulnerabilities. According to Wilson and Kiy (2014), the use of the Nine D's concept is demonstrated as analysis tool that permits ranking of the expected effectiveness of some potential countermeasures; it presents practical defensive tactics in an easily remembered scheme. Wilson and Kiy (2014) identified the nine Ds as Deter attacks, Detect attacks, Drive up the difficulty, Differentiate protections, Dig beneath the threat, Diffuse protection throughout the payload, Distract with decoys, Divert attackers to other targets, and Depth of defense.

Starting with Deter attacks sub concept, deterrence is the first line of defense. It can be used as a measure to reduce an attacker's will to conduct an attack, such as threats of legal action or other punitive measures (Wilner, 2017). The second D is Detect attacks. Rehman et al. (2021) acknowledged that detection of malicious activity is necessary if affirmative reactions are part of the defensive strategy and proactive, automated defenses are to be used. Examples of detection methods are a password failure counter that locks a user account and monitoring for excessive network traffic. Drive-up difficulty involves using technical protection measures (TPMs) to make attacks more burdensome by driving the level of difficulty beyond their ability to cope (Wilson & Kiy, 2014). In differentiating protections, Wilson and Kiy (2014) emphasized that each defensive protection system must focus on one or more specific classes of threats. Threat classes are piracy, tampering (altering functionality), and reverse engineering (discovering buried IP in a distributed executable program). Dig beneath the threat involves implementing hardware-based protections as an effective measure against attackers. Wilson and Kiy (2014) indicated that protection at a lower

layer than an expected cyber-attack might be able to defeat the attack, even if it was an expert-level attack. In diffuse protection throughout the payload, Wilson and Kiy (2014) suggested that cyber attackers should face multiple layers of encryption and access controls and not only a single layer. The goal of diffusing protection throughout the payload is to leave the hacker with limited options, either bringing along functioning protections or else forfeiting the payload value. Next is distract with decoys, there are two factors that make the attackers give up, frustration or the feeling of success. Distracting with decoys is an effective protection strategy because it encourages a false belief in success which triggers frustration and the thought of failure. An example of distraction with decoys is the cybersecurity honeypot (Wilson & Kiy, 2014). The next sub concept is divert attackers to other targets, security system implementers have an option to divert the attackers' attention to a more attractive target elsewhere. The way to accomplish this protection strategy is to persuade an attacker to target some other target (Sawyer & Hancock, 2018). The last D is depth of defense. The concept of defense in depth is valuable for use against sophisticated hackers. Rahman et al. (2020) defined depth in defense as a multilayer defense strategy where several independent countermeasures are implemented in the device to provide aggregated protection against different attack vectors.

Theories

Cyber Deterrence Theory

Deterrence is considered a traditional security theory that could be superimposed on cyberspace. The objective of deterrence theory is to eliminate attacks by making the costs and consequences outweigh the benefits. The cyber deterrence theory guided the research on how cybersecurity threats in AI-based technology can impact a business's strategy and decision-making (Kramer et al., 2009). As indicated by Haley (2013), the objective of deterrence theory is to

eliminate attacks by making the costs and consequences outweigh the benefits. Implementing the deterrence concept requires two essential factors. The first is to have a strong defense. Kramer et al. (2009) suggested that if the defense is sufficient to make an attack exceedingly difficult, an opponent might choose to stand down; this first objective is considered a practical solution to the most cyberattacks in the cyber realm, The second is the retaliation factor, if successful aggressors face severe retribution following their malicious actions, other aspirants may choose not to attack at all.

Mazanec and Thayer (2016) indicated that the concept of deterrence is about keeping an opponent from doing a harmful activity by making a threat of unacceptable consequences. Mazarr (2021) suggested that deterrence can be done in two forms - deterrence by punishment (the power to hurt) and deterrence by denial (the power to deny victory); keeping someone from conducting a malicious activity may be brought about by threatening unacceptable punishment if the action is taken, this is called deterrence by punishment (Mazanec & Thayer, 2016). Deterrence by denial, on the other hand, seeks to deter action by making it infeasible or unlikely to succeed, thus denying a potential aggressor confidence in attaining its objectives (Mazarr, 2021). Mazanec and Thayer (2016) acknowledged that deterrence by denial convinces the adversaries that their objective will be denied to them if they attack. Both forms of deterrence may apply in the case of an AI-related cyberattack against the technology organizations in the United States.

According to Mazanec and Thayer (2016), the theory of deterrence was developed early in the Cold War between the United States and the Soviet Union by academics coming to explore the novelty of the political and military impact of nuclear weapons; the deterrence concept was able to prevent a world war by allowing politicians and decision-makers to understand the risks associated with nuclear war. According to Haley (2013), thousands of cyberattacks occur per day, suggesting

great difficulty in distinguishing serious threats from minor ones; worst of all for technology organizations in the United States, the United States is specifically vulnerable to cyberattacks due to the pervasiveness of advanced technology in every aspect of its citizens' lives, as well as the American tendency to value freedom over security and innovation over- regulation. Bendiek and Metzger (2015) acknowledged that deterrence theory has long been considered a valuable concept to achieve restraint from attacks.

Goodman (2010) has identified organizations can employ eight elements of deterrence to keep adversaries from attacking the interest: an interest, a deterrent declaration, denial measures, penalty measures, credibility, reassurance, fear, and a cost-benefit calculation. a deterrent declaration serves as a warning to the opponent, "Do not do this, or else that will happen." The consequences of proceeding with the act can be either denial measures, penalty measures, or both. Maintaining credibility and reassurance is crucial in the deterrent declaration. It emphasizes the truthfulness of the declaration. Fear is another essential element as it deters potential adversaries from taking undesirable actions. All the seven elements mentioned above factor into the cost-benefit calculation that calculates the benefits and costs of action versus the benefits and costs of restraint.

Actors

Chief Information Security Officers

Also called the VP of security. The primary role of CISOs is to monitor and analyze the risks that a company faces in order to guarantee data and information protection. CISOs are responsible on organizations information and data security. Information security tasks include security operations, data loss and fraud prevention, identity and access management, cyber risk and cyber intelligence, security architecture, investigations and forensics and governance (Islam et al.,

2021). CISOs are effective actors in this research due to their nature of responsibility the solely focus on internet security.

Customers

Customers are the affected actors in case of cyber-attacks, that makes them one of the main actors in this research. Customers' data could be compromised due to a cybersecurity vulnerability (Lee, 2021). Customers expect service providers to protect their data from any cyber threat. Companies strive to gain the trust of customers to keep the business going.

Cyber-attacks and data breaches not only cause financial losses to companies, but it can also damage its reputation which result in losing customers (Ameen et al., 2021).

Hackers/Cybercriminals

Hackers threaten businesses' data, which is the most valuable asset to the organizations. Hackers, cybercriminals, and other state/non-state actors considered the offensive action initiators. Therefore, it is appropriate to list them as important actors in this study. Whether it is Malware attack, phishing attack, denial of service attack or man in the middle attack. Hackers have several reasons to initiate such attacks against companies and firms. Depending on their motive and affiliation (state/non-state), their financial interest is the most common reason (Kennedy et al., 2019).

Organization's Decision-Makers

Decision-makers are key players in the companies' security. They make final decisions that lead to counter cyber-attacks and incursions. Decision makers determine the organization's strategy and have an effective influence over functions and operations. Business executives have the authority to determine the company's future steps (Liu et al., 2020).

Constructs

Business Executives

Managers and executives must have a good understanding of cybersecurity within the organization (De Arroyabe et al., 2023). Business leaders have the authority to make an articulated decision on Cybersecurity based on the firm's financial standing. Executives responsible on establishing company policies and procedures for all departments to include the organization's security department. They have the authority to make decisions on the organization's security posture (Mangelsdorf, 2017). Camélia and Nadia (2022) mentioned that executives must be continually vigilant about cyberthreats despite their job function and responsibilities. Executives ensure that the organization adopt appropriate cybersecurity measures to manage and control the risk of cyber-attacks against its networks.

IT Security Efforts

De Arroyabe et al. (2023) assumed that cybersecurity investment is a strategic decision in organizations. Their study explores how cyber-attacks drive investment in cybersecurity systems. Investing efforts, time, and resources to enhance IT security posture and reduce attack surface can save organizations time and funds. According to De Arroyabe et al. (2023), "One of the greatest challenges that organizations face nowadays is determining the level of investment in cybersecurity systems that provides an adequate level of protection" (p. 1). Building a reliable security network is more effective than recovering from a significant cyber-breach. Companies should increase their cyber awareness by educating their employees. Cybercriminals look for vulnerabilities to gain access to systems. Lack of cybersecurity knowledge within employees increase the vulnerabilities of organization's system. Raising cybersecurity awareness is as important as investing in IT security infrastructure (Usman et al., 2020).

IT Security Professionals

IT security professionals help business executives make major decisions based on facts that stem from practical knowledge in the cybersecurity field (Mangelsdorf, 2017). Organizations must enhance cybersecurity teams' incident response to build an effective cybersecurity defense against the cyber-attacks that are increasing and evolving rapidly. Security teams considered a strong line of defense to the organization and providing cyber incident exercises and training would provide skills and knowledge required to handle real-time cyber-attacks in various scenarios. Due to the lack of real-life scenarios in the cybersecurity world, it is challenging to educate cybersecurity teams on responding to all types of cyber-attacks. Therefore, the continuous efforts to building robust defensive skills within the security team helps countering different types of attacks (Alothman et al., 2022).

Network Security Vulnerability

Hackers target weak security systems; organizations with robust IT security have way less chance to be targeted by hackers (Walkowski et al., 2020). Companies must maintain network and data security and ensure to protect the legitimate interests of customers. They key factors of network security protection is the detection of unknown network security vulnerabilities. The ability to detect security vulnerabilities is a crucial part of the network defense system, it can prevent major security incidents and reduce cybersecurity threats. Cybercriminals exploit network security vulnerabilities to conduct remote attacks. Common network intrusions resulting from exploiting high-risk vulnerabilities include cross-site scripting, denial of service attacks, and SQL injection attacks (Luo, 2020).

Risk Mitigation

To ensure a secure network, companies must take the necessary measures to reduce

cyber-related risks and have the right risk assessment tools to predict the types of future attacks. Zadeh et al. (2020) indicated that today's businesses must make difficult decisions regarding the mitigation of cyber-attacks risks. Cyber-attacks risks and threat have different types, including physical threats, human threats, communication and data threats, and operational threats. Cyber-attacks and data breaches have negative consequences on businesses, including negative changes to market value, share price, and stock market return (Zadeh et al., 2020).

Relationships Between Concepts, Theories, Actors, and Constructs

A model of conceptual framework relationships between concepts, theories, actors, and constructs appears in the conceptual framework part of this study. Each concept and theory helped address the research questions by guiding the interpretation of the data collected. Applying the Confidentiality, Integrity and Availability triad concept guides the interpretation of data collected from research questions concerning how technology organizations can maintain secure networks and information systems against AI-powered cyber-attacks (Gao et al., 2020). Actors determined in the study have a direct impact on the cybersecurity decision-making process. The Nine D's cybersecurity risk management concept guided data from research questions related to risk management and mitigation; In this case, security teams, decision- makers and CIOs determine risk management strategies and how to react in case of a cyber breach (Usman et al., 2020). These two concepts help inform how technology organizations deal with the rapid development of AI and ML in the cybersecurity field and its threat against organizations' security systems. Deterrence theory supported the two above concepts by identifying methods to deter cyber-attacks and ways to deal with adversaries. Deterrence theory provides measures decision-makers can take to change attackers' behaviors and actions before the attack occur (Quackenbush & Zagare, 2016). Deterring attackers from using sophisticated AI technology and tools will achieve data confidentiality,

integrity, and availability. It will also help reduce cyber-attacks risks by dealing with hackers, cybercriminals, or even state actors, the root cause of the problem (Wilner, 2017). The three interrelated concepts and theories comprise the conceptual framework that guides the development of themes from collected data, interpretation of data, documentation of research findings, and support research conclusions.

Summary of the Conceptual Framework

The conceptual framework of this study shown in Figure 1 is designed for viewing the risks and threats technology organizations face as a result of using AI for malicious purposes that could lead to negative outcomes for the organization and its customers. The conceptual framework illustrates how the concepts interact within the cybersecurity domain. It identifies the relationships between constructs and actors; it also determines the outputs and how research concepts and theories influence actors. The researcher designed this conceptual framework to better understand the research problem and help form potential themes and perceptions discovered through the research design and method. The research framework of this study guides executing research as designed to resolve the research problem. Alignment amongst research problem, purpose, questions, nature of the study, and conceptual framework supports the qualitative multiple case study further exploring AI-led cyber-attacks as an academic field of study.

Definition of Terms

The following term definitions aid understanding of this multiple case study's research design, findings, and conclusions.

AI (AI). The ability of a digital computer or computer-controlled robot to perform tasks commonly associated with intelligent beings by developing systems endowed with the intellectual processes characteristic of humans, such as the ability to reason, discover meaning, generalize, or

learn from past experience (Copeland, 2022).

Attack surface. The set of points on the boundary of a system, a system element, or an environment where an attacker can try to enter, cause an effect on, or extract data from that system, system element, or environment **(**Ross et al., 2019).

Attack vector. A path or means by which a malicious actor gains access or delivers malware onto a computer or network (Ullah et al., 2018).

Cyberspace. The interdependent network of information technology infrastructures includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries (Ross et al., 2019).

DDoS attack. A distributed denial of service attack is a type of attack in which devices are attacked from multiple sources in a distributed manner, creating a denial of service to users (Yin et al., 2018).

Deep Learning. A subset of ML, deep learning incorporates computational models and algorithms that imitate the architecture of the biological neural networks in the human brain, also called ANNs or artificial neural networks (Jakhar & Kaur, 2020).

Intellectual property (IP). Any patent, trademark, copyright, design right, registered design, technical or commercial information, or any other product of the human intellect that the law protects from unauthorized use by others (Bently, 2012).

Internet of things (IoT). A network of physical objects that connect anything with the internet based on stipulated protocols through information sensing equipment to conduct information exchange and communications to achieve smart recognitions, positioning, tracing, monitoring, and administration (Patel et al., 2016).

ML (ML). The capacity of systems to learn from problem-specific training data to

automate the process of analytical model building and solve associated tasks (Janiesch et al., 2021).

Malware. Malware is short for "malicious software," refers to any intrusive software developed by cybercriminals or "hackers" to steal data and damage or destroy computers and computer systems. Examples of common malware include viruses, worms, trojan, spyware, adware, and ransomware (Cisco, 2022).

Zero-day attack. A computer attack exploits an exposed or an undiscovered vulnerability to affect/damage networks or programs. The term "zero-day" refers to the number of days available to the software or the hardware vendor to issue a patch for this new vulnerability (Al-Rushdan et al., 2020).

Assumptions, Limitations, and Delimitations

The assumptions, limitations, and delimitations are essential to improving the quality of a research study, as they could affect findings and conclusions and provide a lens to the data presented in the research. The three elements help plan the study by clarifying the restrictions that may occur when conducting the research, which enable the researcher to adjust the method accordingly. Each element leads to identifying potential weak points within the research project. Assumptions discover any underlying beliefs held by the researcher; they can influence the research for which the researcher somewhat has no control, such as participants' knowledge level of the problem (Berg & Lune, 2017). Limitations help researchers clarify the constraints of the selected methodology and design of the study. Dixon (2015) acknowledged that limitations exist when the researcher cannot anticipate the honesty level of interviewee responses. Delimitations are under the researcher's control; they are characteristics that limit the scope and define the research boundary (Simon, 2011). Delimitations enable researchers to articulate what the study will include and exclude (Simon & Goes, 2017).

Assumptions

In research, some assumptions are accepted as true or certain to happen with proof (Bonell et al., 2013). Assumptions are somewhat out of researchers' control but without them, the study becomes irrelevant. Since this study used triangulation as a data collection approach, the researcher assumed that the participants have experience in the information security field and are knowledgeable about the AI trends in the cybersecurity world and are transparent when answering the research questions (Dixon, 2015). This assumption helped researchers get closer to the truth through data triangulation by discovering themes from the data gathered from several sources. The themes discovered from data collection identified the effectiveness of AI in the cybersecurity field (Fusch et al., 2018). The researcher mitigated the issue by interviewing cybersecurity professionals that have a strong background in AI technology to make sure the participants have knowledge in both fields. Additionally, the study assumed that participants will be transparent and answer the research questions to the best of their ability without fear of reprisal or harm to their reputation and organization. Petrova et al. (2016) indicated that providing a safe environment to research participants by maintaining their anonymity and confidentiality will ensure quality and honest responses to the research questions. to guarantee. Simon (2013) stated “A classic example is the assumption that participants in a study will answer survey or interview questions honestly and factually.” Since it would take considerable time and effort to validate answers of each participant, we assume honest responses. The researcher also assumes that the data gathered from interviews would accurately depict what is happening in reality (Petrova et al., 2016). The researcher’s strategy to mitigate data accuracy issue is to seek answers of real-world scenarios by asking field specific questions. Assumptions are so basic yet a critical element; without assumptions, the research problem itself could not exist or progress. Lastly, the researcher implemented specific

procedures to preserve the anonymity and confidentiality of each participant in the research to create a safe environment that allows participants to express their honest opinions and not those of another (Leedy & Ormrod, 2019).

Limitations

Limitations are potential weaknesses in the research study and are out of the researcher's control. "A limitation associated with qualitative study is related to validity and reliability, because qualitative research occurs in the natural setting it is extremely difficult to replicate studies" (Wiersma, 2000, p. 211). Price and Murnan (2004) defined limitation as the systematic bias that the researcher did not or could not control and could inappropriately affect the study results. They categorized limitations into two major categories, threats to internal and external validity. A common threat to the internal validity of a study occurs when participants do not respond truthfully to the research questions. In other words, answer in a socially desirable way. Several other threats to internal validity include maturation bias, confounding variables, attrition of subjects, statistical regression toward the mean, and multiple tests of significance (Price & Murnan, 2004). The first limitation of this study is that information security and AI experts provide inadequate data due to their limited knowledge or experience of the involvement of AI in cybersecurity field. To mitigate the risk of inadequate data, the researcher focused on the knowledge factor when selecting the participants. The second limitation is that AI applications and technology continue to evolve in the information security world, which might limit participants' knowledge in the new trends and technology. The researcher avoided interviewing participants with lack of knowledge in the field and ensured that participants are aware about the latest trends in automated cyber-attacks. The third limitation is the amount and type on information technology experts willing to share with the researcher without compromising the privacy of their organizations and clients, the researcher

sought statistical data pertaining to AI-related cyber-attacks on the organization, employees are limited to what they can and cannot share with the researcher. Since this is a multiple case study, the results were specific to the technology organizations. To eliminate this risk, researchers implemented a risk mitigation plan and provide participants with nondisclosure agreements to the legality of the process.

Delimitations

Delimitations are boundaries set by the researcher in a study (Moed, 2010). As opposed to limitations, researchers control delimitations and are defined by Price and Murnan (2004) as a systematic bias intentionally introduced into the study by the researcher. Delimitations require challenging the researchers' assumptions and openly exposing shortcomings that might have been better tackled (Theofanidis & Fountouki, 2018). Examples of the delimitations that the researcher can control are the study for a particular age group, sex, race/ethnicity, geographically defined region, or some other attribute that would limit to whom the findings are applicable. By setting delimitations, researchers fence the study. The specific methodology and variables in the research set a boundary on what findings can ascertain. Technically, factors that delimit the study include the research questions, variables of interest, theoretical perspectives that the researcher adopted, as well as the population the researcher chooses to investigate.

Since the delimitation defines the boundaries and limits the scope of the research study, the researcher’s mitigation strategy is to limit this study to technology organizations located in the United States. The delimitation of the study is the sample size, the type of business, the location of organizations studied, the data collection methods and the type of participants to be cybersecurity professionals with knowledge or experience relating to AI-based cyber-attacks. All of the mentioned delimitations were controlled by the researcher to ensure data validity and reliability.

The data triangulation approach is used in this study to ensure data saturation. This type of the business is limited to technology companies to control the information received and appropriately direct the findings. For interview accessibility, the researcher limited the participant population to be in the United States.

Significance of the Study

The significance of this qualitative doctoral study resided in the effort to discover effective cybersecurity defenses for technology companies against malicious AI that adversaries use to automate cyberattacks and conduct data breaches. This research study addresses a unique challenge resulting from emerging technologies and innovations by exploring adversaries' advancement using AI capabilities to promote attacks against multi-billion-dollar technology organizations. High-tech companies and the information security field can benefit from the findings of this research study. Initially, the research findings may benefit cybersecurity decision-makers in implementing best practices to detect and deter these high-level threats. The genesis of this research study exists in the increasing pace of technological advancement, specifically in the AI and ML domain, creating unanticipated internet security questions technology decision-makers confront that result from technical innovations. The importance of this multiple case study incorporates understanding how the outcome of AI-powered cyber-attacks impacts organizational reputation, finances, and intellectual property in the context of a technology services company. The results led to an increase in the understanding of the new era of cybersecurity in cyberspace as the attack surface is in a continuous expansion. The study provided useful insights into the risk of this emerging technology and how organizational decision-makers recognize it and deal with it. The rationale for this case study includes current academic literature that does not clearly articulate the effectiveness of AI applications in launching devastating attacks against large firms. The findings

and conclusions of this research study illustrate the current and future challenges presented by AI and encourage further study of this research problem.

Reduction of Gaps in the Literature

While there is a large amount of scholarly literature on traditional cyber-attacks, data breaches, and hacking, there is little research on how the use of ML enables threat actors to develop a deeper understanding of the tools and controls technology companies use to reduce attack surface to prevent them from conducting future attacks. Brundage et al. (2018) acknowledged that while countless of AI and ML beneficial applications are being developed and can be expected over the long term, less attention has historically been paid to the ways in which AI can be used maliciously. This study sought to help fill in the gaps in the landscape of potential cybersecurity attacks from malicious uses of AI and ML technologies and how to use the same technology to prevent and mitigate these attacks. This study's findings may curtail the existing gaps in understanding how adversaries can take advantage of automation to attack technology companies' networks and gain access to important information pertaining to the company. Since AI is fairly new in the cybersecurity field, some researchers have explored the rationales of using ML in detecting and preventing cyber-attacks, but limited studies have been conducted to reveal its malicious use of it by cybercriminals and threat actors. There is also little information shown as to what AI and ML tools and techniques adversaries utilize to attack businesses and whether adversaries have the capability to develop these tools without relying on their availability to the public. As well as how organizations leverage AI as a core component of their security operations. The percentage of the AI-based cyber-attacks that targeted technology organizations is not surveyed either. The researcher sought to bridge the gaps through this study.

This multiple case study added to the understanding and practical application of

cybersecurity best practices during the period of adopting AI techniques in the internet security domain. The unique research philosophy and conceptual framework of this study bridged the gap in the current academic literature by addressing the research problem. The researcher utilized a pragmatic philosophical paradigm to conduct the research in an innovative and dynamic way and find solutions to research problems and support an interpretation of findings within a biblical worldview. The researcher incorporated operational decisions based on "what will work best" in finding answers to the research questions. The conceptual framework of this study distinctively applied pragmatic research philosophy through exploring cybersecurity concepts related to the research problem. The research uniquely linked the vulnerabilities of cyberspace with the advancement of AI technology.

Implications for Biblical Integration

As Christian researchers, we must have a relationship with God and not just have a belief in God and Jesus Christ (Fambro, 2016). Fambro (2016) pointed out that every Christian researcher should seek spiritual significance and have three distinct qualities, which are a spiritual calling, prayer with God on what to research, and a Christian worldview. Being different than the world and having a higher standard, one that is accountable to Biblical principles, is what sets a Christian researcher apart from a typical researcher. When work becomes difficult, we need to understand that it is part of the curse of the fall in Genesis as well. "By the sweat of our brow," and in spite of thorns, we will eat our bread. We cannot take sinful shortcuts; we must remain faithful to God and His Laws, even in difficult situations (Keller & Alsdorf, 2012). As we live in the world, both at work and also at leisure, Christians exist in an environment that generally gives little or no thought to Christian or even spiritual things. It is therefore vital that the Christian academic tries live by standards that assert the need for him to act in a more Christ-like way and to make this way plain to

those around him. Peter 2.12 “Live such good lives among the pagans that, though they may accuse you of doing wrong, they may see your good deeds and glorify God on the day he visits us.” For the Christian academic, knowledge of the Lord ought to be at least as important as the academic knowledge which is possessed. That spiritual knowledge should say a great deal to the academic about how he conducts his life and work. He works that the Christian academic should involve not only passing on knowledge but also the greatest care in searching out and understanding that knowledge for himself in preparation for the task. For the Christian academic, knowledge of the Lord ought to be at least as important as the academic knowledge which is possessed. That spiritual knowledge should say much to the academic about how he conducts his life and work.

The biblical theme of creation influences the perception of computing and information technology concepts (Anderson, 2016). Theologies always believe that information technology machines can replace the work of men. The controversy on whether to integrate information technology thus becomes an increasing concern as the problems that border the moral ethics and the Christian faith in cyberspace are the cornerstones of biblical considerations. The question of whether God was concerned with information technology, or the tool is simply used to fulfill the mandates of the devil continues to be controversial (Williams, 2017). This field is seeking the permission of the biblical concepts to permeate all human endeavors in the use and application of information technology. People continue to fear and be anxious about the relationship between theology and information technology. This paper, therefore, makes the subject of information technology using biblical concepts an exciting theological dissertation.

The scriptures in the Bible do not directly mention the word ‘technology' or ‘information technology.' However, these are inferred from God's spoken words inscribed in the Bible (Hutchings, 2017). The first biblical context views technology as the things that were revealed in

the book of Colossians Chapter One, verses 16 to 17. This scripture states that God created the whole world through Jesus Christ and for all humankind. This implies that any technological invention established today will continue to be invented in the future, within the knowledge and the authority of Jesus Christ. Information technology has increasingly become a dormant way of communicating to the Lord and doing things on earth that are not in accordance with biblical teachings. The Bible states that all things should be created for the Lord and through him.

Benefit to Business Practice and Relationship to Cognate

Cybersecurity is one of the most critical components of information systems. At the same time, AI plays a significant role in the future of information systems, including information security as a growing technology. Information systems are all about protecting information, which generally focuses on the information's confidentiality, integrity, and availability (CIA). When it comes to achieving these three goals, it became necessary for business decision-makers and IT professionals to invest in cybersecurity tools that enable security teams to counter the use of AI and automation in conducting data breaches and malicious activities that could cause serious financial damage to businesses. Information security ensures the prevention of unauthorized access, counter threats, confidentiality, disruption, destruction, and modification of business information. Information security protects an organization's data, which is secured in the system from malicious purposes. The research problem directly relates to the information systems cognate, as addressing the problem requires understanding the nature of AI-related cyber-attacks and its role in negatively impacting the business process in the technology sector in the United States.

The technology sector is a vital component of the economy in the United States, it provides services to all other sectors. Regarding security, the technology sector leads

cybersecurity efforts and innovation, making it a value target of cyber-crimes. Due to the technology sector's responsibility, technology organizations decision-makers need to adopt effective strategies for cyber protection. This research is intended to provide technology organizations with a better understanding of the threats AI-related cyber-attacks pose on the business and customers, and the most effective business practices to protect their data from AI bases cyber-attacks. Geetha and Thilagam (2021) classified AI-related attacks based on attack vectors and can be identified at three different layers: Hardware, Network and Application. Attack vectors represent the vulnerability exploited by an adversary to gain access to a network or computer system to perform malicious actions. One of the benefits to business practices is the use of deep learning technologies in cybersecurity analysis and intrusion detection. Deep learning techniques are widely used for malware analysis and finding unforeseen threats because of malicious software (Geetha & Thilagam, 2021).

Summary of Significance of the Study

The study provided critical data that acknowledges the threat of AI in cybersecurity through conducting business research on the technology businesses in the United States. This information relates to the field of information systems because information security affects businesses in many aspects including daily operations; non-secure environment can cause major financial losses by disrupting business operations, intellectual property loss, or customer trust loss. This research study sought to reveal appropriate business practices to deal with automated cyber-attacks against the technology sector. The research focused on the security aspect of the information technology field. It fills the gap in the current academic literature by closely examining the growth of AI technology in the cybersecurity field. It is essential to note that the biblical worldview must be applied and incorporated into the research study. The section also

highlighted the benefit of this study to the business practice and its relationship to information systems cognate.

A Review of the Professional and Academic Literature

The purpose of this literature review is to investigate the underlying problem of how cybersecurity threats in AI-based technology can impact a business. This study has extended the published literature on the dark side of AI that plays a significant role in today's internet security by defining the conceptual domains of cybersecurity. The cyber deterrence theory revealed common themes of cyber-attack prevention and provided the reasoning behind attackers' behaviors and effective measures to curb AI-related cyber threats. The researcher reviewed the effectiveness of two cybersecurity concepts and one theory. The two concepts of the study complement the cyber deterrence theory. The CIA triad and the Nine Ds of cybersecurity concepts drew a clear picture of how to shrink the attack surface to avoid advanced cyber-attacks powered by AI technology. Since the cybersecurity field has evolved with technologies like AI and ML over time, attackers' approaches to committing malicious attacks and data breaches have also progressed throughout the years. The researcher specifically addressed the tech sector, considering that it is ground zero for cyberattacks for different reasons, including the very valuable information it has and that employees of the tech sector tend to be early adopters of new technologies that are still growing and are especially vulnerable to cyber-attacks and exploits.

In addition to exploring the harmful side of AI and ML, this literature review intends to identify the effectiveness of AI applications and cybersecurity in the war against cybercrimes by identifying some business practices that help organizations prevent the risk of having to deal with the consequences of cyber-attacks. The researcher examined four business practices to support the literature review: Employees' cybersecurity awareness and compliance, using ML algorithms

to improve cybersecurity, the adoption of AI in cloud computing security, and patching management. Business practices included in this study provide tools and measures to prevent AI-based cyber-attacks and show how to employ the same advanced technology used by adversaries to combat cyber threats. The related studies section of this literature review presents different perspectives and opinions from multiple scholarly reference materials, not just the viewpoint that supports the researcher's perspective. The literature review concludes with anticipated and discovered themes that draw AI as a double-edged sword that can harm the technology sector just as much as it is to any other sector. Lastly, a summary of the discoveries from the professional and academic literature review.

Business Practices

Improving Employees' Cybersecurity Awareness and Compliance

Due to the increase of reliance on information technology by employees in today's business processes, the strategic interests of businesses have never been more vulnerable to cyber breaches and threats. This weakness can lead to catastrophic consequences, including the leakage of intellectual property and trade secrets, as well as the disruption of mission-critical operations and systems (Bada et al., 2019; Willison et al., 2018). Kemper (2019) suggested that employees are categorized as the main vulnerability of an organization despite the scale and the size of the business. In order to reduce cyber-attack risks, an organization should consider investing in employees' cybersecurity training and awareness. To achieve that, organizations must devise creative methods to engage and encourage employees to actively contribute to the organization's information security.

Building a cybersecurity organization culture is a successful investment that may save the organization huge damages. Kemper (2019) believed that one effective way to raise employees'

awareness is to create a cybersecurity policy and compliance plan to educate employees on following security best practices. Cyber security in the workplace is what people struggle with when it comes to cyber threats, which makes employees the most significant vulnerability and number one threat to the business. Employees' vulnerability to cyberattacks tends to increase with the evolving cyber threat landscape: cyber attackers have gotten smarter and more capable of equipping themselves with cutting-edge technologies such as AI and ML and are continuously presented with new attack surfaces, part of the reason is the embrace and advancement of the Internet of things (IoT). Kemper (2019) suggested that to avoid employee threats, organizations must boost employees' awareness and compliance by using cyber security initiatives among employees.

Zakaria et al. (2007) argued that building a strong cybersecurity culture helps to improve employees' security behavior. While Dojkovski et al. (2010) acknowledged that building a strong cybersecurity culture is important to prevent cyber breaches resulting from employees' non-compliance with cyber organizational guidelines. Da Veiga et al. (2020) argued that organizations must take a comprehensive approach to develop a cybersecurity culture in which security is "everyone's responsibility" and where doing the right thing is the norm. Therefore, the need for a comprehensive framework and guidelines to assist organizations in building a cybersecurity culture was recognized early in the literature (Alshaikh, 2020). Alshaikh (2020) acknowledged that recent security reports show that a significant proportion of cybersecurity breaches and incidents stemmed from employee noncompliance with organizational cybersecurity standards and policies.

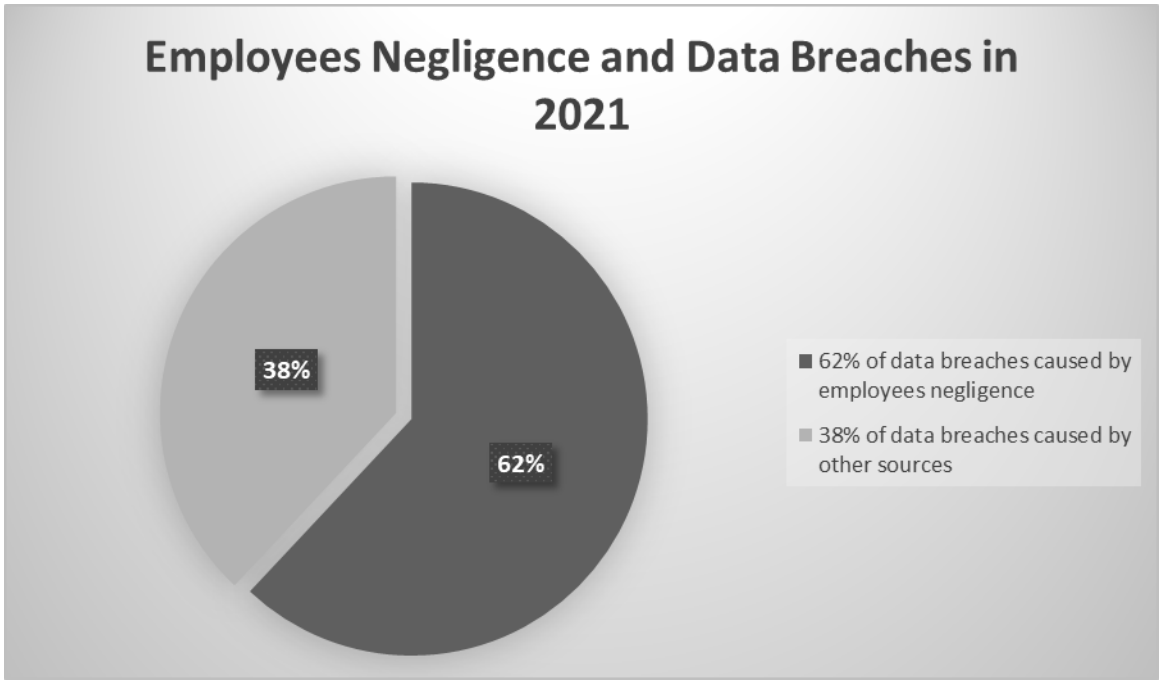
Kessler et al. (2020) indicated that although the popular press often attributes data breaches to external hackers, most breaches are the result of employee negligence and failure to comply with information security policies and procedures. According to Gioulekas et al. (2022), "Cybersecurity

culture denotes the combination of attitudes, behaviors, knowledge, and awareness the organization's personnel display about common cyber risks and threats to protect the information assets." It is important to initiate education programs to raise employees' sense of responsibility and cultivate organization personnel's culture. Employees' awareness of the policies and procedures can play a major role in protecting organizations' data when processing sensitive information in daily business operations, thus preventing attacks or leakages. Hegwer (2017) considered employees as the first line to defend the organization; at the same time, one employee that is not aware of the risks of cyber-attacks may cause significant losses to the organization, in addition to making the organization an easy prey for attackers and infiltrators, 90% of all successful electronic attacks are the result of information provided by employees without their knowledge.

Hegwer (2017) added that a recent benchmark survey conducted by the Ponemon Institute concludes that cyberattacks have surpassed employee negligence as the main cause of data breaches. The data breach can cause significant financial damage to the business. According to the 2022 Ponemon Cost of Insider Threats Global Report, 62% of all insider data breaches resulted from employees' negligence in 2021. Figure 2 shows the percentage of data breaches resulted from employee negligence compared to the other sources.

Figure 2

Data breaches caused by employee negligence in 2021.



Kelly (2020) indicated that employee negligence or malicious acts accounted for two- thirds of cyber breaches. He also acknowledges that better people-management protocols can help prevent cyber-attacks, saving American companies millions of dollars annually. To be specific, the majority of cyber-attacks are estimated to cost the average American business more than $15 million every year. Li et al. (2019) acknowledged the importance of employees' awareness organization's information security policy and procedures; awareness makes employees more competent to manage cybersecurity issues and react to them than employees who lack knowledge of cybersecurity policies. Li et al. (2019) suggested that employees' cybersecurity compliance behavior is positively affected by the organizational information security environment, which impacts employees' threat appraisal and coping appraisal abilities.

Utilizing ML Algorithms to Improve Cybersecurity

According to an article written by Balbix, an advanced InfoSec company that uses the

power of AI to automate organizations' cybersecurity posture; analyzing cybersecurity posture is no longer a human-scale problem, and since attackers are ahead of the game using AI technology, IT professionals found it necessary to use ML to detect cyberattacks at an early stage and to stay ahead of attackers, instead of waiting for the attack to occur and having to deal with the consequences. ML methods and techniques can improve a company's cybersecurity by constantly monitoring for suspicious activity and resolving the issue before it becomes a significant problem. Several elite cybersecurity companies are incorporating ML into their security systems and products to defeat attackers and gain customers' trust. Nowadays, companies are actively using the power of AI to enforce cybersecurity best practices in their business (Balbix, 2022).

Since the human brain can only process so much information at one time, it is almost impossible for cybersecurity employees to process and analyze masses of data as AI does. According to Truong et al. (2020), "AI possess powerful data analytics capabilities and it can be used to study huge and large amounts of electronic data with great speed, efficiency, and accuracy." Zeadally et al. (2020) indicated that the use of AI technology to counter security threats is unavoidable because AI systems are more efficient than other traditional systems as it is capable to predict future cyber-attacks based on past threats, even if the threats changes. Abdullahi et al. (2022) confirmed the existence of different types of cybersecurity attacks, threats, and vulnerabilities in Internet of Things (IoT), these attacks include Denial of Service (DoS), Distributed Denial of Service (DDoS), malicious, ransomware, blackhole, sinkhole, reconnaissance, and wormhole attacks. Several AI approaches have proven to be effective in tackling and reducing cyber-attacks in Internet of Things (IoT) systems. These approaches are smart intrusion detection systems, anomaly detection techniques, and intelligent architectural frameworks. In their study, Abdullahi et al. (2022) found that LSTM and Recurrent Neural

Network (RNN) techniques are effective in hunting IoT malware and OpCodes sequence. “An efficient DL based classification and technique has been used to detect cyber-attacks in IoT networks communications through the development of new autonomous DL classification systems using CNN” (Abdullahi et al., 2022).

The rapid development of ML (ML) and Deep Learning (DL) models such as Long Short-Term Memory (LSTM), XGBoost, Convolutional neural network (CNN), Neural Network (NN), and Temporal Convolutional Network (TCN) models provide efficient classification with high accuracy. With today’s ever-evolving cyber-attacks and the proliferation of devices, traditional software-driven approaches are no longer effective in threat detection compared to automating threat detection using AI tools (Balbix, 2022). ML technology helps train a self-learning cybersecurity posture management system that can cover the shortfall of skilled IT security professionals and deter hundreds of attack vectors that could threaten many organizations’ IT infrastructure. ML capability ensures data gathering from across the organization’s information systems. the system then analyzes the data and performs a correlation of patterns across millions to billions of signals relevant to the organization's attack surface resulting in new levels of intelligence feeding cybersecurity teams across a variety of categories of internet security (Balbix, 2022).

AI and ML can improve an organization’s cybersecurity by performing real-time monitoring of an ever-changing cyber threat landscape, deriving risk insights by analyzing tens of millions of observations, quantifying cyber threats and risks for key decision-makers, prioritizing vulnerabilities based on business criticality and other metrics, and using natural language capabilities to increase usability and efficiency (Balbix, 2022). Incorporating ML techniques in cybersecurity enables security teams to precisely assess the organization’s cybersecurity posture

and help them improve security team efficiency with a major reduction in breach threats. Shaukat et al. (2020) indicated that various ML techniques could be used as detection methods to detect potential cybersecurity risks. Cybersecurity detection methods are spam detection, fraud detection, intrusion detection, and malware detection. ML techniques are important to counter cybersecurity threats by detecting intrusion, malware, phishing, spam, and fraud on the network and host computers. On top of the capability of cybercrime detection, ML techniques can address the limitations and constraints faced by conventional detection methods (Shaukat et al., 2020).

There is a significant increase in sales of cybersecurity software that relies on AI techniques to provide defenses against cyber-attacks. This software enables organizations to instantly detect and respond to intrusions before they breach the network. And the emphasis on the ability of ML and AI to prevent cyber-attacks. Hackers are still able to manipulate security algorithms by targeting the datasets that train the system and poison the original data. Due to the rapid growth of the Internet of things (IoT) technologies that increases the attack surface by connecting different types of devices and applications to the cloud. AI has become one of the main pillars in the field of cybersecurity. Especially with the availability of AI-based tools to the public and the potential for abuse by rogue states, criminals, and lone attackers. While cybersecurity companies rely on ML algorithms in general to train algorithms on how to react to different situations by feeding them with big datasets. Most existing cybersecurity applications cannot come up with accurate results without new datasets and training. Systems must learn how to interact with different use cases and scenarios that usually require human interaction in the form of upgrades, corrections, or configuration changes. While the promise of AI is that corrective action will take place automatically based on decisions made by technology (Stojnic et al., 2021).

It is known that many hackers use traditional methods to steal passwords from users

through the Internet. recently hackers have started using modern and advanced methods in theft operations, such as keylogger software, which records all the words that are typed via the keyboard. In addition to the existence of methods used to impersonate users and force them to type the password, technology companies must understand these modern methods that hackers use and realize the consequences behind the fall of AI technology in the hands of cybercriminals. Some cyber criminals moved from using traditional techniques to employing AI methods to steal passwords. Using a keyboard and sounds in the hacking process is the most common. It allows them to steal passwords by extracting individual's data easily. For example, hackers use the Keytap3 tool to translate the keyboard sounds while typing, then guess the passwords that were typed, as the sound of the pressures is recorded through the computer's microphone (Stojnic et al., 2021).

ML security solutions are the most powerful AI for cybersecurity to date. Within ML technique, data patterns reveal the probability of an event occurring. ML is somewhat incompatible with real AI in some ways; it relies in particular on "accuracy" not "success." In other words, ML intends to learn from a data set that focuses on tasks and concludes with finding optimal performance for the given task. Then it will pursue the only possible solution based on the data provided, even if it is not the ideal solution. With ML, there is no real interpretation of the data, which means that this responsibility still rests with human teams. ML excels at tedious tasks like identifying and adapting to the pattern of data. Humans are not well suited for these types of functions due to task fatigue and a general lack of tolerance. However, while the interpretation of data analysis is still under human control, ML can help frame the data in a readable and understandable presentation (Stevens, 2020).

ML enhances data classification by classifying data points to build attack profiles for

vulnerabilities and other aspects of proactive security. This point is fundamental to the integration between ML and cybersecurity. ML has data aggregation capability by gathering all the classified data and putting them into "aggregate" data sets with common features. For example, ML can be used when analyzing attack data for which the system has not already been trained. These data sets can help determine how an attack occurred, as well as what was accessed and exposed. ML technology provides course-of-action recommendations that help increase the effectiveness of the security system. It recommends actions based on past patterns and behaviors. These actions can facilitate the decision-making process and greatly help respond to threats and mitigate risks. ML provides probability synthesis based on lessons from past data sets. The synthesis improves the process of investigating vulnerabilities in enterprise systems (Ahsan et al., 2022).

Saad et al. (2019) argued that ML methods could detect polymorphic and new attacks and potentially lead to the future of threat detection as it is more effective than all other conventional detection methods. On the flipside, ML can be manipulated by attackers. A simple example is an iPhone's Face ID access feature that uses neural networks (NNs) for face recognition, making it susceptible to adversarial AI cyber-attacks. Attackers could construct adversarial images to bypass the Face ID security features and easily continue their attack without drawing attention. According to Rawindaran et al. (2021), using ML techniques allows organizations to identify the cause-effect relationships between breaches and their impact on businesses. These relationships can contribute to the safety of data management within the organization environment. ML uses statistical techniques to enhance the detection of zero-day attacks in cyberspace by revealing characteristic behaviors and patterns of the attack. In their research, Rawindaran et al. (2021) mentioned that Google's Gmail, Amazon's Amazon Web Services, and Facebook are all taking advantage of ML knowledge within their cyber security models to enhance their threat detection efforts. Siemens

Cyber Defense Centre succeeded in evaluating 60,000 potentially critical threats per second by building an AI-enabled platform; this automation initiative led to improving the company's threat detection efforts.

In an article posted on CSO online, Korolov (2017) acknowledged that Google was able to use ML in detecting and removing malware from mobile devices running on android. Korolov (2017) added that Google Gmail has succeeded in spam filtering and used ML to identify threats, such as virus delivery, Denial-of-Service (DoS), and other imaginative threats. There are other big companies that adapted ML by using deep learning algorithms to detect and remove fraudulent behavior within milliseconds of the transaction occurrence; some of these companies include PayPal, Visa, and Mastercard. Another ML success story is with Mastercard, which had experienced over 200 fraud attempts per minute and successfully employed ML algorithms to counter cyber- \attacks. Mastercard, too, chose to implement deep learning algorithms within its network. Hao (2020) wrote an article in the MIT technology review that explained how hackers tried to manipulate Tesla's autopilot technology into veering into the wrong lane while driving. It is an example of an adversarial attack where hackers manipulate a machine-learning model by feeding in a specially crafted input. Tesla's investment in ML proved a success in overcoming the problem. The company used automation to secure its Wi-Fi and browser vulnerabilities using zero-day exploits to limit tampering with autonomous vehicles, which can be disruptive. Adversarial attacks are growing to be a major concern as AI is used more widely, especially in areas like network security (Rawindaran et al., 2021). When it comes to phishing emails, cyber-attacks use machine-learning security tools in two ways, they use it to create the phishing emails, and to verify if these phishing emails can get past spam filters. Cybercriminals propagate these attacks on illegal forms and create fraud campaigns to generate emails that have the ability to pass through the spam filter.

Vorobeychik and Kantarcioglu (2018) mentioned that cybercriminals use any available open-source security tool as leverage to conduct their attacks, these tools have some form of AI or ML built in and are available online, some free and some not. An example of these available open-source tools are antiviruses. Attackers use these types of tools not to defend against attacks but to improve their attacks and tweak the malware to evade detection. In addition to using AI-powered security tools to leverage attacks, cyber attackers a lot of different technologies that are not security related. For example, users might be able to detect phishing emails by spotting grammar mistakes. To mitigate that, cybercriminals use AI- powered grammar checkers like Grammarly to improve their writing (Vorobeychik & Kantarcioglu, 2018).

Patch Management to Reduce Attack Surface

Roumani (2021) argued that the major security concern facing organizations is zero-day vulnerabilities. Many of these organizations rely on mission-critical apps and sensitive data. Timely patch release is a priority to the organization and software vendors once detecting a vulnerability as timing can impact the risk of zero-day attacks. However, the patching release time of such vulnerabilities is affected by different factors and varies across products and vulnerability types. According to National Vulnerability Database (NVD), the number of reported vulnerabilities from 2017 to 2019 is reaching an ahistorical high of more than double. It is the software vendor's responsibility to discover and patch security vulnerabilities that often occur because of a glitch, software flaw, human error, or weakness that compromises the affected system. Issuing a security patch on time prevents hackers from exploiting the security gap and publicly disclosing it (Roumani, 2021). Roumani defines zero-day vulnerability as a newly discovered vulnerability with no security patch and unknown to the software vendor. Patching management plays a major role in eliminating these vulnerabilities. The best scenario is when the software vendor releases a timely

fix to avoid zero-day exploits. Attackers exploit security vulnerabilities by releasing them to the public and are likely to use them to attack vulnerable systems. Thus, any delay in patching these vulnerabilities implies higher risks for zero-day exploits. For example, Oracle reported two Java-related zero-day vulnerabilities in April 2012; by the time the company scheduled the patch release, attackers were ahead in exploiting these two vulnerabilities, and it was already too late to react to the issues. Another example is the vulnerability reported to Microsoft in Microsoft Word. Nevertheless, because of the delay in issuing a security patch, the vulnerability was exploited by cybercriminals. Both examples above caused financial and political attacks that put millions of potential victims at risk.

Dissanayake et al. (2022) acknowledged that the process of patching security vulnerabilities in large systems is very complex. It requires the involvement of multiple stakeholders that have the ability to make interdependent technological decisions. Dissanayake et al. (2022) emphasized that patching is the most effective strategy to protect systems against cyber-attacks. These cyber-attacks are the most critical threat facing modern corporate networks because they can cause devastating consequences to businesses, such as reputation and financial losses. Equifax is one of the large firms that had to deal with such losses when attackers breached the confidentiality and integrity of company data. Additionally, some of these attacks can cause human deaths because of the unavailability of software systems. Emmitt (2021) indicated that AI could increase patching efficiency, and automating the process minimizes the IT team's workload. However, human interaction is still required for reviewing, approving, or rejecting patches in certain cases. The primary driving force for patching management for applications is to ensure there is consistency in the configured platform that is secure to new vulnerabilities and any defects that might arise during application performance. Patch Mmanagement has several benefits to organizations; it minimizes

system downtime resulting from ransomware, functional bugs, and cyber-attacks; patching software regularly improves the security of the IT environment against breaches. It also reduces compliance fines imposed by regulatory bodies. Patch software vulnerability helps maintain the functional operation of the software and enhances a solid security posture. Patching software vulnerability reduces the attack surface and impedes cybercriminals from finding gabs and weak points in the software. As per a Ponemon Institute report, 60% of breach victims said they were breached due to the exploitation of a known vulnerability where the patch was not applied. In today's business, companies use a variety of computing devices such as security appliances, servers, laptops, desktops, and mobile devices to increase productivity and enhance performance in the ever changing and dynamic world of Information Technology. The increase of Information Technology use expands the attack surface which will require more security efforts to protect organizational IT assets. It became very necessary for organizations to maintain the availability, integrity, and confidentiality of its systems. Maintaining CIA contributes to organizational success and helps achieve competitive advantage. Therefore, companies must use a robust patch management process to protect the confidentiality, integrity, and availability (CIA) on systems and the data they transmit or store. Patch management involves systems daily processes and activities engineered towards obtaining and installing a wide range of bug fixing and updates to an existing computer application. Patches protect networks from cases of cyber-attacks which are always on the rise.

Zhu and Liang (2019) defined security vulnerability as different types of defects of information technology and related products that directly affect the normal operation of the entire information system. If cybercriminals exploit these defects maliciously, they can cause serious damage to the integrity, confidentiality, and availability (CIA) of the entire system.

Detecting and preventing security vulnerabilities is no longer an easy task, it requires plenty of human resources and large budgets. It has become crucial to apply AI technology such as ML and natural language processing to security vulnerability. Applying AI to the security aspect of information technology can achieve automated and efficient vulnerability mining, vulnerability utilization, vulnerability assessment, and vulnerability repair. (Zhu & Liang, 2019). AI subsets is predicted to be used widely in systems vulnerability detection and mining, the most effective subnets are ML and natural language processing, the use of these two AI technologies helps automate the processing of program code, provide valuable information on the nature of the vulnerability and the potential threat resulted from the system weakness.

With the increase of cyber-attacks that target organizations and the increase of cybersecurity regulations as a result of these attacks in recent years, network security became more important than ever for IT companies. Ensuring the safety and privacy of customers is one of the most significant concerns for these businesses in the shed of recent increase in cyber breaches that exposed large number of customers' records in different organizations (Olswang et al., 2022). According to the National Institute of Standards and Technology (NIST), the number of new vulnerabilities has spiked from about 5632 to 16,514 in 10 years (from 2008 to 2018; NIST, 2019). The way attackers compromise the critical assets or organizational data is by penetrating the weakest link in the network and use a chain of vulnerabilities to discover an attack path within the network, this allows attackers to conduct advance cyber-attacks and achieve their desired objectives. Although security administrators work hard to maintain the safety of their organization's network and decrease the effectiveness of adversarial attacks, patching all vulnerable information technology assets at the same time in large organizations is difficult because of the large scale of networks and the impact on operations that can be interrupted during

maintenance. The security team must consider operational and security consequences such as downtime due to software patching. Giving the large attack service and the number of vulnerabilities in the organization, security team must prioritize the vulnerability patching activities based on their perceived risk and impact "Vulnerability patching is one of the most important yet most expensive security operations in terms of budget, manpower, and service continuity" (Olswang et al., 2022).

Olswang et al. (2022) acknowledged the Common Vulnerability Scoring System (CVSS) as a formal framework for identifying the severity of vulnerabilities. CVSS system identifies a vulnerability regardless of the criticality of the vulnerable system and its circumstances within an enterprise. a vulnerability in a non-critical system may be a steppingstone on a path to a critical asset. A good example of exploiting a vulnerability is the cyber-attack against Target in 2013, the attack that exposed more than 40 million credit cards identities. Attackers were able to gain access to a third party HVAC system company and allegedly penetrated Target's network through the third party company. Cybercriminals were able to find a vulnerability in the point-of-sale system and exploit it to steal payment card numbers of some 40 million customers and the personal data of roughly 70 million. The attack tarnished the giant retail's reputation, significantly reduces its profits, and cost its CEO and CIO their jobs (Olswang et al., 2022). Yadav et al. (2022) stated that "not all vulnerabilities are always exploited by the attackers; and not all vulnerabilities can be patched due to the resource constraints such as people, infrastructure, tools and time available to patch every vulnerability" (Yadav et al., 2022).

No Code/Low Code Platforms and The Adoption of AI in The Cloud Computing

AI and ML complement cloud computing growth and security. It enables companies to easily access, store and share data with ensured security and reliability. The mix between ML and

cloud computing has contributed to the birth of a new technology known as the “Intelligent Cloud.” An intelligent cloud can save information, analyzing and learning from it, then passing it on to other servers and clouds. Patil et al. (2020) indicated that ML enables rapid innovation and transforms nearly every industry; incorporating ML in business has proven to help organizations drive efficiencies and meet customer demands at an unprecedented scale and pace. As organizations are increasingly mature in ML, the heavy reliance on large data sets and the need for fast, reliable processing power are driving the use of ML in cloud computing security.

The adoption of AI in the cloud environment will advance the level of security by spotting the inconsistencies in the cloud infrastructure, which can be accomplished by taking advantage of ML to ease data processing, which will help identify and learn more data patterns. As a result, it will detect and hinder any threats, block unsafe codes into the system and prevent any form of unauthorized access to the cloud environment. Cloud ML adopters realize that cloud ML is the future of AI and emphasize its benefits of it to cloud security. The growth of the cloud ML market is estimated to be worth between $2 billion and $5 billion, with the potential to reach $13 billion by 2025 (Patil et al., 2020).

According to Candelon et al. (2022), No code/Low code NC/LC platforms democratize A.I. (i.e., make AI accessible to people with limited to no knowledge in software development). In the corporate environment, it allows employees that are not technically qualified to develop AI solutions and applications without relying on software developers. The internal development of these applications helps multiply the business’s AI capabilities by giving employees the power to develop algorithms faster and at lower costs.

Tech giant companies like Amazon, Google and Microsoft are interested in investing in No Code/Low Code platforms for many reasons. NC/LC will help create 450 million applications in

the next 5 years. It will fill a one million developer shortfall, and it will lower entry barriers to coding and speeding up the delivery of business apps. Brown (2022) indicated that according to Gartner, low code application development will take over more than 65% of application development activity by 2024. According to Goodman (2020), around 40% of low code no code applications users come from business backgrounds; this will directly influence the company's conduct of IT business. Nearly 60% of all custom apps are now built outside the IT department. Of those, 30% are built by employees with either limited or no technical development skills. Candelon et al. (2022) stated that "42% of IT professionals plan to deliver ten apps or more for their organization. However, the average time to develop these apps is five months or more. 24% of low code users had no experience before using low code platforms, and 40% of users come from a mostly business background" (Candelon et al., 2022).

Chat GPT and Generative Pre-trained Transformer Models.

In addressing the evolving landscape of cybersecurity, the challenges extend beyond traditional threats to encompass the risks associated with advanced AI models, such as GPT (Generative Pre-trained Transformer). As humanity contemplates defending against offensive AIs surpassing human intelligence, the intersection of AI and cybersecurity introduces complex considerations. Offensive AIs pose big threats, from AI-driven social media manipulation to the potential of writing malware using language models. The infiltration of AI "trolls" on social media, learning from users to influence opinions, and orchestrated cyber-attacks employing millions of AI-driven viruses challenge conventional cybersecurity defenses designed for human-driven attacks. The collaboration between AI systems and the potential creation of malicious code made it necessary for organizations to consider the urgency of establishing robust policies and cybersecurity defenses. Simultaneously, language models like Chat GPT introduce unique risks to

cybersecurity. Capable of generating human-like text, GPT can be exploited to produce misleading content, automate social engineering attacks, and enhance the sophistication of phishing efforts. The natural language proficiency of models like Chat GPT makes it challenging for individuals to discern between genuine and malicious communication, amplifying the effectiveness of social engineering tactics. Additionally, the prospect of AI-enhanced cyber-attacks, where AI components communicate and adapt dynamically, adds another layer of complexity to the cybersecurity landscape (Bengio, 2023).

Addressing these challenges requires a comprehensive approach. Policies and defenses must not only consider the threats posed by malicious AIs but also account for the specific risks introduced by advanced language models like GPT. As AI systems approach or surpass human intelligence, the potential for dangerous power concentration escalates, necessitating the rapid development of countermeasures. However, deploying AI assistance against smarter adversaries demands caution. The risk of AI assistants transforming into rogue entities, coupled with the lack of foolproof safeguards against misalignment, emphasizes the importance of careful implementation. Ongoing research into methods to reduce misalignment and prevent loss of control becomes imperative, driven by the scientific community and industry's rapid progress in developing more powerful AI systems. The risks associated with AI models like GPT, and the broader implications of malicious AIs emphasize the need for continuous research, education, and the development of advanced cybersecurity tools to effectively navigate the evolving intersection of AI and security (Bengio, 2023).

The Problem

The general problem to be addressed is the use of AI and ML to conduct cyber-attacks against organizations resulting in the inability of organizations to effectively secure their networks

from data breaches and malicious attacks. Al-Moshaigeh et al. (2019) discussed how the growth of AI will trigger a wide range of cyber-attacks even more than before. It enables hackers to target organizations and businesses at a more rapid penetration rate with more effective cyber-attack means. Olenick (2018) indicated that while AI-based technology becomes more widely used, an increase of cybersecurity threats and attacks is becoming an ever-growing problem amongst the business industry all across the United States. Gao et al. (2020) indicated that damage caused by data breaches could negatively affect an organization's finances and reputation. According to statistics, United States breach incidents in 2017 hit a record high of 1,579 breaches. Paoli et al. (2018) predicted that the projected financial loss resulting from the continuous growth of cybercrime is expected to reach $6 trillion annually by 2021. The specific problem to be addressed is the potential use of AI and ML to conduct cyberattacks against organizations within the technology industry in the United States, resulting in the inability of organizations to secure their networks from data breaches and malicious attacks effectively.

The rapid development of AI and ML in technology drew the attention of information technology experts and even the U.S. government. Despite the advantage that AI adds to the cybersecurity field and the critical role ML plays in cybercrime detection and prevention. In this digital age, AI became essential in several areas of human interactions including computer vision, pattern recognition, expert systems, language processing and translation, speech recognition, biometric systems, robotics, and IoT (Shamiulla, 2019). Artificial intelligence indeed has a dark side as it can enhance the capabilities of AI-powered cyber-attacks. The use of AI and ML technologies for cyber-attacks have begun to appear in the United States. As AI increases the risk and effectiveness of cyber-attacks, technology organizations should prepare to counter the malicious AI that could cause severe damage to many businesses. Deploying AI and ML

technologies to conduct cyber-attacks can create a practical business problem for the technology organizations that provide products and services to the most critical sectors in the United States. According to Dixon and Eagan (2019), offensive AI's highly sophisticated and malicious attack code threatens the technology field. It mutates itself, learns the environment, and then compromises systems with a small chance of detection. Paoli et al. (2018) indicated that cyber-attacks are becoming ubiquitous and recognized as one of the world's most strategically significant risks today. These cyber/digital attacks targeted governments, critical infrastructure, private corporations, educational institutions, and non-profit organizations. That made experts realize that no sector or entity can be immune to these harmful attacks as the level of sophistication of AI-powered attacks continually increases (Dixon & Eagan, 2019).

The use of AI-enabled cyber tools is not just limited to IT professionals; it is now available to state-sponsored actors, criminals, loan actors and even individuals. This availability has dramatically increased the risk of AI-powered cyber-attacks. Hegwer (2017) mentioned that cyber attackers nowadays range from the ubiquitous "kid in the basement" hacker to professional crime syndicates and nation states, and many of those cybercriminals are hired by foreign governments. This study explored how technology companies can face serious business problems without taking the necessary measures and constantly evolving their security practices. It also focused on cybersecurity as one of the areas most affected by the technological advancement of AI and ML, representing a significant applied business problem to the technology organizations. According to Carriço (2018), the greatest danger posed by AI is its ability for weaponization.

Yamin et al. (2021) defined weaponized AI as malicious AI algorithms that can degrade the performance and disrupt the normal functions of benign AI algorithms while providing technological edge attack scenarios in cyberspace and physical spaces. Kaloudi and Li (2020)

acknowledged that highly targeted and evasive attacks in simple and harmless carrier applications and have demonstrated the intentional use of AI for harmful purposes. Social engineering attacks, phishing attacks, password attacks, distributed denial of service (DDoS) attacks, data manipulation, and mutating malware attacks; all such attacks could be operationalized through simple applications the victims use on their devices. Therefore, the risk derived from the abuse of AI technology can strike targets far faster than humans can.

Current academic literature recognizes the practical business problem of AI-powered cyber-attacks as a current concern, not a hypothetical future idea. The critical building blocks for using offensive AI already exist, including highly sophisticated malware and financially motivated cyber criminals willing to use all the available tools to break into systems and increase their financial profits (Dilek et al., 2015). Despite several studies on AI and security, researchers have not clearly explained the adversary's actions and how to develop proper defenses against AI-based cyber-attacks. Deficiencies in current information systems literature include an incomplete understanding of how an AI-enabled cyber-attack can be a critical threat with the advancement of technology, whereas academic literature expansively addresses the benefits of AI-based technology on securing organizations' systems and how it contributes to improving them. The focus on the positive side of AI and the lack of the negative impact of AI in the field of information systems represents a gap in current literature.

Concepts

The Confidentiality, Integrity, and Availability (CIA) Triad Concept

The CIA triad is considered the core concept of information security. It is central to the research problem that helped explore the cybersecurity challenges within the technology industry in the United States. The CIA triad consists of three primary concepts in information security.

Maintaining confidentiality, integrity, and data availability are necessary to achieve the cybersecurity goal of protecting information from unauthorized access, modification, and deletion (Gao et al., 2020). The data's confidentiality, integrity, and availability are vital in cybersecurity as it provides essential security features; implementing the CIA triad helps organizations avoid compliance issues, ensures business continuity, and prevents reputational damage. According to Kar Yee and Zolkipli (2021), the purpose of data security and protection is to preserve data integrity and availability for necessary use while maintaining user privacy through confidentiality. The triad achieves information security objectives to ensure data protection (Alkhudhayr et al., 2019). The CIA triad is a widely used cybersecurity model that can guide an organization's efforts and policies to keep its data secure (Alhassan & Adjei-Quaye, 2017). The initials stand for the triad on which information security rests.

Confidentiality. Confidentiality is a necessary component of privacy. Technology organizations take user privacy seriously and focus on providing secure services to their customers. Achieving confidentiality ensures that only authorized users and processes can access or modify data. Khidzir et al. (2018) defined confidentiality as the restrictions on using and storing various data types. Confidentiality protects sensitive information from unauthorized disclosure while in transit over a network (Andress, 2014). The concept considers a set of rules and restrictions that limit access to certain types of information and supports the user data as secret, private, and not viewed even by the cloud service provider. Common methods of ensuring confidentiality are data encryption, user identity documents (IDs), passwords, cards, retina scans, voice recognition, fingerprints, security tokens, and key fobs tokens (Tchernykh et al., 2019).

Integrity. Data integrity involves maintaining the consistency, accuracy, and trustworthiness of information to prevent unauthorized people from changing, altering, deleting, or

illegally accessing the data. It ensures that no entity can modify or change the information other than the owner during the creation, transmission, and storage processes. Integrity supports a complete data structure as a fundamental concept of information security (Tchernykh et al., 2019). Measures to ensure integrity include file permissions and user access control are the measures controlling the data breaches in an organization. Common attacks that compromise data integrity include attacks that penetrate the webserver, Man-In-the-Middle (MITM) attacks, salami attacks, trust relationship attacks, session hijacking attacks, and malicious code attacks (Weaver et al., 2013).

Availability. The final leg of the CIA triad is availability; service availability depends on the robustness of the hardware, hardware repairs and maintaining a correctly functioning operating system environment, system upgrades, and preventing the occurrence of bottlenecks (Tchernykh et al., 2019). The term "availability" refers to enabling the authorized users' access to the related assets and information when needed. It is a security service that ensures the constant availability of resources and services to only authorized parties in a timely manner (Khidzir et al., 2018). As Andress (2014) indicated, loss of availability causes several breaks anywhere in the chain that allow users access to their data. Loss of availability can result from different incidents such as power loss, application problems, operating system issues, network attacks, compromise of a system, or other related problems.

The Nine Ds of Cybersecurity Risk Management Concept

Cybersecurity risk management is a tool used by cybersecurity professionals to prioritize cybersecurity defensive measures based on the potential adverse impact of the threats they are designed to address (Frank et al., 2019). The nine Ds concept is inspired by the department of defense's three tenets of cybersecurity. It is one of the four cybersecurity concepts that enable the

evaluation of protection systems, including analyzing defeats by known exploits and predicting likely vulnerabilities. According to Wilson and Kiy (2014), the use of the nine Ds concept is demonstrated as analysis tool that permits ranking of the expected effectiveness of some potential countermeasures. It presents practical defensive tactics in an easily remembered scheme. Wilson and Kiy (2014) identified the nine Ds as Deter attacks, Detect attacks, Drive up the difficulty, Differentiate protections, Dig beneath the threat, Diffuse protection throughout the payload, Distract with decoys, Divert attackers to other targets, and Depth of defense.

Starting with Deter attacks sub concept, deterrence is the first line of defense. It can be used as a measure to reduce an attacker's will to conduct an attack, such as threats of legal action or other punitive measures (Wilner, 2017). The second D is Detect attacks. Rehman et al. (2021) acknowledged that detection of malicious activity is necessary if affirmative reactions are part of the defensive strategy and proactive, automated defenses are to be used. Examples of detection methods are a password failure counter that locks a user account and monitoring for excessive network traffic. Drive-up difficulty involves using technical protection measures (TPMs) to make attacks more burdensome by driving the level of difficulty beyond their ability to cope (Wilson & Kiy, 2014). In differentiating protections, Wilson and Kiy (2014) emphasized that each defensive protection system must focus on one or more specific classes of threats. Threat classes are piracy, tampering (altering functionality), and reverse engineering (discovering buried IP in a distributed executable program). Dig beneath the threat involves implementing hardware-based protections as an effective measure against attackers.

Wilson and Kiy (2014) indicated that protection at a lower layer than an expected cyber-attack might be able to defeat the attack, even if it was an expert-level attack. In diffuse protection throughout the payload, Wilson and Kiy (2014) suggested that cyber attackers should face multiple

layers of encryption and access controls and not only a single layer. The goal of diffusing protection throughout the payload is to leave the hacker with limited options, either bringing along functioning protections or else forfeiting the payload value. Next is distract with decoys, there are two factors that make the attackers give up, frustration or the feeling of success. Distracting with decoys is an effective protection strategy because it encourages a false belief in success which triggers frustration and the thought of failure. An example of distraction with decoys is the cybersecurity honeypot (Wilson & Kiy, 2014). The next sub concept is divert attackers to other targets, security system implementers have an option to divert the attackers' attention to a more attractive target elsewhere. The way to accomplish this protection strategy is to persuade an attacker to target some other target (Sawyer & Hancock, 2018). The last D is depth of defense, The concept of defense in depth is valuable for use against sophisticated hackers. Rahman et al. (2020) defined depth in defense as a multilayer defense strategy where several independent countermeasures are implemented in the device to provide aggregated protection against different attack vectors.

Theories

Cyber Deterrence Theory

Deterrence is considered a traditional security theory that could be superimposed on cyberspace. The objective of deterrence theory is to eliminate attacks by making the costs and consequences outweigh the benefits. The cyber deterrence theory guided the research on how cybersecurity threats in AI-based technology can impact a business's strategy and decision-making (Kramer et al., 2009). As indicated by Haley (2013), the objective of deterrence theory is to eliminate attacks by making the costs and consequences outweigh the benefits. Implementing the deterrence concept requires two essential factors. The first is to have a strong defense. Kramer et al.

(2009) suggested that if the defense is sufficient to make an attack exceedingly difficult, an opponent might choose to stand down; this first objective is considered a practical solution to the most cyber-attacks in the cyber realm, The second is the retaliation factor, if successful aggressors face severe retribution following their malicious actions, other aspirants may choose not to attack at all.

Mazanec and Thayer (2016) indicated that the concept of deterrence is about keeping an opponent from doing a harmful activity by making a threat of unacceptable consequences. Mazarr (2021) suggested that deterrence can be done in two forms - deterrence by punishment (the power to hurt) and deterrence by denial (the power to deny victory); keeping someone from conducting a malicious activity may be brought about by threatening unacceptable punishment if the action is taken, this is called deterrence by punishment (Mazanec & Thayer, 2016). Deterrence by denial, on the other hand, seeks to deter action by making it infeasible or unlikely to succeed, thus denying a potential aggressor confidence in attaining its objectives (Mazarr, 2021). Mazanec and Thayer (2016) acknowledged that deterrence by denial convinces the adversaries that their objective will be denied to them if they attack. Both forms of deterrence may apply in the case of an AI-related cyber-attack against technology organizations in the United States.

Cyber deterrence is defined as preventing malicious actions against organizational assets that support cyberspace operations. Cyber deterrence consists of three pillars; these pillars are considered the cyber defense strategy's mainstay. which is credible defense, the ability to retaliate, and the will to retaliate (Lilli, 2021). Kostyuk (2021) suggested that cyber deterrence requires the application of new methods to identify the actors. And the target of the attacks was identified without knowing who launched the attack. Without identifying opponents and their goals, deterrence cannot succeed, and cyber-attacks may be repeated in the future. Lonergan and

Montgomery (2021) suggested that cyber deterrence must be an integral part of states' national security strategies. And without cyber deterrence, organizational data will remain vulnerable to primitive and dangerous forms of exploitation and abuse. Including data breaches, stealing of intellectual property, disruption of business operations, and shutdowns of critical systems. Deterrence in the information age is very different from that in the era of the Cold War in type and scope, which requires a comprehensive approach that integrates all military, economic, intelligence, and legal components to enhance information security on the one hand and create deterrence on the other hand (Lonergan & Montgomery, 2021).

Ross (2021) indicated that security experts, scholars, and decision-makers researched Cold War strategies and theories to test the extent to which they can address cyber-attacks. They acknowledged the seriousness of cyber threats and considered cyberspace a war and conflict field. They concluded that open data would remain vulnerable to many forms of exploitation and abuse without cyber deterrence. This raises several problems and questions in terms of deterrence theory. The rules of deterrence do not change from the nuclear and conventional domains to the cyber domain. The theoretical basis on which deterrence is built remains the threat to use force to persuade the opponents to comply with the will of the party initiating the threat. In this sense, deterrence relies on the main pillar involves securing all the requirements of the ability to inflict punishment and influence the opponent psychologically by convincing them that the consequences of conducting the hostile action outweigh the gains. Deterrence has traditionally begun with the threat of using conventional weapons. The most common form of traditional deterrence is to threaten the opponents with a painful punitive blow in the event of aggression on their part, which is called deterrence by punishment. Whereas nuclear deterrence is limited to threatening nuclear weapons, whether this use is partial or complete, limited or comprehensive. In other words,

deterrence relies on the threat of using military force and does not involve the actual use of it, to intimidate the opponents and instill in them the conviction of the ability to take revenge on them without turning the intentions into an act that harms them. This boundary between the threat and actual use of force constitutes the meaning and essence of deterrence. An effective deterrence strategy should include announcing effective response capabilities such as imposing sanctions, developing and deploying defensive capabilities to prevent the success of any potential attack, as well as establishing specialized forces for cyber missions, and developing and strengthening commercial infrastructure in order to repel any possible attack (Ross, 2021).

According to Mazanec and Thayer (2016), the theory of deterrence was developed early in the Cold War between the United States and the Soviet Union by academics coming to explore the novelty of the political and military impact of nuclear weapons; the deterrence concept was able to prevent a world war by allowing politicians and decision-makers to understand the risks associated with nuclear war. According to Haley (2013), thousands of cyberattacks occur per day, suggesting great difficulty in distinguishing serious threats from minor ones. Worst of all for technology organizations in the United States, the United States is specifically vulnerable to cyber-attacks due to the pervasiveness of advanced technology in every aspect of its citizens' lives, as well as the American tendency to value freedom over security and innovation over- regulation. Bendiek and Metzger (2015) acknowledged that deterrence theory has long been considered a valuable concept to achieve restraint from attacks. Goodman (2010) has identified organizations can employ eight elements of deterrence to keep adversaries from attacking the interest: an interest, a deterrent declaration, denial measures, penalty measures, credibility, reassurance, fear, and a cost-benefit calculation. a deterrent declaration serves as a warning to the opponent, "Do not do this, or else that will happen." The consequences of proceeding with the act can be either denial measures, penalty

measures, or both. Maintaining credibility and reassurance is crucial in the deterrent declaration. It emphasizes the truthfulness of the declaration. Fear is another essential element as it deters potential adversaries from taking undesirable actions. All the seven elements mentioned above factor into the cost-benefit calculation that calculates the benefits and costs of action versus the benefits and costs of restraint.

Forbidden Knowledge Theory and Cyber Deterrence

Forbidden knowledge originates in Christianity's idea of Eve eating an apple from the forbidden tree of knowledge. Hagendorff (2021) highlighted the necessity of implementing forbidden knowledge theory in ML as a means of deterrence. Hagendorff (2021) defined forbidden knowledge as "the knowledge that is considered too sensitive, dangerous, or taboo to be produced or shared." Forbidden knowledge restrictions are already implemented in scientific fields like synthetic biology, nuclear physics research, and even Information Technology security. Hagendorff (2021) suggested that this discourse must be transferred to ML research that still embraces the idea of open access because many ML applications can be misused and have harmful consequences.

Hagendorff (2021) proposed an ethical framework for disseminating forbidden knowledge and dual-use software applications for the ML community. ML research community still embraces the idea of open access when it comes to using technology like generative video or text synthesis, personality analysis, behavior manipulation, and software vulnerability detection. "Information about or from such applications may, if improperly disclosed, cause harm to people, organizations or whole societies" (Hagendorff, 2021). At the same time, some technology organizations such as OpenAI, Facebook, Microsoft and other companies do not publish the full-size model of hazardous applications and are somehow strict on making this technology available to the public. Many other freely accessible Internet platforms are emerging elsewhere with no governance or restrictions.

These apps must be kept away from public use due to the risk of malicious use if got into the hands of malicious actors (Hagendorff, 2021).

Constructs

IT Security Efforts. Investing in IT security can save organizations time and funds. Building a reliable security network is more effective than recovering from a significant cyber-breach. Hiring cybersecurity professionals to build a professional security team is a very effective approach to improve organization's security efforts (Usman et al., 2020).

Network Security Vulnerability. Hackers target weak security systems; organizations with robust IT security have way less chance of being targeted by hackers. Investment in advanced security systems can avoid businesses financial and reputation losses (Walkowski et al., 2020).

Business Executives. Business leaders have the authority to make an articulated decision on Cybersecurity based on the firm's financial standing (Mangelsdorf, 2017).

IT Security Professionals. IT security professionals help business executives make major decisions based on facts that stem from practical knowledge in the cybersecurity field (Mangelsdorf, 2017).

Risk Mitigation. To ensure a secure network, companies need to take the necessary measures to reduce cyber-related risks and have the right risk assessment tools to predict the types of future attacks (Zadeh et al., 2020).

Related Studies

Hu et al. (2023) indicated that John McCarthy introduced AI in 1956 during a conference in Dartmouth. This date marked the birth of the AI concept. However, it took five decades after that to discover the deep learning concept 2006 by Hinton et al. (2021), and the deep learning concept is enabled by the rapid growth of computational resources, the fast growth of data on the internet, and

the emergence of more efficient algorithms. AI technology has revolutionized many aspects of humans' daily lives, which motivates large organizations and even governments to lay out major strategic plans for AI. For instance, the release of the "National Strategic Plan for AI Research and Development" by the United States White House in 2016, followed by DARPA's $2 billion future investment plan in 2018 to develop next-generation AI technologies. Akhtar and Feng (2021) stated "Today's digital age necessarily requires the protection of a vast amount of valuable electronic data from cyber-attacks. Cyberattacks can destroy the reputation of organizations even shutdown organizations. The protection of cybersecurity is inevitable." AI empowers humans to improve the decision- making process by rethinking how to use the results and insights of data analyses and information integration to increase the efficiency of the process. Aside from information security in the IT field, offensive AI applies to many other fields in human lives where security is becoming a significant concern, especially in security-sensitive infrastructures.

According to a blog written by Gizmodo, a leading American technology, surgeries involving robotic-assisted surgeons resulted in the death of 144 people from 2000 to 2013. Another example of the bad side of AI is Amazon's AI-based recruiting tool that the company used between 2014 and 2017. The tools raised fairness concerns about the use of AI in the hiring process as it favored hiring men over women. Also, in 2018, Uber's automated vehicle crash sparked concern about the safety of AI and the fact that it is not yet ready to replace humans. Ai is not smart enough to control high-risk fields in human life such as autonomous driving, healthcare, and finance because a basic error or vulnerability could potentially end human lives or end up costing millions or billions of dollars. According to Taddeo et al. (2019), incorporating AI in cybersecurity tasks is attracting more attention from the private sector and government in the United States. "Estimates indicate that the market for AI in cybersecurity will grow from $1 billion in 2016 to a $34.8 billion

net worth by 2025" (Taddeo et al., 2019). AI technology can handle a large amount of data resulting from different activities that occur on organization's servers, such as data transferred daily between clients and organizations and between devices and networks. It is time-consuming for cybersecurity analysts to examine every bit of data for potential risks. Thus, the best option for spotting these threats is AI. ML technology is capable of sorting a large amount of data, tracking servers' traffic automatically and providing accurate analysis of server's activities. In addition, it has the ability to recognize any threats that might be hiding in the information thrust (Taddeo et al., 2019).

The attack surface of the global information environment keeps expanding with the growth of the 'Internet of Things' and data volumes that increases by connecting more computing devices to the network. "To counter cyber threats from this environment, cybersecurity is turning to AI and ML to mitigate anomalous behaviors in cyberspace" (Stevens, 2020). Since humans do not have the cognitive or sensory capacity to cope with the enormous data volumes produced by software and hardware dedicated to alerting systems administrators, collecting and filtering data that involve information systems and threats must be automated. Automation is a reasonable tool to find a solution to this issue, giving the human capital shortfall in the cybersecurity industry. Cybersecurity companies offer a variety of products and software packages for automated malware detection. These products scan network traffic and match data packets to known signatures of malicious software (malware) that install themselves on users' machines and act in deleterious ways. These software packages are capable of detecting and denying worms, Trojans, spyware, adware, ransomware, rootkits, and other software entities searching for and exploiting digital vulnerabilities. "Automated in this fashion, malware can be repelled, quarantined, destroyed, or otherwise prevented from infecting a system and opening it up for exploitation" (Stevens, 2020).

Ahsan et al. (2022) suggested that organizations can identify certain security threats, then implement security controls or measures against these threats by using the National Institute of Standards and Technology (NIST) Special Publications. NIST Special Publications provide step-by-step guidance for applying a risk management framework to federal information systems. It includes a set of security issues and common measures against these security threats. ML is identified as an efficient controls and measures tool. Cyber-attacks consist of five phases. These phases are reconnaissance, scanning, attack, maintaining access, and covering tracks.

The attack phase includes denial-of-service attacks, gaining access using the application and operating system attacks, and network attacks. While maintaining access phase includes using Trojans, backdoors, rootkits, and other methods. Ahsan et al. (2022) indicated that the attack process is structured and connected in a way that any interruption can affect the arrack workflow. In other words, an interruption at any phase of these attack phases can either impede or stop the entire process of attack. Implementing ML algorithms and techniques during any of the attack phases can disrupt the attack process and prevent the occurrence of the attack.

In the preparation phase of the attack, cybercriminals use techniques such as social engineering attacks, including phishing emails and malicious calls. In the case of phishing emails, ML algorithms is an effective way to detect malicious email signatures and block them. When it comes to malicious calls, cybercriminals attempt to call businesses and impersonate a third party to gather useful information to target the business. ML algorithms can flag and block these calls after conducting an all-source analysis and detecting the fake calls. There are several other examples of using ML to strengthen security posture, such as scanning any external devices such as USB to prevent malicious software from propagating through company's devices. The most common example is password recommendations using rule-based ML algorithms that find easily guessed

passwords commonly used by an organization's employees and recommend a list of passwords for use. During the scanning phase, sometimes referred to as weaponizing, that is when cyber attackers use AI technology to exploit the target system's weaknesses.

Cybercriminals use automated tools such as Metasploit, AutoSploit, and Fuzzers to search for vulnerabilities in the system during the scanning phase. ML algorithms are capable of automatically scanning and finding vulnerabilities by an ethical hacker before the attacker can. During the attack phase, ML algorithms are a strong cybersecurity measure against the attack. These algorithms include linear regression, polynomial regression, logistic regression, naïve Bayes classifier, support vector machine, decision tree, nearest neighbor, clustering, dimensionality reduction, linear discriminant analysis and boosting. These algorithms can provide a measure against cyber-attacks through spam detection, malware detection, denial-of- service attacks and network anomaly detection. In phase four of the cyber-attack, adversaries use malware traffic packets to maintain access, such as Trojans, backdoors, or rootkits. "ML algorithms can detect such malware traffic packets when the malware contacts the attacker and vice versa" (Ahsan et al., 2022). Phase five is covering tracks phase. In this phase, cybercriminals attempt to verify that their identity is not being tracked. "Attackers employ different techniques, including corrupting ML tools' training data to misidentify their data" (Ahsan et al., 2022).

Being able to detect threats quickly is critical. With 42% of organizations reporting an increase in time-sensitive threats, relying only on humans takes longer and will not produce the best results. On the other hand, AI can scan large amounts of data at one time and identify cyber threats at the same time, which facilitates the process of achieving security. Fifty-six percent (56%) of organizations report that their cybersecurity analysts are overwhelmed by the number of threats they pose, and 23% are unable to verify detected threats effectively. It is important to mention that

the amount of data passing through cybersecurity analysts is enormous, which makes it difficult to predict future threats. With the ability of ML to deal with a large amount of data at once, it can help detect malicious activity or potential threats in its early stages, this is useful to reduce the waste of time and labor, and it also keeps organizations on alert by taking a step forward to protect their networks. AI can help augment manual effort in detecting threats using the information provided by devices from previous attacks (Ahsan et al., 2022).

According to Capgemini Report Developing AI Cybersecurity, 60% of CEOs experienced an improvement in their security analysts by employing AI and ML technology. Many organizations are affected year after year by the financial impact of data breaches. Studies have revealed that organizations using AI for cybersecurity purposes face an 80% difference in cost reductions, $2.90 million, compared to $6.71 million for facilities not using their services (IBM Cost of Data Breach 2021 report). According to Moore (2021), worldwide spending on cybersecurity technology and services is forecasted to grow 12.4% to reach $150.4 billion in 2021-2022. The strong growth came after the high demand for telework technology and cloud security. Table 1 shows a recent forecast by Gartner Inc. of the growth of cybersecurity and risk management spending between the years 2021 and 2022, according to Gartner Inc.'s recent forecasts.

Table 1

Cybersecurity end user spending by segment, 2020-2021 (Millions of U.S. Dollars).

Market Segment	2020	2021	Growth (%)
Application Security	3.333	3.738	12.2%
Cloud Security	595	841	41.2%

Market Segment	2020	2021	Growth (%)
Data Security	2.981	3.505	17.5%
Identity Access Management	12.036	13.917	15.6%
Infrastructure Protection	20.462	23.903	16.8%
Integrated Risk Management	4.859	5.473	12.6%
Network security equipment	15.626	17.020	8.9%
Other information Security Software	2.306	2.527	6.9%
Security Services	65.070	72.497	11.4%
Customer Security Software	6.507	6.990	7.4%
Total	133.776	150.409	12.4%

It is worth mentioning that not only does the government of the United States include AI in its national cybersecurity and defense strategies, but many other governments explicitly mention AI capabilities as a potential strength. However, trusting ML and neural networks to deliver cybersecurity tasks is a double-edged sword, it can improve cyber-attacks detection and analysis but can also introduce and enhance new forms of cyber-attacks to the AI applications themselves, which may cause severe security risks. According to Taddeo and Floridi (2018), cyber-attacks are becoming more sophisticated and destructive in the shade of AI growth. “Each day in 2017, the United States suffered, on average, more than 4,000 ransomware attacks, which encrypt computer files until the owner pays to release them” (Taddeo & Floridi, 2018). The number was significantly less in 2015, with only 1000 ransomware attacks. The value of AI in cybersecurity is predicted to increase by $17 billion from 2016 to 2023 after it was $1 billion in 2016. AI is poised to revolutionize attacks and counter-attacks activities.

In recent years, the world's use of AI techniques has increased dramatically, and giant technology companies have begun to develop algorithms capable of reducing the spread of cybercrimes, these systems have the ability to predict and react to cyberthreats beyond human capabilities. Attacks will become faster, more precise, and more disruptive to make the response to the attack. Organizations will react to threats in a significantly shorter time, within hours, not days or weeks. It requires a robust AI system to detect threats. If an organization's AI is enforced in real-time, it will ensure a fast response to any attack. Unlike advanced AI-based threat detection systems, traditional cybersecurity systems provide a significantly slower response, easing the attackers' attempts to breach the network.

Additionally, many cybercriminals use AI technology to attack, and for the organization to use traditional cybersecurity systems, it would be difficult to cope with these AI- powered high-speed attacks. Many companies are already using ML to identify vulnerabilities and bugs and verify code. For example, "in April 2017, the software firm DarkTrace in Cambridge, UK, launched Antigena, which uses ML to spot abnormal behavior on an IT network, shut down communications to that part of the system and issue an alert" (Taddeo & Floridi, 2018).

Taddeo (2019) acknowledged that AI could reduce the impact of cyber-attacks and enhance the defenses against them. For that reason, and according to the 2019 annual cybercrime report, private and public sectors are increasingly showing interest in developing AI applications for cyber security. Many organizations are making big investments in AI for cybersecurity, knowing that AI technology keeps on learning tasks, patterns, and behaviors, which helps prevent future attacks. IT technology organizations realized that human security analysts could not handle the increase in cyber-attacks alone. Incorporating AI technology can save them time and effort to react quickly to cyber threats. Taddeo (2019) also emphasized that the involvement of AI in cybersecurity brings

both bad and good news.

Fortunately, the good news is AI can foster the stability of cyberspace and significantly improve internet security and defense measures. It positively impacts cybersecurity from the system level in three areas: system robustness, system resilience, and system responses. The negative and positive impact of AI on cybersecurity suggests serious ethical risks that must be considered. If not addressed, it can hinder the adoption of AI in cybersecurity or cause major problems for the future of the internet. The bad news is that the use of ML and deep learning creates a suitable environment for the escalation process of attacks. It facilitates faster and more impactful cyber-attacks. Adversaries take advantage of the ability of AI to detect systems vulnerabilities that often escape human experts. After detecting these vulnerabilities, they exploit them to attack a given target.

Kaloudi and Li (2020) suggested that the rapid progress of AI technologies has extended their capabilities into several domains; and AI is turning the flood of data into actionable information by quickly collecting and filtering large amounts of data to detect malicious patterns and abnormal behaviors. Kaloudi and Li (2020) emphasized that a lot has been published about the advantages of AI to the cyber field while less attention is given to its disadvantages. The offensive use of AI is changing the landscape of potential threats against a wide range of internet applications. Particularly, the malicious use of AI has the potential to threaten more complex systems such as smart cyber-physical systems (sCPS), which have not been studied thoroughly before. According to Kaloudi and Li (2020), “sCPS refer to advanced CPS systems, which are more interconnected through various technologies like the Internet of Things (IoT), AI, wireless sensor networks (WSNs), and cloud computing to provide a wide range of innovative services and applications” (Kaloudi & Li, 2020). Soni (2019) highlighted the capability of AI to flag and reduce

money laundering and fraud cases in the banking system. The use of AI helps detect the movement of large amounts of money secretly by detecting the unusual activities in the system. In fraud cases, ML technology can detect and flag attacks on banks or clients for money transfers and suspicious actions from bank employees. This can be done through multiple processes of "collecting, analyzing and learning from traditional data to create the Fraud Detection System" (Soni, 2019).

According to Rughani (2017), the more technology advances, the more incidences of cybercrime. Not all of the data breaches daily, cybersecurity experts do not have the ability to curb all cyberattacks because of the rapid advancement of automation technology which makes it difficult to control the attack surface. Additionally, the reported cybercrime incidents receive little response from cyber experts due to the complexities involved in solving such problems. The number of cybercrime experts is fewer compared to the cybercrimes rates. Of 26,907 crimes reported in India, only 397 cases were convicted between 2013 and 2015. Rughani (2017) discovered that a similar situation is experienced in nearly every country. Rughani (2017) suggested that there are still questions on the accuracy levels of using AI-enabled tools since it is based on the input made by humans despite the system's ability to use trained systems to produce more detailed results as the work is automated and less man interaction is required.

Morgan (2019) indicated that investment in worldwide cybersecurity is expected to increase more than $1 trillion from 2016 to 2021. With the internet usage in the modern generation, people around the world exchange huge amounts of data every day, with increase of internet usage, cyber-attacks is also increase dramatically. These cyber-attacks have greatly affected many sectors and fields, especially in online transactions and smart devices, as companies and government agencies have relied on AI-based technology in protecting data from cybercrimes and data breaches. This advanced technology comes with challenges, as the cyber danger has become greater for small

businesses that do not use data protection technology, which makes these businesses vulnerable to data breaches and intrusions. Hence, using AI-based technology in securing large data from this imminent threat became very necessary. For example, small businesses rely to a large extent on third party companies in their transactions and communications, which exposes them to possible data breaches risk from competitors in their field. Therefore, it is important to encrypt these various communications to remain safe (Morgan, 2019).

There is no doubt that the importance of applying AI technology to organizational data and transactions achieves a higher level of electronic security and sensitive data protection. AI is distinguished from other innovations by anticipating actions and not only reacting to them. In the case of cybersecurity, it can predict and prevent intrusions, in addition to securing systems from any vulnerabilities that hackers exploit to breach data. AI technology in cybersecurity is characterized by its speed of reaction, and its ability to react to cyber threats effectively and efficiently at any time of the day (Morgan, 2019). Kabbas et al. (2020) indicated that traditional cybersecurity approaches are no longer effective against sophisticated, creative, and continuously evolving cyber-attacks, traditional cybersecurity approaches include network protection systems and computer security systems. Cybercriminals manage to increase the potency of their tailored attacks which enabled them to launch more automated and effective cyber-attacks. AI is one of the most advanced technology can be used effectively in cyber security and ML have proved very effective infighting cyber-attacks (Zeadally et al., 2020).

Anticipated and Discovered Themes

The potential themes and perceptions in this literature review would be that of technology organizations' investment in AI-based technology to improve IT infrastructure security, incorporating AI tools and ML models to enhance malware detection. Malicious AI can have a

major effect on organizations' infrastructure, reputation, strategy, and other organizational aspects. Technology organizations have a very large attack surface to protect against AI-powered cyber-attacks, which raised decision makers' concern about the risk of the rapidly growing technology and the necessity of an effective action to reduce attack vectors and maintain the CIA. Experts believe that AI is ideally suited to solve some of cybersecurity's most difficult problems; technology organizations realize the importance of investment in detection and countering attack vectors as a step to prevent unauthorized access to organizations' data that they consider the most valuable business. Whether it is a digital or physical attack surface, growing organizations are always on the lookout to protect their data. More growth in the business means more data assets, and more data results in a larger attack surface; a larger digital attack service enables adversaries to exploit all possible locations and entry points to gain unauthorized access to the network or system to extract data or cause a cyber-attack. Thus, organizations continuously seek effective ways to make the attack surface smaller to reduce attackers' chances of gaining unauthorized access.

Cybersecurity professionals use AI to reinforce cybersecurity best practices and reduce the attack surface rather than continually trying to detect malicious activity using human resources, which can be cost-effective and time-consuming. On the contrary, cybercriminals can exploit those same AI tools and systems for malicious purposes such as deploying sophisticated AI-powered cyber-attacks and data breaches; it can also use to propagate cyber-attacks and even manipulate ML systems. Adversarial AI leads ML models to misinterpret inputs into the system and behave in a favorable way to the attacker. Along with the investment in the detection of attacks, companies are also investing in deterring attackers from initiating cyber-attacks; companies use different techniques to change attackers' motives and behaviors which is considered an even more effective measure than waiting for the attacker to launch the attack and then react to it and must deal with

consequences and aftermath. All the above led to discover a major theme, “the use of AI to combat AI,” by employing AI models to predict, detect, and respond to potential cyber-attacks.

In the thematic analysis of semi-structured interviews involving 15 participants, a comprehensive understanding of the relationship between AI and cybersecurity emerged. The identified themes encompassed both the positive and negative dimensions of AI's impact on cybersecurity. The positive aspect revealed a consensus on the strategic necessity of investing in AI technology to fortify cybersecurity defenses. AI deterrence emerged as a strategic theme, revealing participants' perspectives on leveraging AI not only as a defensive tool but also as a deterrent against potential cyber threats. This theme shed light on the proactive use of AI to dissuade and prevent cyber-attacks, contributing to a comprehensive cybersecurity posture. Participants emphasized the essential role of technological advancements, urging organizations to allocate resources for the development and implementation of AI-driven solutions. This theme emphasized the proactive approach needed to stay ahead in the ever-evolving danger of cyber threats. The theme of employee awareness and compliance brought attention to the human factor in cybersecurity. Participants stressed the importance of educating and training personnel to minimize vulnerabilities arising from inadvertent human errors. This recognition of the human element highlighted the need for a holistic cybersecurity strategy that integrates both technological solutions and human-centric approaches.

The financial implications of AI-powered attacks emerged as a significant concern. Participants acknowledged the potential economic repercussions for organizations and customers alike, emphasizing the urgency for robust cybersecurity strategies to mitigate these risks effectively. The discussion on financial implications revealed the broader implications for businesses, reinforcing the idea that cybersecurity is not merely a technical concern but a critical

aspect of overall financial risk management. AI regulations and control is another major theme discovered in this study, participants responses reflected the ongoing debate about the necessity for governance in the AI and cybersecurity domain. Participants articulated the need for a regulatory framework that balances innovation with ethical considerations, ensuring responsible AI deployment. the unique theme of Chat GPT and cybersecurity highlighted the integration of generative AI in cybersecurity protocols. This showcased the dynamic relationship between innovative technologies, such as Chat GPT and other language models, and the evolving strategies employed in digital defense. It emphasized the role of natural language processing and generative pre-trained transformers in enhancing cybersecurity communication and incident response. Finally, the impact of AI on the cloud and Internet of Things (IoT) was a theme that emphasized the interconnected nature of technologies. The themes discovered the evolving technology where AI influences the security dynamics of cloud computing and IoT, emphasizing the need for integrated security measures across these domains.

Summary of the Literature Review

The literature review provided a baseline understanding of the relationship between AI and cybersecurity by exploring the malicious side of AI and its effects on technology organizations' IT infrastructure. It highlights the need for companies to increase their investment in AI and ML solutions to reach their IT infrastructure security goal. The literature review covered the use of AI-powered technology by adversaries to conduct data breaches and cyber-attacks and how businesses use AI- based tools and the state-of-art ML techniques applied to cybersecurity to assist in breach detection and prevention. The elements of this literature review aim to show the connection between the existing knowledge on the new cyber-attacks concepts and the research study. The literature review helped achieve the research project's goal of bridging the gap where knowledge is

missing and adding new knowledge to the current body of knowledge by conducting an in-depth study of the problem and discovering new aspects and solutions. This research added to the literature concerning AI and cybersecurity as associated with technology that has become part of the present generation. It will also advise various technology organizations on whether investing in AI and its subnet (ML) solutions in cybersecurity is the solution to countering cyber-attacks. The research will help explore adversaries' intent to develop a deeper understanding of organizations' defense mechanisms against cyber-attacks and the measures taken to prevent penetrating their environments. The literature review emphasized the importance of leveraging AI as a core component of an organization's security operations to keep up with the sophistication of the automated cyber-attacks and using the right technologies to fight intelligence with intelligence.

Summary of Section 1 and Transition

Thus, concludes Section 1, the Foundation of the Study, in which the background of the problem, problem statement, purpose statement, nature of the study, research questions, conceptual framework (one theory and two concepts), definitions of terms, assumptions, limitations, delimitations, the significance of the study, and a review of the professional and academic literature were examined in detail. The key points presented in section 1 described how the research method and design were aligned with the study problem, purpose, and research questions. As discussed, technology businesses in the United States remain valuable targets to adversaries, which save no effort to use anything possible to expose the growing attack surface of these businesses. AI and ML techniques are the most effective means to reach this goal. Thus, data-rich organizations need to rely on AI to strengthen their defenses as a means to stay at least one step ahead of the adversaries who use the same technology. Since countering cyber-attacks is no longer a human-scale operation, AI enables cybersecurity teams to form powerful human- machine partnerships

that drive cybersecurity in a way that shrinks the attack surface and improves the organization's security posture. The purpose of Section 1 is to form the groundwork to transition into the research by providing the essential information to inform the readers and future researchers about what has been established concerning the defenses against AI-powered cyber-attacks against technology organizations. The following section focuses on the research method and data collection; it presents the methodology and procedures related to the field study, offering the researcher a framework for answering the research questions. Section 2 allowed the researcher to define the project through reflection on the purpose statement; it identified the role of the researcher and participants in the research. It also discussed the research design and methodology and provided details on the population and sample method, the data collection process, and data analysis.

Section 2: The Project

This qualitative multiple case study research involved analyzing multiple cases to understand a phenomenon or process. In this study, the participants were selected based on their relevance to the research question, and the population are a group of individuals that share a common characteristic. The sampling method for this research involved purposive sampling, where the cases are selected based on their ability to provide rich and diverse data that can help answer the research question. The cases were selected based on certain criteria, such as their relevance to the research question, their accessibility, and their willingness to participate in the study. The sample size for a qualitative multiple case study research included 15 Information Technology professionals from different technology organizations nationwide. Data collection in this qualitative multiple case study research involved using multiple sources of data to provide a comprehensive understanding of the phenomenon being studied. The main data source included interviews with professionals from different organizations with the information technology sector. The data collection process was iterative and ongoing, with data collection and analysis occurring simultaneously. The collected data were analyzed using a variety of techniques, including coding, categorization, and theme identification. The organization plan involved creating a data management system to organize and store the data collected. This system included procedures for data entry, coding, and storage, as well as protocols for data security and confidentiality. The data were analyzed using qualitative data analysis software, while the findings presented using thematic analysis to provide a detailed and comprehensive understanding of the case being studied.

Purpose Statement

The purpose of this flexible design multiple case study was to explore how AI and ML-based technology can affect organizations' cybersecurity. The research sought to determine the

threat AI can pose an organizations' assets and the tools used by adversaries and cybercriminals to conduct AI-powered cyberattacks, data breaches and malicious activities that can damage business assets and reputation. Since AI in cybersecurity is a two-edged sword, the research shed light on the benefit of AI to the cybersecurity field as well. Shakeel (2021) stated, “Intruders employ new methods and launch more comprehensive strategies based on AI to compromise systems. Similarly, organizations have started using robust defense systems that use AI (AI) to fight AI-powered cyberattacks.” Therefore, this study examined the measures technology organizations in the United States can take to control such malicious attacks by answering the research questions that specifically seek to discover existing trends in AI-based cyber-attacks and cyber defenses. Exploration of the problem occurs through an in-depth study of the negative impact technology businesses across the United States experienced as a result of cybersecurity threats in AI-based technology and the countermeasure taken to deter, mitigate or prevent them using the same type of technology.

Cybercriminals employ AI to power cyber-attacks in several ways, including social engineering attacks by detecting patterns in behavior that they use to manipulate behaviors, gain access to sensitive information, and compromise networks. Human hackers can use AI to develop mutating malware to mutate software from detection; ML can help in data manipulation, which can have a devastating impact on technology business. According to Munk (2022), adversaries take advantage of AI to identify network vulnerabilities. Fortunately, AI enables defense methods and services to detect and respond to cyber threats, which allows organizations to invest in ML technology to secure their networks and enhance their defenses against automated attacks, investing in robust cybersecurity systems that use the detection capabilities of AI and ML can form robust defense systems that can detect abnormal behaviors, automates identification, and mitigation

operations. The study intends to extend the current body of knowledge by identifying existing methods and techniques used to execute AI-based cyber-attacks.

Role of the Researcher

In qualitative research, the researcher is considered the primary instrument for collecting and analyzing data. According to Creswell and Poth (2018), the researcher has access to the participants' natural environment, which enables him to perform data collection and analysis. To ensure the integrity of the study and the safety of participants, researchers must abide by the principles of the Belmont Report which is found to protect the rights of research respondents. The researcher is obligated to be aware of biases and try to eliminate them in the study. In the data collection phase, the researcher used different interview protocols in order to ensure the reliability of the study. Negative assumptions cause major mistakes in qualitative research due to the conflict that could occur between the participant's truthful feedback and the researcher's idea. This conflict interrupts the overall research process and drives a specific conclusion. Therefore, the researcher remained conscious of the previous ideas and understandings to identify potential biases, which helped ensure accurate research outcomes (Teherani et al., 2015).

Ponelis (2015) mentioned that researchers transcribe participants' responses to analyze them and find potential themes after the interviews. In this study, the researcher was the only interviewer and focused solely on analyzing the data gathered from respondents to ensure mitigating personal biases in the research. Yates and Leggett (2016) emphasized that the role of researchers in a qualitative study is participatory and action research, which includes different data collection means such as interviews, focus groups, and open-ended survey questions. The researcher used open-ended questions for data collection in this research study. Creswell (2014) indicated that the primary role of the researcher is to lay out the foundation of the study by providing adequate details

about the nature and significance of it. This process helps answer questions related to the basic characteristics of the study. Part of the layout is determining which methods will be used to perform the study. In the case of this study, the researcher used a qualitative research design to investigate the malicious side of AI and its effect on internet security while addressing the size of damage related to AI-related cyber-attacks and data breaches.

The researcher is responsible for bracketing out any personal experiences and thoughts through the epoché process, in Greek philosophy, "suspension of judgment" (p. 85) indicated by Moustakas (1994) in order to explain a problem in terms of its own inherent system of meaning, it helps researcher set aside all his beliefs and assumptions about a specific problem and the issue presents itself in the world of the participant, examining the research problem this way enables the researcher to understand the perseverance experiences of participants fully. Stake (2010) stated that "for qualitative research, the researcher him- or herself is an instrument, observing action and contexts, often intentionally playing a subjective role in the study, using his or her own personal experience in making interpretations" (Stake, 2010, p. 20). Additionally, the researcher of this study has no knowledge of, or a relationship with, any of the individuals who are participants. Protecting the rights of participants is another essential task the researcher was responsible for throughout the research. That is, protecting the integrity and validity of the study and ensuring the privacy and rights of study participants throughout all the research phases. The study relied on the experiences of participants rather than focusing on the researcher's interpretation of the details (Moustakas, 1994).

In this research, the researcher designed the study, protected the overall study, including the privacy and rights of research participants, performed data collection, and analyzed, interpreted, and reported the results and findings. Stake (2010) acknowledged that researchers must be involved

in designing the study by formulating, planning, organizing, and implementing procedures of the study. As part of the design process, the researcher must determine data collection techniques appropriate to the study (Stake, 2010). For example, in this research, the researcher identified interviews as the data collection tool that is appropriate to achieve the purpose of the study. The interviews are practical data collection tools for collecting different data types required to reach data saturation. The integration of the data gathered through interviews achieved the desired study outcome for the multiple case study research (Creswell & Poth, 2018). The researcher identified an efficient way to interview participants, the interviews were conducted through telephone. The researcher determined the amount of data that needs to be gathered to sufficiently answer the research questions (Fusch & Ness, 2015).

Summary of Role of the Researcher

In conclusion, the qualitative researcher must have knowledge and understanding of the study participants' social setting while incorporating positionality, reflexivity, and subjectivity. It is important for the researcher to build their skills by devoting time, talent, and resources to ensure the success and credibility of the research project. Additionally, researchers have to be aware that they are a research instrument, and their ideas and beliefs about the study can easily distort the outcome of the research. Therefore, the researcher was aware that examining own beliefs and judgment is necessary to eliminate negative assumptions that are considered a major source of error in qualitative study. The researcher applied reflexivity during the data collection phase to eliminate bias which results in incredible research.

Research Methodology

The purpose of this qualitative, multiple case study research was to explore how cybercriminals and adversaries benefit from AI technologies to achieve their desired objective

either by promoting attacks or conducting automated cyber-attacks that are hard to be contained by organizations. While researchers can select quantitative, qualitative, or mixed research methods (Edmonds & Kennedy, 2017). The researcher determined why the qualitative method is the most appropriate for this study in detail and explained how this method, along with the triangulation approach used for the multiple case study, achieved data saturation, and came up with the desired findings. This study's proposed research method and design is a qualitative, flexible, multiple case study. The researcher selected pragmatism as the research paradigm representing the view of reality and truth for applied business research; the researcher explained how this worldview can guide the study. This section described the research methodology by determining the design and method to study the problem at a very high level, as well as the rationale of the selected design and method. The researcher explained why choosing the qualitative research method and using multiple case study designs to conduct the research. Lastly, the researcher utilized triangulation to analyze results using data collection methods to enhance validity and interrogate various means to better understand the research problem (Kobayashi, 2019). The study supported the function of the selected research paradigm and methodology with multiple citations in order to emphasize their effectiveness to guide the study.

Discussion of Flexible Design

The research can be conducted using three methods: quantitative, qualitative, and mixed methods (Creswell, 2014). This study was conducted with a flexible design using qualitative method(s); specifically, a multiple case study design was used. The qualitative research design is appropriate for this study because the aim is to investigate a particular topic through exploring and understanding the research problem (Stake, 2010). The research method provided a better focus on objectivity, providing the permittance to generalize findings beyond a particular setting (Fletcher et

al., 2016). Creswell and Poth (2018) indicated that qualitative research allows researchers to rely on the collection and analysis of data to explain and describe research findings. The qualitative research method provided the research with the tools to propose solutions to the research problem by better understanding how organizations respond to AI-related cyber threats and what effects cyber threats have on the technology business. The researcher decided not to select quantitative research designs due to the common weaknesses in capturing the subtleties and complexities of individual human behavior. In comparison, it is possible to capture it using a flexible design. In the study, the researcher has no intention to capture group aggregates which mainly involve fixed design. According to Robson and McCartan (2016), "fixed designs are usually concerned with aggregates: with group properties and with general tendencies" (p. 103). Therefore, fixed designs present the danger of ecological fallacy. With fixed design, some problems come under the heading of reliability. The unreliability of fixed design has various causes, including participant error, participant bias, observer error, observer bias, and types of validity (Robson & McCartan, 2016). In terms of multi-strategy design, the researcher avoided using the design due to the complexities and concerns that may produce disjointed and unfocused research. Regnault et al. (2018) identified some disadvantages in the mixed method, one of them is the application of multi-strategy design that can potentially raise practical concerns when integrating both qualitative and quantitative data as the integration process may require additional resources and time. There are also some uncertainties in mixing two differing paradigms in the same research study. "Some theoretical debate still exists on how - or even whether - quantitative and qualitative paradigms can be mixed" (Regnault et al., 2018, p. 3). Mason (2006) indicated that multi-strategy design could severely test the capabilities of the researcher due to the complexity of its implementation. Mixed methods design may require more expertise to gather and analyze data and interpret the findings. In the real

world, combining different methods requires extra resources and can establish certain constraints caused by practical, political, and resource issues (Mason, 2006). Therefore, the researcher focused on one method to ensure the ease of the data collection process.

Discussion of Multiple Case Study

The specific method for this study is a multiple case study. The design of this proposed flexible qualitative study aims to find answers to the research questions by determining the effects of AI-based technology on cybersecurity and how it affects business strategy and decision-making over time. The multiple case study seeks to understand the situation related to the problem through answering research questions and in-depth examinations of the different cases using archival data (Brown, 2020). It explored the events surrounding the problem by examining the interaction between different components that involve people, activities, and business policies. The research is conducted on high-tech cybersecurity organizations and explored how investing in AI can overcome security threats. Stake (2006) stated that the multi-case study is a special effort to examine something having lots of cases, parts, or members. In the study, the researcher followed Stake's approach and defined multiple-case studies as being investigations of a particular phenomenon (or group of phenomena) at several different sites. This does not preclude a multi-case study from being conducted within one organization. Stewart (2012) identified three sequential processes or tracks of the multiple case study analysis. The first stage identifies themes in each of the cases, maintaining situational detail. The second track identifies factors, and the third track is the cross-case analysis, which involves generating a case-ordered descriptive matrix that establishes a basis for comparing the cases on several factors.

Qualitative research includes five design approaches narrative, phenomenological, ethnographic, grounded, and case study approaches (Creswell & Poth, 2018). After examining all

of the research methods and comparing them to each other, the researcher realized that the multi-case study is the most appropriate method for this study and made a choice not to use a single case study due to the significant potential difference between single and multi-case studies in terms of the range and reach of the multi-case study. Stewart (2012) indicated that, unlike the single-case study, all cases in the multi-case studies are chosen for their similarities rather than their differences and that multi-case studies are essence comparative. As a multi-case researcher, the researcher is interested in using contrast or variance as a significant research tool for the case under study. Fitzgerald and Dopson (2009) denoted that the multi-case study researcher could examine the differences and similarities between cases within a specific context. Qualitative research aims to more fully understand the phenomenon studied contextually from the participants' perspective (Creswell, 2014; Creswell & Poth, 2018; Fletcher et al., 2016; Stake, 2010). Creswell (2014), Creswell and Poth (2018), and Yin (2014) advised that the case study research design is most suitable for researchers to explore a given process within a specific context or bounded situation. A case study researcher's goal is to obtain descriptive content to better understand the phenomenon of interest (Creswell & Poth, 2018). Creswell (2016) suggested the case study design for the exploration of a specific issue. Yin (2014) shared that the use of multi-case studies can produce more robust and compelling results. Mumford et al. (2009) cautioned researchers on the single case study's limitation of generalizability. Therefore, the researcher chose a multi-case study methodology for this study to achieve data saturation and improve the generalizability and validity of the findings.

The phenomenological methodology is not appropriate for this research because participants do not encounter a unique event together, which presents the risk of expanding beyond the limited scope determined for this study. The researcher intends to stay focused on the intended

study and within the scope by obtaining information from participants on the negative effect of AI on Cybersecurity. According to Bondwe (2019), the phenomenological approach is appropriate to explore the lived experiences of the individuals of a phenomenon, which can be used to study how individuals interact when experiencing AI-related cyber-attacks. However, that is not the primary focus of the study, it is absolutely part of it, but the data collected using the phenomenological approach did not cover the intended topics the researcher intended to cover. Creswell (2007) acknowledged a common challenge of using the phenomenological method, which is the difficulty of bracketing personal experiences, which requires the researcher to decide how to introduce his personal understanding into the study.

Narrative research is an old research tradition. It illustrates individuals' life stories (Lewis, 2015; Morawski & Rottmann, 2016). Creswell and Poth (2018) mentioned that narrative research is appropriate when studying a phenomenon involving a single person or a small group of individuals, typically two or three individuals. The individual provides his or her unique personal experience for the researcher, researcher record the story and experience of the participant. In this research, the researcher interviewed several individuals, not only a few and collected information from many participants in different businesses across the technology industry in the United States. Since the intent of this study is not to record a human's story chronologically nor to interview a single or a few individuals to collect data. Therefore, the narrative design is not a good fit for this study.

The ethnographic research method stems from anthropology and sociology, where the researcher explores shared patterns of behavior, language, and actions of a specific sample within the same cultural group over an extended period (Creswell, 2014). According to Creswell and Poth (2018), ethnography researchers conduct research in a "culture-sharing" environment. Ethnographers observe social behaviors and explore patterns of life surrounding a group of

individuals (Ting-Toomey & Dorjee, 2018). Grey (2016) indicated that patterns of life include different activities within the cultural cycle. These cycles could be beliefs, dialects, festivities, or spiritual lifestyles. The ethnographic research method is inappropriate for this study because it is designed to examine in detail the cultural characteristics of the work environment, which did not contribute to gaining a good understanding of the research problem in the case of this study. Therefore, the ethnographic approach to inquiry was ruled out.

The grounded theory research defers from all other approaches as it does not focus on individual/group stories nor highlights shared experiences. It instead aims to generate or uncover a theory (Creswell & Poth, 2018). Creswell and Poth (2018) described grounded theory as a process or action performed by a researcher who seeks to explain an emerging theory of a specific plan. In the grounded theory approach, the researcher grounds the theories that he or she develops in the data that was collected from individuals or groups who had somehow experienced part of the process or action. Researchers then record and analyze data. Stake (2010) acknowledged that the grounded theory approach focuses on the generation or discovery of a theory. Investigators use memo writing techniques to shape the process and to record and analyze the gathered data (Johnson, 2016). The grounded theory method is appropriate to advance or identify a theory because it considers the perspectives of the research participants to explain a specific process, action, or interaction (Creswell & Poth, 2018). This study does not seek to develop emergent theories about the processes, actions, and interactions carried out by AI and cybersecurity professionals dealing with AI-related cyber-attacks. Therefore, the grounded theory design is not appropriate for this study.

Discussion of Methods for Triangulation

The researcher used multiple methods of qualitative data triangulation to address the

research questions; in this study, the researcher intends to use triangulation as a research strategy to confirm and validate the quality results of the study (Carter et al., 2014). Robson and McCartan (2016) emphasized that triangulation is a valuable strategy that has many advantages to the study, triangulation enhances the rigor of the research and helps to counter all of the threat of validity. Triangulation achieved objectivity, truth, and validity (dependability and credibility) of research by using multiple sources instead of a single source, which provides the researcher with more insights and enable the researcher to recognize and remove inconsistencies (Fusch et al., 2018). To study this information systems business problem, the researcher used interviews and member checking. Interviews were used as the most common qualitative data collection methods to collect data pertaining to the effects of AI-related cyber-attacks on the technology organization in the United States; The use of semi- structured interviews and member checking led to the development of different datasets and helped achieve triangulation. The results from the datasets were analyzed independently then compared to each to determine if results lead to the same conclusions. The use of interviews and member checking as a qualitative method provided validation through triangulation and proved to yield accurate and concrete results and findings.

According to Nightingale (2019), triangulation is used to enhance the validity of research findings, create a more in-depth picture of a research problem, and interrogate different ways of understanding a research problem. Nightingale (2019) suggested that researchers look for three types of data triangulation - convergence, complementarity, and divergence. Convergence refers to the degree of overlap and accuracy between the data sets collected using different methods. The complementarity type clarifies the research results by allowing the results from different methods to inform each other while divergence presents a different set of challenges within the methods. Williamson (2017) noted that there are four common forms of triangulation: Data source

triangulation which involves using different sources of information to increase the validity of a study. Method triangulation which means the use of multiple methods in the same study to gather data, such as interviews, observations, questionnaires, and documents; theory triangulation involves using more than one theoretical scheme in the interpretation of the case (Guion, 2002). In this study, the researcher used the methodological form of triangulation to develop a comprehensive understanding of the case. The researcher followed a data collection plan that used interviews as the main data collection source and member checking to triangulate the qualitative study. The data collection plan assisted the researcher in obtaining the extra data needed to support the interview findings and reach data saturation.

Summary of Research Methodology

After reviewing the research problem and questions, the researcher determined the research paradigm based on the researcher's worldview, the research methodology, and the data triangulation methods for this study. The researcher explored all the primary research paradigms and identified pragmatism as the worldview that constitutes truth, and knowledge which guide the researcher's thinking, beliefs, and assumptions about the study. The researcher determined the design for this study to be flexible design using qualitative method, the research is conducted using multiple case study method for data gathering that helped finding answers to the research questions. The researcher used this methodology to investigate the use of malicious AI to conduct cyber related attacks, the research methodology determined for this study helped exploring and understanding the research problem, it summarized the research process and determine how the research proceeded. The study used data triangulation to address the research questions, the researcher utilized interviews and member checking to collect data and ensure the validity of the research results. The research approach determined for this study aimed on understanding the

connection between philosophical worldview and research methodology which helped the researcher find better ways to go about investigating the topic.

Participants

The study sought to interview participants who are currently or previously employed as information technology professionals at technology organizations and have knowledge in the Cybersecurity field. There were no limitations on the position function, gender, race, or ethnicity of the participants. Instead, the minimum required years of experience in the information technology field is two years of employment by their respective companies, and the minimum age of each participant was determined to be 23 years old. The researcher limited the required experience to two years to ensure sufficient exposure to the company procedures, policies, and culture. Several technology organizations are available nationwide, allowing a large sample of participants. Since the study focused on the Tech industry in the United States, Information Technology professionals were the ideal candidates who were able to share their experiences and thoughts to provide quality research data. The researcher interviewed eligible participants who could offer applicable answers to the research questions. Recruiting eligible participants impacted the quality of data gathered for the study by sharing their practices and thoughts related to the topic (Dempsey et al., 2016). Qualitative researchers must ensure that participants have the required experience with the case or phenomenon being studied (Farooq & de Villiers, 2017).

Yin (2018) mentioned that participants who meet the research requirements should be able to provide relevant information about the central research questions. Before conducting the field study and selecting the participants, the researcher prescreened the eligibility of each participant to determine the criteria. Throughout prescreening, the researcher decided who can provide relevant information to the study (Yin, 2018). The researcher looked for knowledgeable and experienced

interviewees. The researcher took appropriate measures to initiate contact with employees, multiple ways of contact were used to reach out to participants, including email, LinkedIn, phone calls, in-person contact, etc. The study required research participants to sign an informed consent document before participation. Research participants aided the study by providing experiences with operations, functions, and everyday responsibilities of their current and past security teams and the influence of the organization's decision-making (Jogaratnam, 2017).

Population and Sampling

The population for this research study consisted of current and previous information technology professionals with knowledge in IT security and cyber defense of the technology organization in the United States. The population included employees in different career levels. Qualified participants who consent to interviews were required to be aware of the cyber threats faced by the organization they are currently affiliated with or were affiliated with throughout their careers. Yin (2014) emphasized that case study participants can provide valuable information and interpretations of the phenomenon under study. This study used purposeful sampling in conjunction with the snowball sampling method to recruit eligible research participants. The selected population sample ensured data saturation and an in-depth understanding of the research problem.

Discussion of Population

The target population for this qualitative multiple case study was 15 Information Technology professionals who have experience in the IT field and specific knowledge in the cybersecurity part of the field in their respective organizations. The population could include employees in different career levels; there were no limitation on the positions and roles of employees. To ensure data diversity and saturation, the researcher explored the research problem from different perspectives of individuals with varying types of experience and positions in the

Information Technology field as long as they meet the minimum experience required to participate in the research (Robson & McCartan, 2016). Employees can be team members, managers, supervisors, high-level management professionals, etc., depending on their eligibility to participate in the study. Research participants were selected from an effective technology organization within the technology sector in the United States. Eligible Populations must have knowledge of different types of cyber-attacks, including these attacks powered by AI and ML. There were limitations on the years of experience participants have in the IT field. The researcher found it necessary to set this limitation to ensure that the research respondents have sufficient knowledge and experience to provide valuable information to the research. In addition to knowledge and expertise, participants must be well familiar with their organization's procedures, policies, and culture. The minimum required experience was 2 years in the information technology field. Mathews (2018) indicated that the researcher must be selective when determining the research populations and participants. Selecting appropriate participants increases the reliability and validity of the data. Therefore, this study only sought suitable candidates that meet the participation requirement.

Discussion of Sampling

The researcher used two sampling methods in this study: purposeful sampling, commonly used in qualitative research, and snowball sampling or chain-referral sampling. In the purposeful sampling method, the researcher selects individuals and sites for the study and can directly contact the potential research participant. Selected individuals can purposefully inform the research and understand the research problem and central phenomenon of the nature of the cyber-attacks on the technology organizations in the United States (Creswell & Poth, 2018). Snowball sampling is purely based on referrals; it identifies cases of interest from individuals who know about others who know about cases that are valuable to the study (Creswell, 2007). The researcher can generate

the sample by getting referrals from other participants and organizational members if necessary. In snowball sampling, the primary data source nominates other data sources for potential participation in the research study. The inquirer is responsible for making the decision on how many sites and individuals need to be sampled (Creswell, 2007). This study used maximum variation and critical case as the sampling strategies. Maximum variation sampling strategy ensured documenting of diverse variations and the discovery of common patterns. In contrast, the critical cases sampling strategy ensures the availability of specific information about people and sites, which provides easy access to the sample and data collection. This study used nonprobability sampling as a common qualitative study sampling approach. In this approach, the sample is selected in a non-random way. Although nonprobability samples are much easier to achieve, they have more risk of bias if the researcher chooses a sample based on the most convenient and accessible members of the population. Therefore, the researcher was aware of the limitations and carefully considered potential biases.

The sampling frame of this research was specific positions and titles of the participants within the population. According to DiGaetano (2013), the sampling frame is the actual list of individuals from whom the sample will be drawn. The sampling frame is the specific individuals selected from the target population that the researcher intends to cover in the study. After defining the population's requirements, the sampling frame helped the researcher specify the individuals that meet the requirements of the study. Population generalizes the study group and does not specify the participant, while the sampling frame selects participants from the general group.

The sample size of this qualitative research included 15 Information Technology professionals from different technology organizations nationwide. Selecting individuals with different positions from different organizations helped achieve the goals of this multiple case study.

According to Tran et al. (2016), in qualitative research, sample size is relatively small and is very labor intensive, preforming analysis on a large sample is time consuming and often impractical. Thus, reaching data saturation is influenced by sample size during the data collection process. In this study, researchers are concerned with the meaning of the gathered information and not making generalized hypothesis statements. The sample size was large enough to ensure that it covers all the research areas by gaining insights from different expertise in the field. Although larger samples could help to validate data, the researcher avoided large samples as it can potentially generate repetitive and eventually, superfluous data. Therefore, selecting an appropriate sample size contributed to generating the required data to achieve data saturation. The data collection plan for this research aimed on achieving saturation, the researcher's course of action in case data saturation could not be achieved with the pre-determined sample size was to continue interviewing participants until reaching the saturation point. Data saturation was reached after interviewing 15 participants, the researcher started getting similar responses from the participants, themes and subthemes started emerging through the interview process.

Fusch and Ness (2015) emphasized that data saturation is achieved when researchers stop obtaining new data from participants and only get repeated information that is not useful to further support the research. To ensure saturation, researchers continued to interview participants until the collected data became mostly consistent to the point where the information has little to no significant impact on the study. The researcher conducted thematic analysis after the interviews to check for any new themes and patterns emerging from the data collection. Once identified repeated themes, the researcher ended the interview process as an indicator that saturation point was reached. In qualitative research, the researchers are responsible for determining the saturation point by using their judgement to decide whether participants are providing new data or not. After data

coding and thematic analysis, researchers must be able to draw conclusion on the saturation point (van Rijnsoever, 2017). The collected data helped explore the research problem from the perspective of various organizations with different cybersecurity assets, capabilities, policies, and procedures. After identifying the participants, the researcher started the procedures for gaining access to the sample by initiating contact with the participants. Explanatory conversations were used to communicate the intent and conceptual framework of this academic study to the research participants. The conversation recognized the benefits of exploring research problems in increasing academic and practical knowledge. The researcher introduced the nature of the research to the participants by explaining the benefits and goals the researcher wants to reach. The researcher allowed participants to ask questions related to the nature and scope of the study.

To gain access to the sample, the researcher communicated the worthiness of the study and explained the benefit it adds to the specific field of study and assured that the research will not result in any harm to the participants. Finding successful strategies to gain access to the research sample is important. Gaining access to the sample required the researcher to have knowledge in the operational hierarchy of the organization to be able to find participants. Ensuring a successful access to the sample requires the interviewer to adopt a formal stance and professional etiquette (Wassenaar & Singh, 2016). The researcher kept the commitment to ensure that anonymity and confidentiality of the study sample is preserved. This research ensured that the information collected in the study will not be used immorally or illegally and that the study sample members are respected and dealt with ethically. The study intended to provide a safe environment to the research participants to speak openly about their experiences. Therefore, after human subjects' research practice, participants signed an informed consent. The informed consent allowed participants to exit participation at any time.

Summary of Population and Sampling

This qualitative, multiple case study utilized a population of Information Technology professionals from different Technology firms in the United States. The expertise of the research participants provided a unique opportunity to gain insights into an emerging business problem in the technology world. In this research, the goal is not to test a hypothesis about a large population but to develop an initial understanding of an under-researched problem and to deeply understand a specific context, not to generalize to a population. The researcher had a clear rationale for why this particular case is suitable for answering the research questions and collected as much data as possible about the context. Participants in this research were selected in a non-random way using the nonprobability sampling approach. The combination of purposeful and snowball sampling methods simply included individuals who were easily accessible to the researcher. The two methods were effective to collect in-depth information from the right respondents and achieve data saturation.

Data Collection and Organization

Data collection helps support the research and is an essential part of all qualitative research studies. Data collection generates new data that can be compared to the existing data for better results. In this qualitative multiple case study, the researcher captured the right information through different sources to better understand the research issues and draw conclusions on the potential solutions to the research problem. McMahon and Winch (2018) mentioned that data organization involves collecting, managing, storing, retrieving, analyzing, and coding the data collected during the study. Stake (2010) indicated that all research inquiries require data collection and interpretation. This research examined multiple cases involving AI and ML's impact on cybersecurity. The qualitative method multiple case study design involved in-depth data collection

using qualitative data sources to enhance the reliability and validity of the data (Creswell, 2007).

Data Collection Plan

This case-study data collection process aimed to capture common themes and patterns from study participants to explore the nature of AI-related cyber-attacks against organizations. The collected data were organized and prepared for data analysis. The researcher conducted semi-structured interviews with cyber security and AI experts. The researcher collected the data through interviews followed by member checking. The semi-structured interviews explored participants' understanding of each case study context (Marshall & Rossman, 2016). The researcher interviewed eligible participants that meet the research criteria. Interviews were conducted via phone, each interview was recorded and transcribed. The researcher used open-ended questions to allow participants to express their thoughts and experiences in their own words. This method allowed for rich data that can be analyzed in detail (Braun & Clarke, 2019). The researcher purposively drew 15 participants from the research population for interviews. The semi-structured interviews used open-ended questions, this type of question allowed the researcher to ask follow-up questions to build upon the initial answer and obtain more in-depth information from the participant. The interviews were audio recorded to help the researcher transcribe the answers. Following the data transcription and interpretation, the researcher provided participants with a copy of the interview answers for their review. There were some strategies for purposefully selecting participants to learn the most about the case or the problem under study. Selecting participants was very purposeful and nonrandom. The researcher subjectively chose individuals that can contribute insight into the topic. Although the researcher specified the number of individuals to be interviewed, the researcher was aware that it might be necessary to interview more participants in case data saturation is not reached. The collected feedback and responses is analyzed after each interview and during data

collection to find themes and insights. The discovered themes helped determine how much more data needed to be collected and whether the researcher needs to continue collecting or whether data saturation was reached. The researcher sought to gather first-hand information to help with the systematic investigation and guide the results.

In qualitative research, bias can be presented by both participants and researchers; in this study, proper measures is taken to prevent bias from both sides. Creswell and Poth (2018) defined data collection as systematically gathering and evaluating data to answer emerging research questions. Data collection is fundamental to finding answers to research questions by interacting and building rapport with the interviewees. The researcher was aware of the responsibility to maintain integrity and mitigate biases and personal assumptions during the data collection stage of the study. Integrity and biases can impede the researcher from achieving valid and reliable results (Bondwe, 2019). The researcher performed member checking to ensure data accuracy by requiring participants to review the interview transcripts and provide feedback and insights (Creswell & Poth, 2018). The researcher protected the anonymity and confidentiality of the participant by removing any identifying information. This research intended to create a safe environment for the participants to express their opinions honestly and transparently. Consent forms were provided to the participants with the option to exit the research anytime. Lastly, research data were secured in a password protected computer with the secure access for 3 years to avoid data loss and damage. NVivo software was used as a qualitative analysis tool for this study. Member checking was conducted to ensure the credibility of the qualitative study by allowing participants to confirm or deny the accuracy of data provided during the interview. Robson and McCartan (2016) acknowledged that member checking is a very valuable way to protect the research against researcher bias. It expresses the researcher's appreciation of the participant's contribution to the

study. Member checking is integral to creating trustworthiness in qualitative research (Creswell & Miller, 2000; Lincoln & Guba, 1986; Stake, 1995). It is commonly used to maintain validity in qualitative research (Candela, 2019).

Instruments

The researcher was the primary instrument for collecting data, and collected information directly from participants through interviews, then compared it to other data collection sources to ensure validation of the information. Stake (2010) indicated that human researchers are often the primary research instrument in qualitative studies. According to Robson and McCartan (2016), a researcher must be flexible when conducting flexible-design research, and the approach to research makes a great demand on the researcher. It does not rely on specialist tools and instruments, the approach commonly known as 'researcher-as-instrument.' They added, "the quality of a flexible design study depends to a great extent on the quality of the investigator" (Robson & McCartan, 2016, p. 148).

Interviews were the primary approach for data collection in this multiple case study; interviews can be used as the primary and only data collection technique in the research due to their flexibility. Yin (2018) stressed that case study interviews are most commonly semi-structured, which include open-ended questions that seek respondents' opinions about an event. The interview questions were designed to allow the respondents to tell their stories and experiences by asking questions that allow the conversation to flow freely. Open-ended questions led the researcher to uncover new topics within the subject matter that he was not aware of previously. This helped the researcher to collect meaningful data.

The researcher utilized a less structured interview type to approach participants because it allows the interviewee much more flexibility in answering research questions. Therefore, a semi-

structured interview was the best fit for this study. It allowed the researcher to ask follow-up questions should the participant mention new information during the interview. Semi-structured interviews did not limit the researcher to specific questions (Creswell & Poth, 2018). Semi-structured interviews commonly used interview guides to keep the researcher on track to address the interview questions. The interview guide for this research included a list of questions covered during the interviews. It ensured the researcher covers all the topics needed to answer the research questions. The interview guide in this research acted as an unobtrusive road map the researcher could turn to during the interview to get back on course. The interview guide provided the researcher with prompts and general direction.

Interview Guide. An interview guide is an outline that helps the researcher cover topics and key concepts during the data collection. The interviewer addressed the research questions with proper interview questions to clearly address the problem. The interview questions for this research were written in plain and nontechnical language with no ambiguity to ensure that the interviewees understand and answer the questions freely (Creswell & Poth, 2018). The interview questions are based on the different effects of AI and ML on cybersecurity. There are four main interview questions that have at least one sub-question each; the researcher addressed each research question with a proper set of interview questions. The interview questions consisted of four areas. The researcher designed each area to address part of the research questions with specific interview questions about the topic. Each of the interview questions area assisted in examining the relationship between the research findings and the problem under study though a set of detailed questions. These areas included the negative and positive impacts of automated cyber-attacks on network security. The researcher crafted eight interview questions to address the negative impact and another eight questions to address the positive impact. The questions focused on the malicious

use AL/ML technology by cybercriminals, the type of AL/ML cyber-attacks attacks and the damage it cause the organizations. The financial implications questions included the effect of AI/ML-related cyber-attacks on organizations and customers as well as the role of decision makers in taking critical financial decision in case of cyber-attacks. Investment in AI/ML-based technology included questions related to the effect of investment in AI/ML-based technology to protect the network from automated attacks and data breaches. Employees awareness and compliance included questions regarding how important it is to raise employees awareness to prevent AI related cyber-attacks. AI governance addressed the level of governance on the AL/ML tools that are available online for public use. AI deterrence addressed the techniques can be used to predict and prevent cyber-attacks before it occurs to avoid the damages it can cause after its occurrence. Lastly, Cloud Computing and IoT area of the interview questions addressed the effect of AI/ML technology on Cloud Computing and the growing attack surface of the Internet of Things (IoT).

The open-ended questions allowed the interviewer to discover more facts about the problem by asking follow-up questions. All interviews were audio recorded to preserve the accuracy of the answers and to ensure capturing the important interview details. The interviewees signed an informed consent to acknowledge that the interview will be audio recorded. Creswell and Poth (2018) recommended the interviewers use a recording tool to ease the data collection process and avoid missing important inputs from the research participants.

Data Organization Plan

Merriam (2009) indicated that data organization enables a researcher to access any piece of data anytime needed and that data management and organization put the researcher in control over the large amount of data collected during the research project. Krathwohl (2009) acknowledged that valuable insights and information from interviews must be recorded, and relying on the

interviewer's memory can cause such an issue. Therefore, this research utilized audio recordings in the interview process. The researcher transcribed the audio recordings into a Microsoft Word document. The researcher ensured that the transformation process from audio to text through transcription did not include any identifying information to protect the confidentiality and anonymity of the participants. The researcher followed the IRB protocols pertaining to record retention and data destruction by keeping all audio recordings for 3 years following the study. During the data collection phase of the research, the researcher maintained a journal to reflect on and bracket out any ideas, thoughts, or assumptions related to the phenomenon under study. Any journal or notes captured by the researcher was kept in an MS Word document and used during data analysis and coding. To organize data researcher utilized NVivo software to store and organize data. NVivo is a data management tool that can identify patterns and perform data querying and visualization. NVivo served as a repository for interview notes, interview audio transcripts and research journal notes. The software allowed the researcher to classify and categorize gathered data and identify data patterns to find codes (Robson & McCartan, 2016).

The purpose of data organization is to prepare the data for analysis. Data organization for this study was done in three steps: data transformation, cleaning, and classification. Data transformation aimed at having all data in one format. That included moving the data from one format to another, such as moving it from an audio format (MP4 file) to a textual format (Word document) and then importing it to a qualitative data analysis software. The cleaning stage of data organization included looking for verbatim transcribing, eliminating nonverbal cues, and marking spaces of silence. Because the ways in which something is said is important, the researcher read the verbatim textual transcript and corrected things that were not interpreted correctly and removed all the identifiers to ensure that the research follows the IRB protocol. Classifying data is required

before the analytic process. It is basically trying to identify the characteristics of the data and getting it ready for coding, particularly using qualitative data analysis software. Yin (2014) emphasized the importance of organizing case study data in several forms, such as notes, documents, and audio-recorded interviews. The researcher reviewed the interview transcripts and highlight notes written about emerging themes to further use in the data analysis phase.

Member Checking

This research utilized member checking as a means of study validation, which involved sharing research findings with study participants to get their feedback and validation. The technique supported data triangulation by providing a way for the researcher to ensure the accurate portrayal of participant voices. Triangulation is an effective strategy to counter all the threats to validity. The technique used multiple sources of data collection to enhance the rigor of the research (Robson & McCartan, 2016). Member checking ensures the credibility of the qualitative study by allowing participants to confirm or deny the accuracy of data provided during the interview. Robson and McCartan (2016) acknowledged that member checking is a very valuable way to protect the research against researcher bias. It expresses the researcher's appreciation of the participant's contribution to the study. Member checking is integral to creating trustworthiness in qualitative research (Creswell & Miller, 2000; Lincoln & Guba, 1986; Stake, 1995). It is commonly used to maintain validity in qualitative research (Candela, 2019). The researcher provided a copy of the interview transcript to each participant after the interview to confirm the accuracy of the information provided during the participation in the research. The researcher asked the research participants to email him back in case of any changes needed to be made to the transcript.

Follow-up interviews

While member checking and follow-up interviews are two methods commonly used in qualitative research to enhance the validity and reliability of data; they differ in their approach and purpose. Rubin and Rubin (2012) described follow-up interviews as a method for clarifying or elaborating on the initial findings of a qualitative study. They suggest that follow-up interviews can be especially useful in cases where the initial interviews yielded ambiguous or conflicting data (Rubin & Rubin, 2012). Charmaz (2006) argued that follow-up interviews can be a valuable tool for generating new insights and refining the researcher's understanding of the phenomenon being studied. She noted that follow-up interviews can help the researcher explore unexpected findings and identify patterns or themes that were not apparent in the initial data. Follow-up interviews are particularly useful when the initial data are incomplete or ambiguous, or when the researcher needs more information on a particular topic. Follow-up interviews can also help the researcher to increase the trustworthiness of the findings and validate them by cross-checking information obtained from multiple sources (Charmaz, 2006). In this research, the researcher did not find the need to follow up on more details or clarifying any ambiguity from the initial interview with the participant and no new interview questions arise from responses to the initial interviews.

Summary of Data Collection and Organization

In summary, the primary data collection sources for this study was interviews. In this research, the researcher was the primary instrument for data collection and collected the data correctly from the research participants. the researcher used interview guide as a research instrument, interview guide assisted in addressing the research questions and allowed for in-depth exploration of the research questions, provided rich data that can be used to build theories or identify patterns. Member checking was a valuable method to enhance the validity and reliability of

this qualitative research data. Member checking was useful for verifying the accuracy of the data (Candela, 2019). Qualitative data collection is instrumental in exploring complex social phenomena and understanding the meaning of the experiences and perspectives of individuals. According to Silverman (2016), qualitative research provides an in-depth understanding of social phenomena by collecting rich narrative materials. The researcher employed data collection techniques to better understand a research topic's nuances and complexities. The researcher addressed each research question with a set of interview questions to ensure getting the best answers possible from the research participants. For data organization, Interviews were audio recorded and transcribed to ensure the reliability of the data. In addition, the researcher maintained a journal to reflect on and bracket out any ideas and use NVivo software to store and organize data (Creswell & Poth, 2018). This research ensured the confidentiality and anonymity of participants during the data collection process by requiring participants to sign an informed consent and allowing them to withdraw their participation at any time in the research process.

Data Analysis

According to Creswell and Poth (2018), data analysis is a systematic process involving data organization, themes and patterns discovery, data coding and interpretation. The data analysis process primarily relies on the researcher’s critical thinking and analysis skills and ability to find relationships and differences within the collected data. Yin (2018) considered qualitative data analysis as a challenging phase as it entails reviewing several transcripts to identify significant themes and patterns within the data gathered in the data collection phase. Green et al. (2007) indicated that data analysis consists of four major steps, data immersion, data categorization, data coding and themes creation. During the data analysis phase, the researcher looked for similarities and differences in the participants' experiences and realities, which helped discover emergent

themes (Yin, 2018). The data analysis strategies for this qualitative research included several steps: discovering emergent ideas, coding themes, data interpretation, data representation, and analysis for triangulation.

Emergent Ideas

To find emergent ideas, the researcher conducted an initial review of the database by reading the transcripts quickly, browsing through all the transcripts, then making notes about the first impressions. After the initial review, a deep exploration took place by reviewing concepts, ideas, or themes emerging from the transcripts. Data immersion is one of the key steps of data analysis. It involves a deep level of involvement of the researcher with the object of study. The researcher was immersed in the interview data by reading and examining the participants' input in detail (Green et al., 2007). The researcher developed a good understanding of the database by studying the data to retrieve any piece of data in the data analysis phase. Using an inductive reasoning approach enabled the researcher to identify significant themes and patterns from the interview data using a coding scheme. Studying data includes reading the interview transcripts repeatedly to get a sense of emergent ideas before sorting out ideas into themes and starting the coding process. The researcher discovered data patterns and interpreted findings by identifying emerging themes and sub-themes. Thus, the researcher used NVivo qualitative research to gather transcripts, journals, and notes, categorized them into emerging themes and ideas, displayed the emerging patterns, coded them for similarities and differences, and found relationships within the participants' responses (Creswell & Poth, 2018).

Coding Themes

The purpose of coding is to identify patterns, relations and theories concerning coding. Creswell and Poth (2018) defined coding as the analytic process of exploring collected data line by

line or paragraph by paragraph and denote it as concepts. Data represent significant events, experiences, or feelings. A code can be a label, concept, or word that signifies what is happening in this data piece. Through coding, researchers label any important information in the text. Sutton and Austin (2015) pointed out that the researchers code data to understand the data collected during interviews. They define coding as discovering themes, relationships and issues within the data gathered from the research participants. Coding is one of the qualitative data analysis steps. After preparing and organizing the data for analysis, the process of coding and condensing the codes occurs to reduce the data into themes. The researcher used NVivo software to code data into themes. NVIVO is a powerful tool for coding themes, it has the ability to manage and analyze large amounts of data in a systematic way and provides a range of tools for exploring patterns and trends in the collected data. Once the coding step is completed, the researcher represented the data in figures, tables, and discussions. These steps are considered the core elements of qualitative data analysis (Creswell & Poth, 2018). Coding is a straightforward process when the researcher is fully familiar with the data, mainly labeling sections or passages of text with code words. The investigator employed research skills to identify interesting or salient data features related to the research questions or objectives. Regardless of the size of the database, the researcher limited developing categories of information to a certain number that allows the researcher to reduce and combine them into a few themes. Creswell (2007) recommended not to develop more than 25-30 categories, enabling a researcher to derive five or six themes. He mentioned, “those researchers who end up with 100 or 200 categories-and it is easy to find this many in a complex database-struggle to reduce the picture to the five or six themes that they must end with for most publications” (Creswell, 2007, p. 152).

Creswell and Poth (2018) asserted that the key steps of data coding are reducing the data

into meaningful segments, labeling segments by assigning names to each, integrating, and classifying all codes into themes, then representing the data and comparing using graphs, tables, and charts. The researcher labeled relevant pieces of data such as words, phrases, sentences, or sections in the transcripts. These labels can be about actions or activities or significant input from the transcript. The researcher knows that the data are relevant to the code when repeated in several places, or perhaps it surprises and gets the attention of the researcher. The researcher aimed for a conceptualization of underlying patterns. The research investigator is the interpreter of the collected data and has control over determining what data must be coded depending on the importance of it the case of multiple cases under study (Yin, 2018). The researcher decided which is the most important codes and create categories by combining several codes. The next step in the coding process after creating categories is labeling these categories. The researcher labeled categories and decided which are the most relevant and how they are connected to determine which categories to keep. The coding process was done by writing marginal notes, drafting summaries, and noting categories' relationships (Creswell & Poth, 2018). Since qualitative case study data analysis can be too detailed and time-consuming, using computer bases qualitative research tools for qualitative data analysis helps simplify the coding process (Cypress, 2019).

Interpretations

In case study research, the researchers look for a detailed description of the particular case or cases to engage in qualitative data interpretation. According to Creswell (2007), qualitative data interpretation is understanding and making sense of the data. Interpretations can be made in different forms, including interpretations based on hunches, insights, and intuition (Creswell, 2007). The process of interpretation for this study included forming more significant meanings of the discovered themes by grouping the emergent themes, ideas, and patterns and drawing relevant

and meaningful conclusions. This research used direct interpretation to interpret data. Stake (1995) defines direct interpretation as the process of pulling the data apart and putting them back together in more meaningful ways. In the direct interpretation, case study researchers search for a single instance, not multiple instances and draw meaning from it. The researcher used creative and critical capabilities during data interpretation to make the right judgments about the data gathered during data analysis. During data interpretation, the researchers establish patterns and seek correspondence to show the relationship between two or more categories (Stake, 1995).

The researcher used cross-case synthesis as an analytic technique for this multiple-case study. The method is useful in studying two or more cases (Yin, 2003). The researcher used a thematic framework to explore the Interview data. Data were inductively coded, allowing codes and themes to emerge and develop from data. A thematic analysis takes bodies of often quite large data and groups them according to similarities. In other words, themes helped the researcher make sense of the context and derive meaning from it by reviewing the data and then identifying the themes that crop up repeatedly within the data. Thematic analysis can be very useful for discovering people's experiences, views, and opinions. After performing data reduction and removing the data that is not necessarily related to the topic, useful data were filtered and became ready to develop some themes. Themes were identified by reading the transcripts to know what seemed important and relevant to the interviewee. The researcher used generative coding to identify commonalities and repetitions of similar concepts or words in the database. It helped discover the most important parts of the information that interviewees mentioned during the interview. Generative coding helped draw a clear picture for the researcher during data interpretation.

Data Representation

Data representation is the final phase of the data analysis spiral. In this phase, a researcher presents packages found during the data collection and analysis process in text, tabular, or figure form. After coding the data, the researcher identified emerging themes and patterns, organized themes into categories, and finally categorized central themes for data representation. Castleberry and Nolen (2018) indicated that there are two common methods to represent qualitative data, hierarchies and matrices; both can be used to organize data within themes. The researcher used tables, bar charts, hierarchy charts, a sunburn chart, and diagrams for data representation.

Creswell and Poth (2018) recommended creating a visual image of information, like flow charts and diagrams, to visually discover overlapping patterns and themes and draw relationships among emerging ideas and codes. The data may be presented using a comparison table, flow charts or a matrix. These tools help the researcher with evaluating participants' feedback and experience analytically.

Analysis for Triangulation

To conduct analysis for the triangulation, the researcher used member checking to enhance the credibility of data, ensure validity in the research, and promote participant engagement. Member checking allowed research participants to review themes and confirm the accuracy of the captured data (O'Neil, 2019). It supported data triangulation by providing a way for the researcher to ensure the accurate portrayal of participant voices. Triangulation is an effective strategy to counter all the threats to validity. It uses multiple sources of data collection to enhance the rigor of the research (Robson & McCartan, 2016). The researcher provided a copy of the interview transcript to each participant after the interview to confirm the accuracy of the information provided during the participation in the research. Patton (1999) defined data triangulation in

qualitative research as using multiple data sources and methods to develop a comprehensive understanding of phenomena. At the same time, Cypress (2017) defined it as the cross-checking of data and interpretations within categories of participants.

The data were collected through semi-structured interviews as the primary source of information in this multiple case study research. The semi-structured nature of the interviews made it possible for innovative issues to emerge from the open discussion. During the semi-structured interview, additional insights emerge consistently with the exploratory nature of the case study. The key informants provide different perspectives on the case under scrutiny. All interview content was recorded and transcribed. Such content represents the primary source of evidence for the case, which was combined with member checking to ensure data triangulation (Creswell & Poth, 2018).

Summary of Data Analysis

The main benefit of qualitative methodologies compared to quantitative ones is researchers can collect data at any time until reaching data saturation which concludes the data collection process. Data analysis was performed by summarizing the collected data, analyzing interviews, triangulating with other data, and interpreting the findings. Data analysis has several approaches. The researcher started the process by creating and organizing information. Then performed general reading and memoing to the information in the database to develop a sense of the data. Then, the phase of description included engaging in qualitative data interpretation. Data analysis was performed both within-case and cross-case. Each case was analyzed as a standalone entity to generate the necessary insight into the issues under scrutiny. Later, a comparison between the different responses from informants was performed for both within and cross-case content analysis from interviews (Creswell & Poth, 2018). Additionally, for this multiple-case study, the researcher used cross-case synthesis to compare findings from all cases and data gathered from different

individuals and organizations. The research followed the inductive or open coding approach for each case. Lastly, the researcher used direct interpretation as a qualitative data interpretation approach.

Reliability and Validity

In qualitative research, validity refers to the accuracy and truthfulness of the findings, while reliability refers to the consistency and stability of the results. Creswell (2014) discussed the importance of validity and reliability in qualitative research, noting that they are often achieved through triangulation, member checking, and reflexivity. Morse et al. (2002) provided a detailed overview of verification strategies that can be used to establish validity and reliability in qualitative research, including triangulation and member checking. Reliability and validity are essential to any qualitative research; it ensures the research is reliable and valid. Reliability and validity help establish the research design, which includes the selection of cases, sampling procedures, and data collection techniques. Reflexivity in qualitative research refers to the practice of acknowledging and examining the role of the researcher in the research process. It involves reflecting on the assumptions, biases, values, and experiences that may influence the researcher's interpretation and analysis of data. Reflexivity helps to ensure that the researcher's perspectives are made explicit and that the research is conducted in a transparent and rigorous manner. Richardson (2000) argued that reflexivity is essential in qualitative research because "the subjective positionality of the researcher always mediates the construction of knowledge" (p. 82). The data collection for this research was rigorous and systematic. Data were collected using multiple methods to ensure that multiple perspectives are captured. The data were collected consistently and systematically using standardized protocols and procedures (Denzin & Lincoln, 2002). This ensures the data are reliable and the findings can be replicated. The investigator analyzed the data using a systematic and

transparent process to ensure the findings are valid and accurately represent the case under investigation. It is important to ensure that the findings are credible and trustworthy. This involves presenting findings clearly and concisely, using appropriate language and terminology. This research ensured that the findings are supported by evidence from the data and as consistent with previous research on the topic. Denzin and Lincoln (2002) argued that validity and reliability are not simply technical issues in qualitative research but are part of a larger process of making claims about social reality. Validity and reliability can be enhanced through reflexivity, bracketing, and thick description (Denzin & Lincoln, 2002).

Reliability

Ensuring the reliability of the data is one of the key challenges in qualitative research, which refers to the consistency and stability of the findings over time and across different researchers (Creswell & Poth, 2018). Qualitative researchers use several techniques to ensure reliability, including triangulation, member checking, and inter-coder reliability checks. These techniques involve cross-checking data sources and involving participants in the research process to increase the validity and reliability of the findings. Qualitative researchers can ensure reliability in their studies by employing a range of strategies that enhance their findings' credibility, transferability, dependability, and confirmability (Creswell, 2014). According to Creswell and Poth (2018), triangulation involves using multiple data sources such as interviews, observations, and documents, to corroborate findings and increase the reliability of the data. On the other hand, member checking involves sharing the findings with participants to ensure their accuracy and validity.

Credibility. To enhance credibility, the research ensured that the study's findings are believable and trustworthy. This was accomplished by implementing three techniques:

triangulation, member checking, and reflexivity (Finlay, 2002). Triangulation involves using multiple sources or methods to collect data to provide a more comprehensive and accurate understanding of the case being studied. Member checking was implemented by sharing the study findings with participants to ensure that their perspectives are accurately represented. Reflexivity ensured that the researcher is aware of and accounting for own biases, assumptions, and perspectives (Morse et al., 2002).

Transferability. Transferability is achieved when the findings can be applied to other contexts or populations. It allows readers to assess whether the findings are applicable to their own situations, this can be achieved by providing a thick description of the participants and the research process. The researcher enhanced transferability by providing detailed and comprehensive descriptions of the research context, participants, and methods to enable readers to understand the study's relevance to their own context (Denzin & Lincoln, 2002). Another way to ensure transferability is by selecting participants and contexts that are diverse and representative of the population of interest (Morse et al., 2002).

Dependability. This research ensured the consistency and stability of the findings over time and across different contexts (Denzin & Lincoln, 2002). The researcher used an audit trail to enhance dependability by keeping detailed records of the research process. That includes data collection, analysis, and interpretation. This process ensured that the findings can be replicated and traced back to the data. The researcher can achieve dependability by duplicating the same steps to gather data (Morse et al., 2002).

Confirmability. The research findings of this multiple case study was based on the data collected rather than the researcher's own biases or perspectives. The researcher relied on the data collated from the interviews and was analyzed and interpreted systematically to ensure the data's

reliability. To enhance confirmability, the researcher focused on participants' experiences when interpreting the findings, verified interpreted findings with various sources of data. Reflexivity helps to ensure that the researcher's perspectives are made explicit and that the research is conducted in a transparent and rigorous manner. Reflexivity is appropriate for this study because it helped to ensure that research findings are grounded in the perspectives and experiences of participants, rather than solely reflecting the biases and assumptions of the researcher. Therefore, the researcher implemented reflexivity along with audit trail, and triangulation to enhance confirmability (Denzin & Lincoln, 2002).

Validity

Researchers use various methods to ensure validity in their studies, including bracketing, triangulation, and saturation. These techniques can help to increase the credibility and rigor of research findings by minimizing bias and increasing the reliability of results. Qualitative research focuses on the quality and richness of the data collected. Therefore, ensuring the validity of the data becomes paramount. There are a few types of validity, including internal and external validity. Internal and external validity aims to establish the credibility and generalizability of the research findings. According to Patton (2014), internal validity in qualitative research is established through multiple sources of evidence, careful selection of participants, and attention to researcher bias. Meanwhile, Lincoln and Guba (1985) argued that external validity could be enhanced through purposive sampling, thick description, and transferability. In this research, the investigator maintained internal validity by limiting personal biases, using the same approach for each interview, and keeping a record of the interview transcripts. The researcher carefully considered the validity threats to their study design and employed appropriate techniques to mitigate them. Ensuring validity in research is crucial to the scientific process and can be achieved through

various methods, including:

Triangulation. Triangulation is an effective technique to validate the research findings by using multiple data sources to cross-check and verify the accuracy of the findings. It increases the research findings' validity and provides a more comprehensive understanding of the phenomenon being studied (Denzin & Lincoln, 2018). The researcher collected data from multiple participants, then compared and contrast the data to identify patterns and themes. It is an effective approach for convergence and validation of data. Data triangulation helped the researcher to increase both the reliability and validity of the research findings. The researcher used member checking to enhance the validity of the collected data and achieve data triangulation.

Saturation. Data saturation helps the researcher determine when the data collection process is complete. Reaching data saturation involves continuing data collection until no new information or insights are being gathered from the participants. Morse (2015) defined saturation as the point in the data collection process when data analysis stops revealing new concepts, themes, or categories. This technique will be implemented in the study to ensure that the data collected are comprehensive and complete. It also confirms that the researcher has explored all possible aspects of the research topic. The researcher achieved data saturation after interviewing 15 participants, the researcher ended the interview process after realizing that answers to the interview questions were repeated and no new information coming from participants responses.

Bracketing

Bracketing is an effective method to enhance validity in qualitative research. Qualitative research is susceptible to bias due to the subjective nature of data collection and analysis. Bracketing is a technique used in qualitative research to acknowledge and address researcher bias. Some bracketing techniques researchers employed to address bias in qualitative research include

identifying preconceptions and assumptions about the research topic that may be affecting the interpretation of the data (Cypress, 2017). This technique was used to ensure that the researcher's preconceptions, biases, and assumptions do not influence the data collection process or analysis. It involves the researcher identifying and acknowledging their preconceptions and biases about the research topic. Creswell (2014) emphasized that bracketing aims to suspend any preconceptions and potential biases the researcher has during the study.

Bracketing sets the researcher aside during the data collection and analysis process to ensure that the collected and analyzed data are unbiased and reflect the participants' experiences. This can be done through a variety of methods, such as journaling, discussing biases with colleagues, or engaging in reflective practice (Finlay, 2002). Reflective journaling is another technique the researcher employed to address bias by writing down thoughts, feelings, and ideas about the research. Journaling helped the researcher to become more self-aware of biases and preconceptions, which may influence their data analysis (Finlay, 2002). Triangulation is the following technique that was used to reduce the effects of researcher bias by comparing data collected from different sources or by using different data collection methods. Lastly, member checking was conducted to ensure that the research findings accurately represent the participant's experiences and perspectives. Baksh (2018) emphasized that bracketing can help the researcher mitigate the potentially harmful effects of own assumptions that could potentially influence the research process. The researcher in this study needed to ensure that the research is transparent and ethical. This involves providing a clear and transparent account of the research process, including any potential biases or limitations. The study was conducted ethically, with the rights and well-being of participants being protected. Signed informed consent was obtained from participants, and their anonymity and confidentiality was maintained throughout the research process.

Summary of Reliability and Validity

In summary, qualitative researchers ensure the validity of their studies by using techniques such as bracketing to avoid preconceptions and biases, leading to more credible and trustworthy research findings. Triangulation to cross-check and validate findings. And saturation to ensure comprehensive data collection. Patton (2002) emphasized the importance of validity and reliability in qualitative research, noting that they are often achieved through triangulation and member checking. Ensuring the reliability and validity of qualitative multiple-case study research requires a systematic and transparent approach to research design, data collection, data analysis, and reporting. By following these steps, researchers can ensure that their research is credible, trustworthy, and provides a comprehensive understanding of the phenomenon under investigation.

Summary of Section 2 and Transition

This research aimed to generate rich, descriptive data that can be used to understand the complexity of the problem being studied. The participants of this qualitative multiple case study research design were selected based on certain requirements determined by the researcher to help providing insights on the contemporary research problem that involve using AI in the internet security domain. The population of this study was a larger group of individuals that share the characteristics of the participants. Purposeful and snowball sampling was used to determine the study sample. The researcher was the primary instrument for this study and the data collection used semi structured interviews as the primary source of data collection. Open-ended questions was used in the interview to give the research participants the opportunity to speak freely about their experience and express their opinions. The researcher collected data from each case and compared and contrasted the data across cases to identify patterns and themes. The organization plan involved careful analysis and interpretation of the data. The researcher used a coding system to identify

patterns and themes then compares the cases to identify similarities and differences and develops a cross-case analysis that synthesizes the findings from all cases. Lastly, the researcher ensured the validity and reliability of the study and used bracketing to address bias by suspending own presupposition, biases, assumptions, or previous experience about the research problem.

The purpose of Section 2 is to form a clear picture of the research project. It enabled the researcher to define the project through reflection on the purpose statement; it identified the role of the researcher and participants in the research. It discussed the research design and methodology and provided details on the population and sample method, the data collection process, and data analysis. The researcher discussed the methodology applied to explore the effect of automated cyber-attacks on technology organizations in the United States. The section consists of the purpose statement, role of the researcher, research method and design, participants, data collection plan, data analysis plan, and the validity and reliability of the research findings. Section 3 is the presentation of findings. It provided an overview of the study, followed by the presentation of findings which presented the discovered themes and sub themes that emerged from the participants responses to the interview questions. Section 3 explored the relationship of the findings with the research questions, the problem and the conceptual framework, the literature and the anticipated themes. Section 3 identified the application to professional practices and suggested new areas for future study by providing four recommendations of future study topics related to the use of AI in the cybersecurity field. The researcher concluded Section 3 with reflections on personal and professional growth and biblical perspective.

Section 3: Application to Professional Practice and Implications for Change

Section 3 served as the conclusive segment of this qualitative multiple case study, encapsulating a comprehensive overview of the study, and presenting the research findings derived from participants' responses to interview questions. Within this section, the interconnection with the preceding two sections is explored, elucidating the alignment of findings with research questions, the research problem, and the conceptual framework from Section 1, as well as their relationship with the literature and anticipated themes outlined in Section 2. Furthermore, this section evaluated the practical applications of the research, illustrating how it enhances general business practices and proposing potential application strategies. Future study recommendations in the field of AI and cybersecurity are also offered. The conclusion of this section incorporates reflections on personal and professional growth, while weaving a discussion on the integration of business functions explored in the research with a Christian worldview, supported by relevant scripture references. This holistic presentation aimed to provide a seamless synthesis of the study's components, offering insights, applications, and avenues for further exploration.

Overview of The Study

The advent of AI and ML has transformed the landscape of cybersecurity. While these technologies have proven invaluable in enhancing the defense mechanisms of organizations, they have also opened the door to a dark side where adversaries harness the power of AI for malicious cyber-attacks. This qualitative multiple case study explored the depths of this emerging challenge, aiming to uncover the extent of the threat AI poses to organizations and to identify defensive tactics that can be employed to mitigate these risks. This study adopts a flexible design, utilizing qualitative methods, with a focus on multiple case studies. It intends to shed light on the ever-evolving AI-powered cyber-attacks and the countermeasures that organizations, particularly in the

United States, are employing to safeguard their cybersecurity infrastructure. The research questions aim to unveil existing trends in AI-based cyber-attacks and the corresponding defenses, providing valuable insights into this critical aspect of modern cybersecurity.

Cybercriminals have seized upon the capabilities of AI and ML to exploit vulnerabilities, automate attacks, and conduct malicious activities. These technologies have empowered adversaries to engage in a wide array of cyber threats, including automated attacks, sophisticated phishing scams, rapid password cracking, and personalized social engineering campaigns. In particular, the use of AI models developed on the dark web has amplified the threat landscape, making it imperative for organizations to remain vigilant and adapt their cybersecurity strategies continually. One of the most concerning aspects of AI-powered cyber-attacks is their ability to cause extensive and rapid damage. These attacks are highly scalable, efficient, and adaptable, targeting multiple organizations simultaneously. The impact and financial losses vary depending on the industry, system, and targeted data. The interviews with the research participants provided a comprehensive exploration of AI and ML-powered cyber-attacks, covering everything from continuous attacks and deep fakes to technical aspects like DNS poisoning, MAC address table manipulation, and polymorphic malware. Adversaries employ a variety of AI and ML tools to execute cyber-attacks, including tools like Chat GPT, Pin Schema, Domo, and Google BARD. These tools serve multiple purposes, from generating malicious code to conducting social engineering attacks, greatly enhancing the effectiveness and automation of cybercriminal activities. AI and ML-driven cyber threats have become a paramount concern for businesses, necessitating strategic planning and decision-making to safeguard their operations.

While AI presents significant challenges in terms of cybersecurity, it also offers a plethora of advantages. Participants highlighted that AI enhances cybersecurity by improving response

times, automating tasks, enhancing threat detection, and streamlining processes. These technologies enable cybersecurity professionals to protect systems and data more effectively in an increasingly complex threat landscape. ML algorithms have become indispensable in malware detection and prevention efforts, allowing organizations to analyze and respond to threats more effectively. In particular, behavior-based detection and post-breach intervention have gained prominence in modern cybersecurity strategies. Keeping systems updated and harnessing the latest ML technologies are crucial to staying ahead of evolving threats.

The adoption of no-code and low-code applications has proven beneficial, offering advantages like improved accessibility, faster development, reduced coding effort, and generic tool creation. These advancements streamline application development and improve efficiency. The research participants collectively emphasized the importance of being informed about AI-related cybersecurity threats, implementing compliance measures, practicing strong access controls, and preparing for disaster recovery. Embracing these techniques is crucial to mitigating the risks associated with AI-related cyber-attacks. Investing in AI technology for cybersecurity is not just a matter of choice; it is a necessity, particularly for high-tech organizations in the United States. AI promises financial rewards, improved decision-making, and effective defense against cyber threats. However, challenges such as counter AI and legislative lag need to be addressed as part of a comprehensive cybersecurity strategy.

The research explored the critical role of employee awareness and compliance in bolstering cybersecurity. Regular training, testing, and accountability measures are essential components of creating a security-conscious culture. As technology evolves, organizations must adapt their training programs to address new and emerging threats. Communication and information dissemination are also vital to keep employees informed about evolving threats. Participants

expressed concerns about the misuse of AI and emphasized the need for stronger governance and regulations to address potential threats. Open-source AI tools like Chat GPT, while advantageous, can be manipulated for malicious purposes, highlighting the importance of responsible AI use and oversight.

The research participants raised concerns about the security and privacy risks associated with Internet of Things (IoT) devices. Vulnerabilities stemming from inadequate updates, the potential for malicious intent, and the need for manufacturers to be held accountable for device security were highlighted. The role of AI and ML in addressing these challenges varied among participants, with some advocating for manual security measures and others embracing the potential of AI-driven solutions. Addressing the growing challenges associated with IoT devices in our interconnected world requires a multi-faceted approach, involving security-conscious cultures, updated systems, and vigilant monitoring. AI and ML have the potential to play a significant role in enhancing the security of these devices, but the nuances of their application and their limitations should be carefully considered.

As technology organizations in the United States and worldwide face a diverse and evolving array of challenges, they must adapt and invest in cybersecurity measures to stay ahead of the ever-changing threat landscape. The financial impact of automated cyber-attacks and data breaches is substantial, encompassing operational disruptions, legal penalties, reputational damage, and individual financial losses. Decisions surrounding AI technology investments and cybersecurity strategies are complex, involving collaboration, awareness, financial considerations, and adaptability to evolving threats. The role of decision-makers, such as the CIO, CEO, and board members, is important in navigating this issue.

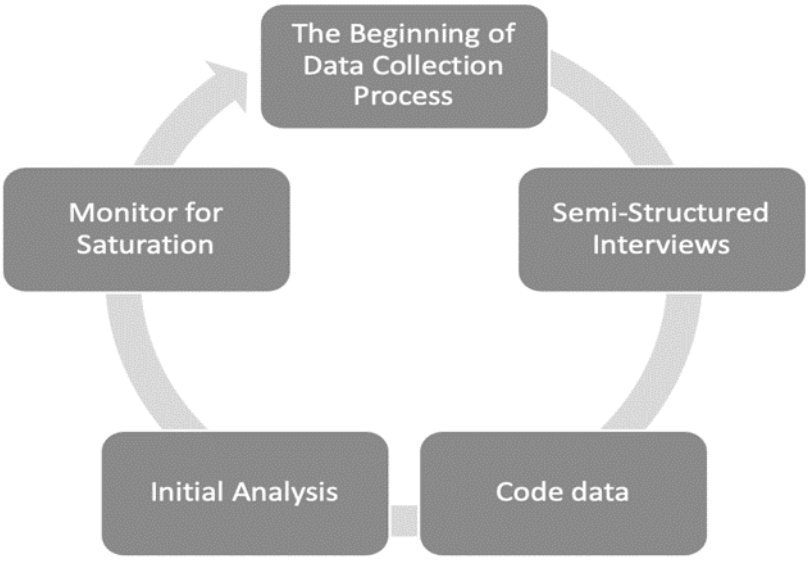
Presentation of the Findings

The purpose of this study is to explore the intricate web of AI's dark side, where algorithms that were designed to facilitate progress are now weaponized to compromise security. The realm of cybersecurity faces unprecedented challenges as AI-driven attacks become increasingly sophisticated, elusive, and automated. In our rapidly evolving digital technology, the fusion of AI and cybersecurity has ushered in a new era of both promise and threat. As organizations and individuals harness the power of AI to enhance the efficiency and effectiveness of their systems, a parallel threat looms on the horizon: the malicious use of this transformative technology. The result of this study provided insight to this emerging threat, discovering the potential consequences, vulnerabilities, and the urgent need for innovative defenses. The research finding navigated this complex issue to understand how AI, once a cybersecurity ally, has become a formidable adversary, and how we can adapt to protect the digital fortresses that underpin our modern world. Creswell and Poth (2017) emphasized the significance of a well-structured presentation that encompasses an introduction, methods, results, and discussion sections to ensure clarity and facilitate the audience's understanding of the research. The researcher interviewed 15 participants after obtaining the approval from the Institutional Review Boards (IRB). According to Hennink and Kaiser (2022), saturation is considered the cornerstone of rigor in determining sample sizes in qualitative research. The researcher conducted initial analysis to the collected data and determined that no new themes are identified, and data saturation is achieved. The researcher achieved data saturation through a rigorous process of conducting semi-structured interviews with a group of 15 participants. This data saturation point allowed the researcher to gain valuable insights into the various facets of the malicious use of AI technology and its impact on cybersecurity from a broad range of experts, practitioners, and stakeholders in the field to ensure a robust and comprehensive

analysis of the issue. The participants signed consent forms to ensure confidentiality and anonymity of their personal information. The researcher conducted thematic analysis to identify the themes and sub-themes from the codes that was generated from the participants' answers to the research questions. Nine themes emerged from the interview responses, each of them has subthemes related to the patterns discovered in the data analysis process. The researcher conducted member checking by sending the interview transcripts to participants to review for accuracy and to guarantee validity and reliability. Data triangulation played a vital role in enhancing the robustness of the research findings. In addition to conducting semi-structured interviews with 15 participants, the researcher employed a member checking process, which involved revisiting these participants and cross-referencing initial findings with their perspectives. After conducting the initial interviews, the researcher provided the participants with the interview transcript. This iterative process provided the researcher a valuable opportunity to identify any discrepancies, clarify ambiguities, and gain further context on the subject matter. The engagement in member checking ensured that the research accurately represented the nuanced viewpoints and intricacies of the topic. Member checking helped increase the reliability of data and enhance the overall quality of the research. Figure 3 shows the full cycle of data collection process used in this research.

Figure 3

Data collection cycle



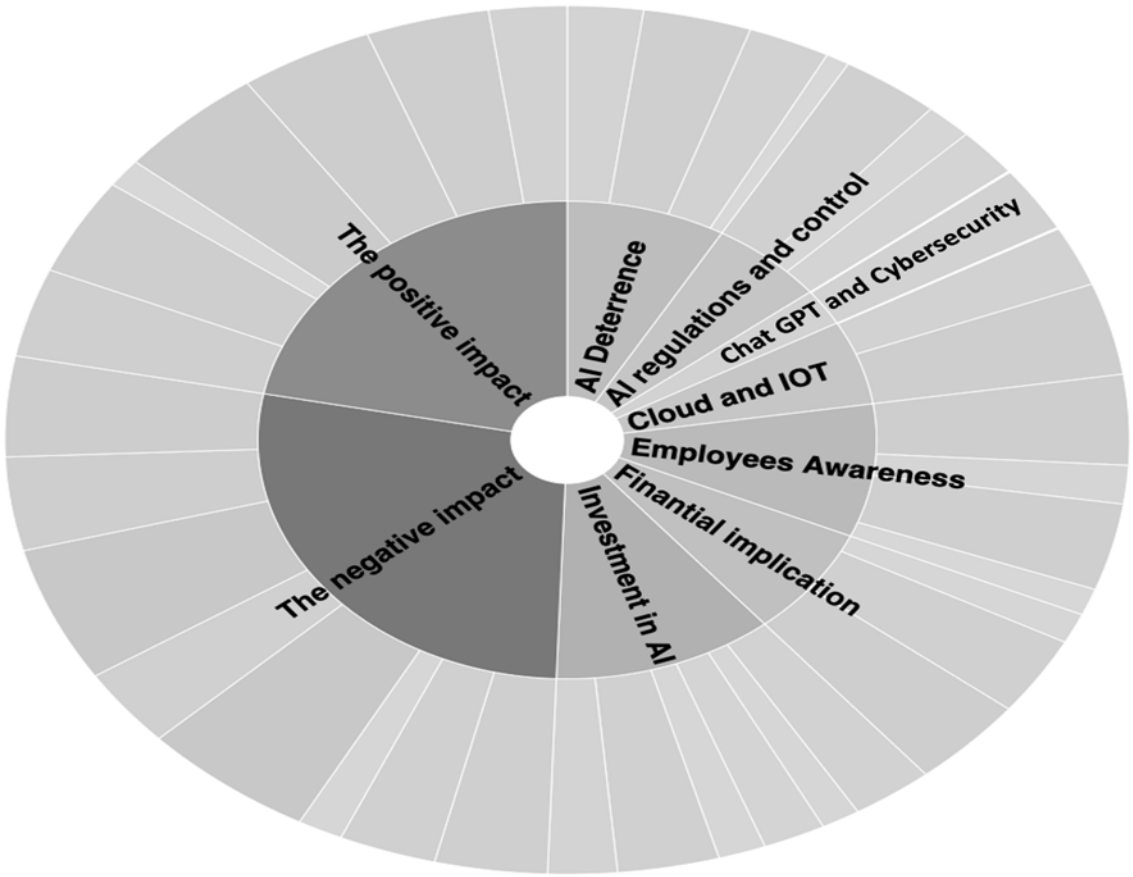
Themes Discovered

In this research, IT and cybersecurity experts from various backgrounds provided insights into different aspects of the research. Themes are recurring patterns or concepts that emerge from data analysis, offering deeper insights into the research subject. These themes help researchers make sense of the data, providing a framework for interpretation and discussion (Creswell & Poth, 2017). After conducting thematic analysis on the data collected through the semi-structured interviews conducted with 15 participants, the following themes were identified as: (a) the negative impact, (b) the positive impact, (c) investment in AI technology to enhance cybersecurity, (d) financial implications of AI-powered attacks on organizations and customers, (e) employees awareness and compliance, (f) AI regulations and control, (g) AI deterrence, (h) the impact of AI on the cloud and Internet of Things (IOT), and (i) chat GPT and cybersecurity. Each theme has a few sub themes derived from the codes, The themes were determined using NVIVO data analysis software, the software were used to categorize the data, code it and discover patterns and themes

derived from the codes. Figure 4 is a sunburst chart of the emerging themes and subthemes. It shows the nine themes discovered in the study findings, and the subthemes related to each theme. The chart was retrieved from NVivo software.

Figure 4

Sunburst chart of the emerging themes and subthemes



Interpretation of the Themes

The research findings include eight themes discovered from coding the data collected from 15 research participants. Participants answered the interview questions, each set of interview questions addressed part of the research questions. Table 2 shows the themes and the corresponding subtheme to each theme. The interview questions were designed to discover related themes for this

study to provide solutions to the research problem by analyzing and understanding the participants' inputs to this research. Figure 3 shows a bar chart that includes bars representing each main theme, each main theme bar includes the total number of participants that supported all subthemes. Braun and Clarke (2006) indicated that researchers can anchor their themes in established methodologies strengthen the rigor of the research and contribute to the existing body of knowledge, fostering a comprehensive understanding of the subject matter. The emerging themes addressed the significant effects on AI on cybersecurity, both in terms of enhancing security measures and posing new challenges, along with the techniques can be maliciously exploited by cybercriminals in several ways using this emerging technology. Figure 5 below shows an overarching chart representing each main theme and the total number of participants that supported all subthemes.

Table 2

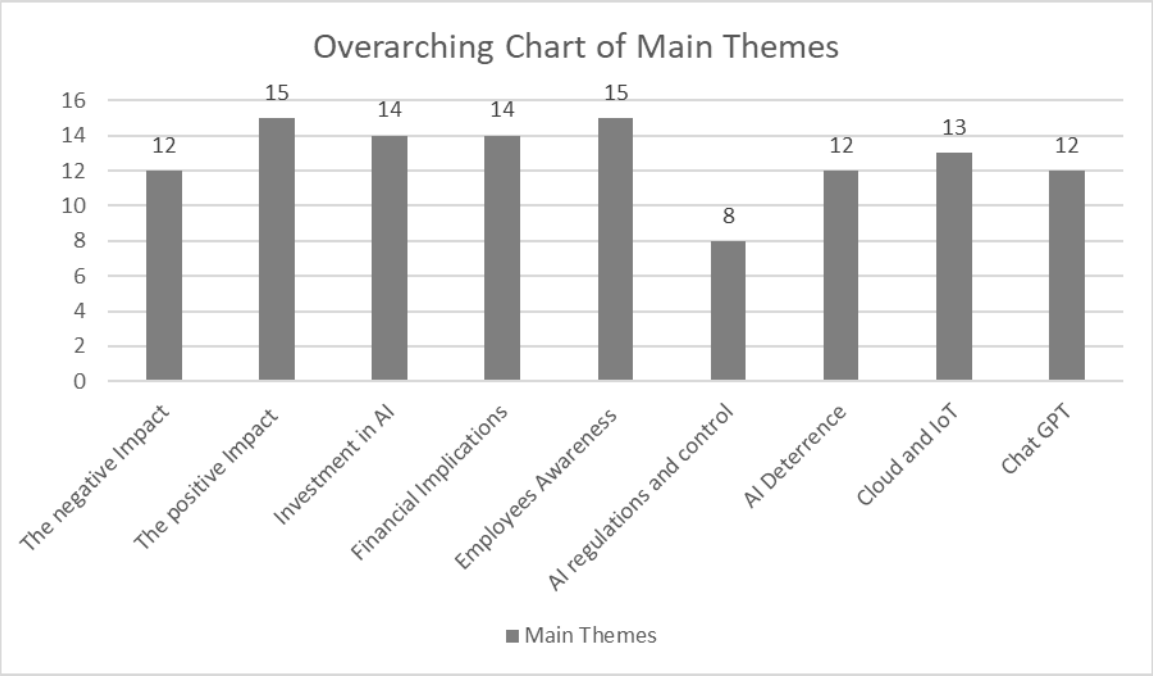
Relationships of data themes, sub-themes/patterns

Themes	Sub-themes/Patterns
The negative impact	The malicious use of AI Automated vs traditional Types of AI cyber-attacks AI tools The effect on business The Advancement of AI Social engineering No code Low code Apps
The positive impact	The advantages of AI ML to improve cybersecurity Malware detection Vulnerability prediction Vulnerability patching Prevention & risk mitigation No code Low code benefits
Investment in AI	The importance The challenges Roles and responsibilities

Themes	Sub-themes/Patterns
Financial Implications	Implications on organizations Implications on customers Financial decision makers
Employees awareness	Employees awareness to enhance cybersecurity Employees awareness techniques Employees awareness effectiveness
AI regulations and control	Current level of governance and control The need for more governance Governance and the future of cyber-attacks
AI deterrence	Deterring a cyber-attacks Influencing hackers not to initiate the attack. Deterrence and cost The effectiveness of the security team
Cloud and IoT	AI to enhance the clous and IoT AI threats on the cloud and IoT
Chat GPT	Chat GPT and cyber-attacks

Figure 5

An overarching chart representing each main theme.



Theme 1: The Negative Impact.

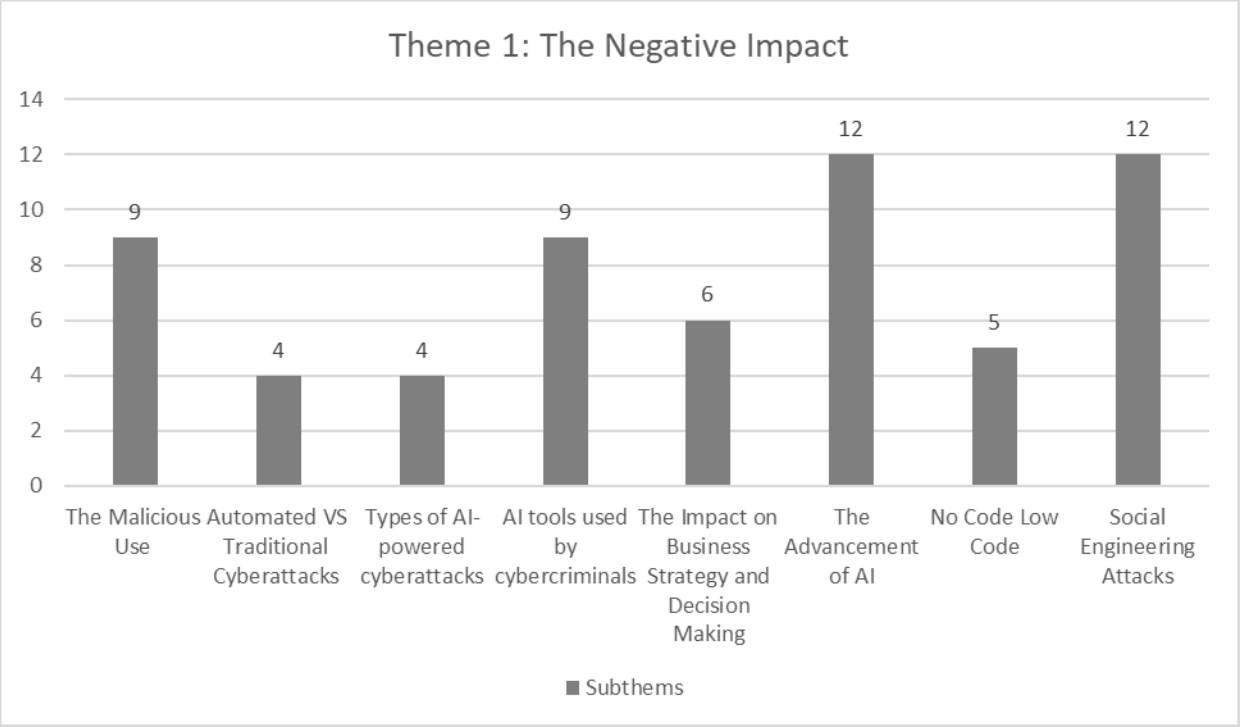
The Malicious use. One prominent method cybercriminal utilize AI and ML is by leveraging language models like Chat GPT to automate attacks. This technology can manipulate these models to generate injection prompts and SQL injection attacks, which are significant security threats. For instance, an attacker could craft input that exploits a web application's vulnerabilities to gain unauthorized access or manipulate a database, which can lead to data breaches and compromised systems, causing significant harm to individuals and organizations (Participants 1, 3, 4, 5, 7, 8, 9, 12, & 13). AI and ML can aid cybercriminals in creating more convincing phishing scams. By generating human-like communication and content, attackers can trick victims into believing they are interacting with legitimate entities. This can include replicating the writing style of high-ranking personnel, such as CEOs or CFOs, in emails to deceive employees into divulging sensitive information or initiating harmful actions. Carlini and Wagner (2017) revealed how AI can be used to generate adversarial examples, deceiving ML-based defenses. As AI-powered tools are adopted in the security domain, a shortage of skilled cybersecurity professionals to manage them becomes evident. Thus, while AI enhances cybersecurity, its misuse and the widening skills gap pose significant challenges.

Cybercriminals also use AI to mimic a CEO's writing style in an email, convincing an employee to wire money to a fraudulent account. This sophisticated approach makes it increasingly challenging for users to discern phishing attempts from genuine communications. AI can be used maliciously to crack passwords with remarkable speed and accuracy. AI algorithms can analyze a target's personal information, such as birthdays, anniversaries, and other details easily accessible on social media platforms, to predict and generate likely passwords. These AI-powered attacks can compromise accounts, leading to identity theft, unauthorized access, and financial losses. Research participants pointed out that AI and ML can automate reconnaissance and decision-making

processes, making them more efficient and dangerous. For example, AI-driven tools can identify vulnerabilities and automate attacks like denial-of-service (DoS) or distributed denial-of-service (DDoS) attacks, overwhelming targeted systems and causing service disruptions. AI can enhance social engineering attacks. By analyzing vast amounts of data, AI can create highly targeted and convincing phishing campaigns, tailoring messages to exploit the specific interests, behaviors, and vulnerabilities of individuals or organizations. This personalized approach increases the success rate of these attacks. Another concerning development in cybercrime involves the creation of dark web equivalents of AI and ML models. These models lack the ethical constraints typically associated with mainstream AI, allowing cybercriminals to access even more potent tools for malicious purposes. While the details of these models remain somewhat obscure, they represent an alarming trend in AI's misuse. Figure 6 shows the subthemes related to theme 1 based on the participants answers.

Figure 6

Subthemes of theme 1 based on the responses gathered from participants.



Automated Cyber-attacks VS. Traditional Cyber-attacks. The research participants generally agree that automated cyber-attacks have the potential to cause significantly more damage compared to traditional cyber-attacks. Automated cyber-attacks leverage AI and ML to carry out attacks quickly and dynamically. They can exploit vulnerabilities and adapt to defenses much faster than traditional attacks conducted by human operators. Automated attacks can initiate actions as soon as they detect a change in the target, making them highly efficient. One key aspect highlighted by the majority of the research participants is the ability of automated attacks to scale. Traditional attacks are often limited by the capacity of human operators, while automated attacks can simultaneously target multiple organizations, making the overall damage more extensive. The participants noted that automated attacks can lead to significant data breaches, including the compromise of sensitive information like biometrics. This can result in severe consequences for

technology organizations. Ransomware attacks, which can lock organizations out of their systems until a ransom is paid, are cited as a specific type of cyber-attack that can cause substantial damage. Automated attacks can carry out such attacks efficiently and on a scale.

The level of damage caused by automated attacks varies depending on the targeted industry and the sophistication of the targeted system. For instance, healthcare organizations may face substantial consequences due to the exposure of patient data, while the impact on other industries could differ. Financial losses due to automated cyber-attacks can be substantial, with estimates reaching millions or even billions of dollars. Revenue losses, costs for recovery, and potential legal consequences are factors that contribute to the financial impact. Participants (3, 5, 6 and 11) indicated that traditional attacks require more coordination and advance planning, whereas automated attacks can be initiated quickly by a single individual, making them more unpredictable and challenging to defend against. Table 3 shows a comparison between AI powered cyber-attacks and traditional cyber-attacks.

Table 3

Automated Cyber-attacks VS. Traditional Cyber-attacks.

Automated Cyber-attacks	Traditional Cyber-attacks
Have the potential to cause significantly more damage at a higher scale	Can cause significant damages at a lower scale
Leverages AI and ML	Leverage traditional software and tools
Adapt to defenses much faster than traditional attacks	Not as effective against defenses as they're conducted by human operators
The ability to scale as it relies on automation	Limited by the capacity of human operators
Can be initiated quickly by a single individual	Require more coordination and advance planning

Types of AI-powered Cyber-Attacks. This theme covers various aspects of AI (AI) and ML (ML) powered cyber-attacks, with a focus on their types and potential applications against technology organizations in the United States. The theme was discovered through several codes involving the continuous attacks that target different parts of technology systems and firewalls. These attacks are characterized as typically AI-driven. Deep fake attacks are highlighted as a significant threat. In these attacks, AI is used to create convincing impersonations of high-profile individuals, such as CEOs, with the goal of infiltrating systems and hacking them. The interview answers briefly mention the use of AI, such as Chat GPT and Google's BARD, to generate programs that seek vulnerabilities in firewalls, Linux systems, and Apple systems. These programs aim to gain unauthorized access or extract information. Participants 1, 4, and 7 identified some attacks targeting DNS servers and MAC address tables, aiming to corrupt network data and disrupt services. These attacks are described as using AI or ML tools to achieve their goals. Participant 2 mentioned polymorphic malware as a type of malware that changes its form rapidly to evade detection by security systems. Several participants highlighted predictive algorithms and the

potential use of ML to predict vulnerabilities in systems and aid hackers in infiltrating them. Another type of AI-powered attacks mentioned is customized phishing attacks which uses generative AI, like Chat GPT, to craft custom phishing messages that appear more convincing to targets. AI and ML are noted in the interviews for their role in creating malicious scripts and generating malware, which can then be used in cyberattacks. Participants identified another type of type of automated attacks involves identity theft and deep fake data and the ability of AI to generate deep fake data particularly for identity theft purposes. Cybercriminals can create realistic personas of individuals, leading to financial fraud and disinformation campaigns. Participants also stressed that AI-powered attacks can involve spreading false information using the identity of prominent figures to damage reputations or manipulate public perception.

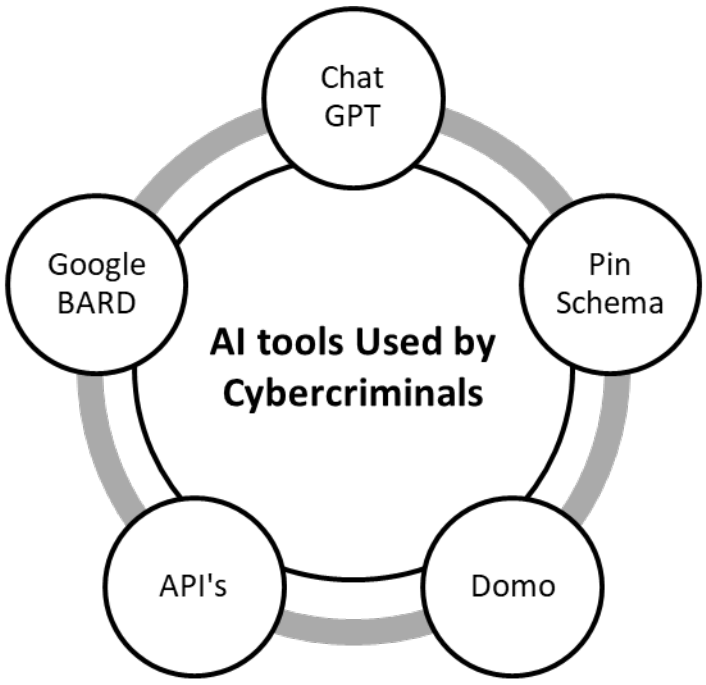
The application of predictive algorithms and ML techniques in hacking endeavors is another sub theme in the research. While the participants acknowledge the existence of these technologies, they express a degree of skepticism regarding their direct employment in attacks. Instead, they speculate that hackers may employ them in conjunction with other strategies to achieve their objectives. Specifically, they suggest that hackers might utilize ML to scrutinize system logs for patterns indicative of vulnerabilities, potentially leading to lateral movement within a network. The participants focused on the crafting of social engineering elements in cyberattacks. They distinguished between the crafting of messages and the subsequent dissemination of these messages. While they asserted that traditional methods are likely to be employed for dissemination, they anticipate that AI-driven generative models may play a pivotal role in customizing messages to enhance their persuasiveness.

AI Tools Used by Cybercriminals. The participants mentioned an arsenal of tools employed by cyber criminals and hackers in executing their attacks. The participants assert that, regardless of

the sophistication of AI-driven techniques, attackers must still secure initial access to a system to deploy their malicious payloads. This access may be gained through various means, ranging from exploiting known vulnerabilities to employing social engineering tactics. The participants suggested that AI and ML tools are being developed and used by cyber criminals to conduct various types of cyberattacks, including firewall and email system break-ins. These tools are being employed to breach security systems and gain unauthorized access. Figure 7 illustrates the tools used by cybercriminals to conduct automated cyber-attacks. The study participants identified the AI and ML tools that Cybercriminals and hackers employ to conduct attacks and target organizations. Some of these tools include:

Figure 7

Tools used to conduct automated cyber-attacks.



Chat GPT. All participants identified Chat GPT as a prominent tool frequently employed by cybercriminals. Chat GPT is known for its versatility in generating content, making it a valuable resource for hackers engaged in various cyber activities. It allows users, including cybercriminals,

to prompt the generation of content, such as malicious code or phishing scams. Chat GPT is available for public in different versions, including a subscription-based option and an open-source version. It can string together more complex prompts, which can result in the creation of sophisticated and intricate content for cybercriminal purposes. The participants suggested that Chat GPT is utilized for generative AI attacks, particularly in the context of social engineering. Hackers use it to craft messages or content that can deceive individuals into taking specific actions, such as clicking on malicious links or providing sensitive information. It was also mentioned that Chat GPT serves as a versatile tool for cybercriminals, enabling them to generate content, impersonate legitimate entities, and craft convincing social engineering schemes. Participant 9 indicated that hackers use AI tools like Chat GPT to create code in a more gradual and indirect manner. They provide prompts to the AI system, which generates code snippets or components. These components can then be assembled in the hackers' backend systems to create malicious software.

Pin Schema. Pin Schema is mentioned as a tool with potential utility for cybercriminals. It is primarily used for predicting PIN codes by leveraging smartphone sensors. In situations where "Bring Your Own Device" (BYOD) policies are in place. Pin Schema exploits sensor data to forecast PINs used for device access. Although smartphone security mechanisms, such as device lockouts, are intended to deter unauthorized access, Pin Schema can, in some cases, successfully predict PIN codes based on sensor data (Participant 2).

APIs. Participant 3 pointed out the significance of Application Programming Interfaces (APIs) in cybercriminal activities. Hackers leverage AI and ML tools with API integration to automate interactions with various programming interfaces. These APIs allow cybercriminals to communicate with and manipulate different software systems, making them valuable for executing cyberattacks efficiently. Participant 3 added that AI tools like Chat GPT are highlighted as being

integrated with APIs for generative AI attacks, and APIs play a crucial role in streamlining cybercriminal activities, enabling automation and remote control over various aspects of their operations, potentially including data breaches and system infiltrations.

Domo. Participant 4 indicated that Domo is a tool employed by cybercriminals for marketing schemes and sales-related activities. It is described as an AI-powered platform known for its extensive access to various data sources. It is implied that cybercriminals may harness its data analytics capabilities to support deceptive marketing campaigns or gather information for their illicit purposes. Domo's capability in aggregating and analyzing data makes it potentially attractive for cybercriminals seeking to enhance their activities.

Google BARD. Google BARD is mentioned by participant 15 as a tool that hackers might potentially employ, although specific details are lacking. Google BARD is a natural language processing model developed by Google to understand context and nuances in language, primarily for improving search engine results. Participant 15 suggested that hackers could explore leveraging this AI tool for cyberattacks. Given BARD's language understanding capabilities, it might be used for crafting convincing phishing messages, creating deceptive content, or attempting to exploit vulnerabilities related to natural language processing in target systems.

The Impact on Business Strategy and Decision Making. The participants provided insightful feedback on the impact of AI-powered attacks on business strategy and decision making. They highlighted various perspectives, including concerns about the financial implications, the need for enhanced cybersecurity measures, the potential for both positive and negative AI utilization, and the disruption caused by cyber-attacks. The majority of participants emphasized that the increasing frequency of cyber-attacks has led to companies investing more in network security tools and systems, and the cost of running a company has grown due to the development of

new cybersecurity tools that can automatically scan networks. They explained that AI and ML cyber threats have the potential to significantly impact business strategy and decision making. Businesses must consider the financial and operational implications of cyber-attacks and the need to enhance cybersecurity measures as these cyber threats can cause significant disruption to business processes. Examples include data corruption, system disturbances, and increased IT support calls. These disruptions can lead to financial losses and affect the overall flow of business operations.

Participant 3 suggested that technologies like EDR (Endpoint Detection and Response), UVA (User and Entity Behavior Analytics), and EPA (Endpoint Protection Agent) are seen as essential for larger organizations to enhance cybersecurity and protect against AI and ML cyber threats, reflecting the increasing need for advanced security measures in the face of evolving cyber risks. Participant 9 highlighted that the market is experiencing a shortage of cybersecurity professionals, leading to companies hiring individuals with certifications to fill critical positions. This highlights the growing importance of cybersecurity in business operations. Participants 4, 7, 8, 11, 13, and 15 acknowledged the positive and negative AI utilization and mentioned that it can be harnessed for market trend analysis and predicting the future, but they can also be employed maliciously to gain a competitive advantage or disrupt competitors.

In the decision-making part, the participants pointed out that cyber threats force executives to prioritize cybersecurity as a part of their business planning and strategy. Failure to do so can expose organizations to internal and external threats. AI and ML cyber threats require organizations to rethink their approach to vulnerability management and compliance. Attacks can now be carried out with increased sophistication, making detection and response more challenging. Impact on employees is another threat to business strategy, Participant 2 mentioned that cyber

threats not only have financial implications but also affect employee morale. The stress and increased workload caused by addressing cybersecurity issues can impact the \workforce negatively. Lastly, depending on the severity of the cyber-attack, some organizations may choose to rebrand or change their identity after a significant cyber-attack to regain customer trust and recover from the damage caused.

The Advancement of AI. The majority of participants agreed that the advancement of AI technology in recent years has significantly contributed to an increase in data breaches in the United States (P1, P2, P3, P4, P5, P6, P7, P8, P9, P10, P11, P12, & P13). This phenomenon is attributed to several factors. The following patterns were discovered from the interviews: AI technology has enabled hackers to automate and streamline their attacks, making them more efficient and effective. Instead of relying on manual efforts, AI-powered tools can execute cyber-attacks at a much faster rate, increasing the likelihood of successful breaches. AI can be used to create highly convincing impersonation attacks. For example, attackers can use AI-generated content to mimic the writing style of company executives or other trusted individuals, making phishing and spear-phishing attacks more convincing and difficult to detect. AI has facilitated the availability of large datasets, which can be exploited by attackers. Organizations sometimes inadvertently upload sensitive or proprietary information to AI models like Chat GPT, which can then be accessed by malicious actors, leading to data leaks and breaches. Advanced Persistent Threats (APTs) are leveraging AI to reduce the time and effort required to gain initial access and maintain control over target systems. AI-powered tools can help attackers remain undetected within a network, making it easier to exfiltrate data. The advancement of AI in facial recognition and biometric technologies poses risks as hackers can potentially create replicas of facial features or fingerprints to gain unauthorized access to secure systems. The growing use of AI in various

industries has expanded the attack surface. As more organizations adopt AI, there are more potential points of vulnerability that attackers can exploit. AI allows for attacks to be carried out at a scale and speed that human hackers cannot match. This rapid execution of attacks can overwhelm cybersecurity defenses. AI can be employed to generate and spread disinformation, leading to confusion, and potentially causing individuals to click on malicious links or engage in risky behaviors that compromise security. AI can be used for corporate espionage, where competitors or malicious actors use AI-driven techniques to gather proprietary information and gain a competitive advantage.

No Code Low Code. Some of the participants addressed the vulnerability of no code, low code, and AI-based applications to cyber-attacks (P1, P2, P4, P5, & P7). Several of them expresses concerns about the vulnerability of these applications. They believe that these applications rely heavily on AI to generate code, and this lack of human oversight can result in security lapses. Traditional software development follows a Secure Development Lifecycle (SDLC) to ensure security at every stage, while no code applications may lack this rigorous security assessment. As a result, these applications may be more susceptible to cyber-attacks, leading to data breaches. Another participant acknowledges the potential vulnerability of no code and low code applications but emphasizes that it depends on the platform and the responsibility of those using it. They suggested that organizations using these platforms are shifting the risk to third-party providers who claim to have secure environments. The level of security, in their view, depends on the trust placed in these third parties.

Participants pointed out that no code and low code applications are highly exploitable, especially when compared to traditional code-based software. They indicated that it is relatively easy to find exploits in these applications but using the term "research purposes" instead of

"exploit" may be a way to navigate ethical concerns. They raised concerns about the removal of human involvement in software development, suggesting that eliminating human oversight can lead to increased vulnerability and frequency of cyber-attacks. They believe that these applications are more vulnerable than traditional ones. However, only one participant views no code and low code applications as generally secure because they rely on third-party providers to maintain security. He sees it as a risk-shifting exercise, where organizations trust their third-party partners to secure their environment adequately.

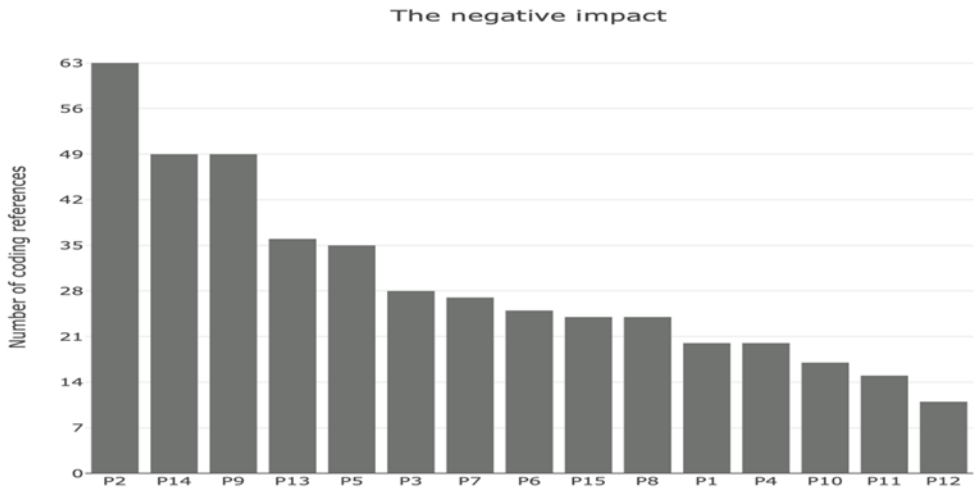
Social Engineering Attacks. Multiple perspectives are shared by the research participants, emphasizing the growing impact of these technologies on cyber threats and social engineering. All participants agreed that AI and ML play an effective role in increasing social engineering attacks. The research concluded that ML and deep learning technologies are considered effective tools for social engineering attacks, with several participants highlighting their potential for email and script generation, one participant suggests that ML can be used to generate emails and scripts for phishing attacks, making it easier to craft convincing messages. Additionally, ML can be employed for reconnaissance in phishing campaigns, enabling attackers to target specific individuals, such as CEOs, more effectively. It can correlate vast amounts of open-source data, providing attackers with precise information about individuals and their patterns of life, making tracking easier.

Participants 1, 2, 3, 6, 9, and 13 noted that AI can scrape the internet for personal information, images, and data, allowing attackers to create convincing fake profiles and websites to deceive victims. Participants 4, 5, 7, 8, 10, 11, and 15 pointed out the use of deep learning to create deep fake videos and audio, where a person's likeness and voice can be manipulated to deceive others. Participants suggested that AI can exploit data from social media and internet usage to learn about individuals' behavior, making social engineering attacks more sophisticated. Participants 12

and 14 emphasized AI mimicry and the ability to mimic human behavior and voice can lead to convincing impersonation in phishing calls, increasing the effectiveness of social engineering attacks. The participant acknowledged the importance of using code words within families due to AI's ability to mimic voices, posing a risk in social engineering attacks. Figure 8 number of coding references the number of coding by participant. The bar chart was created using NVIVO software.

Figure 8

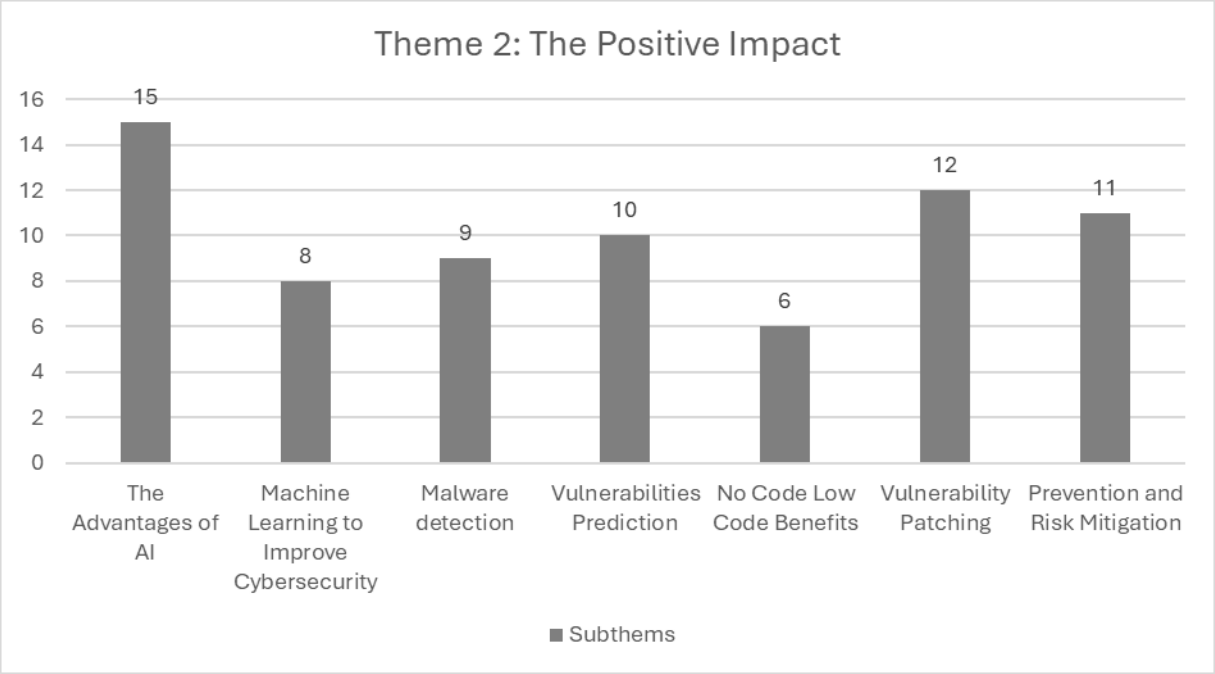
Theme 1 number of coding references by participants.



Theme 2: The Positive Impact. The second theme discovered in this research is the advantages of AI and ML (ML) technology in the field of cybersecurity. It is important to note that AI and ML can both be used to enhance cybersecurity efforts by automating tasks, improving threat detection, and streamlining processes. Figure 9 illustrate the subthemes related to theme 2, below is a detailed discussion of each subtheme:

Figure 9

Subthemes of theme 2 based on the responses gathered from participants.



The Advantages of AI. The participants highlighted various aspects of these advantages, all participants agreed that AI have different benefits to cybersecurity and organizations' security posture. One of the primary advantages mentioned is the ability of AI and ML to provide automated responses to cyber threats. This reduces the time it takes to detect and respond to security incidents. Automated systems can analyze and respond to threats much faster than humans, which is crucial in mitigating damage during cyber-attacks. AI has significantly bolstered cybersecurity by enhancing threat detection and response. ML algorithms can swiftly identify anomalies, predict potential breaches, and improve incident management. According to a peer-reviewed study published in the Journal of Cybersecurity, AI-based systems have reduced false positives and strengthened overall security posture (Ferrag et al., 2019). Some of the responses acknowledged that AI is particularly beneficial for endpoint security. It can quickly identify and isolate malware, block malicious IP addresses, and respond to various threats without requiring

human intervention. This not only enhances security but also frees up cybersecurity professionals to focus on more complex tasks.

Participant 13 suggested that AI and ML technologies help streamline and automate tasks, reducing the cognitive load on cybersecurity professionals. They can focus on high-level tasks and decision-making while AI handles routine and repetitive functions. This can lead to better decision-making and improved efficiency. Participants 3, 4, and 13 indicated that AI systems can operate continuously without interruptions. This round-the-clock monitoring is crucial in the constantly evolving nature of cybersecurity, where threats can emerge at any time. They added that AI can process and synthesize data faster than humans. It can assist cybersecurity professionals in connecting the dots, finding missing information, and making sense of large datasets. This can be particularly valuable in threat analysis and incident response. AI technology can help create more robust defensive measures by learning from past incidents and predicting future threats. This proactive approach can help organizations stay one step ahead of cybercriminals.

The participants assured that automation can reduce the risk of human error in cybersecurity processes. AI systems follow predefined rules and algorithms, minimizing the chances of mistakes in threat detection and response. AI and ML can help allocate cybersecurity resources more effectively. They can identify vulnerabilities and prioritize security tasks based on risk levels, ensuring that limited resources are used where they are most needed.

Among the other benefits mentioned in the responses, AI can be used to generate training tools and responsive tools that help train end users who may not be well-versed in cybersecurity. This contributes to a more informed and security-conscious workforce. It enables quick access to information and data, aiding cybersecurity professionals in their research and analysis. It can assist in searching for relevant information and providing answers to queries in real time. Additionally, it

was mentioned that AI and ML can analyze historical data to predict future cyber threats and trends. This can aid organizations in preparing for and mitigating potential risks.

ML to Improve Cybersecurity. The participants provided insights into how technology organizations utilize ML algorithms and AI (AI) to enhance cybersecurity. Several key points emerged from the research interviews. CrowdStrike is mentioned by participants 1 and 5 as an example of an organization using ML and AI to gain insights into system threats. They leverage ML to identify Advanced Persistent Threats (APTs) based on their database and threat fingerprints. ML models are employed to create attack models, allowing organizations to predict and understand the behavior of cyber attackers, which helps in developing effective defensive strategies and blocking attacks, particularly when attackers attempt to escalate privileges or gain administrator-level access.

Participant 3 indicated that AI and ML enable automated responses to security incidents. These systems can correlate logs with real-time network activity, enumerate the network to detect threats, and respond swiftly to emerging threats without human intervention. Automation is crucial for reducing response times and minimizing potential damage. Participants 1, 7, and 13 explained that ML is used to recognize patterns and anomalies in network data. By processing and analyzing large volumes of data, AI can identify deviations from the baseline, which may indicate a security breach or abnormal behavior. Participant 10 acknowledged that AI is employed to gather intelligence from user behavior and the latest technology trends. The gathered information helps organizations continually improve their security systems and processes, making them more effective in mitigating risks.

Participant 13 asserted that AI algorithms are used to mitigate fraud by associating facial recognition with identity documents and other proof of identity, income, and address. The

technology helps verify the authenticity of individuals and reduces fraudulent claims. Participants 2, 3, and 14 indicated that organizations use tools like Splunk and Nessus for log analysis and vulnerability scanning. These tools generate logs from various servers and applications, helping organizations detect weaknesses and ensure policy compliance. AI and ML further automate these processes and enhance the identification of potential threats. Participant 14 said that AI and ML aid in enforcing security policies, such as password policies. They can detect deviations from policy parameters, such as password history violations or unauthorized access attempts.

Malware Detection. The study found that ML techniques are essential for detecting malware, particularly in the ever-evolving landscape of cybersecurity (P1, P2, P3, P4, P7, P8, P9, P11, & P14). One of the primary methods for malware detection involves using ML algorithms. These algorithms are crucial for identifying and responding to the threats posed by malware, especially polymorphic malware that continuously adapts to evade traditional security measures. Malware detection modules play a critical role in this process. These modules are responsible for analyzing data that has been collected and trained into a model, which subsequently produces results relevant to malware detection. ML models can look for specific patterns and behaviors associated with malware, enabling them to determine whether a file or process is malicious.

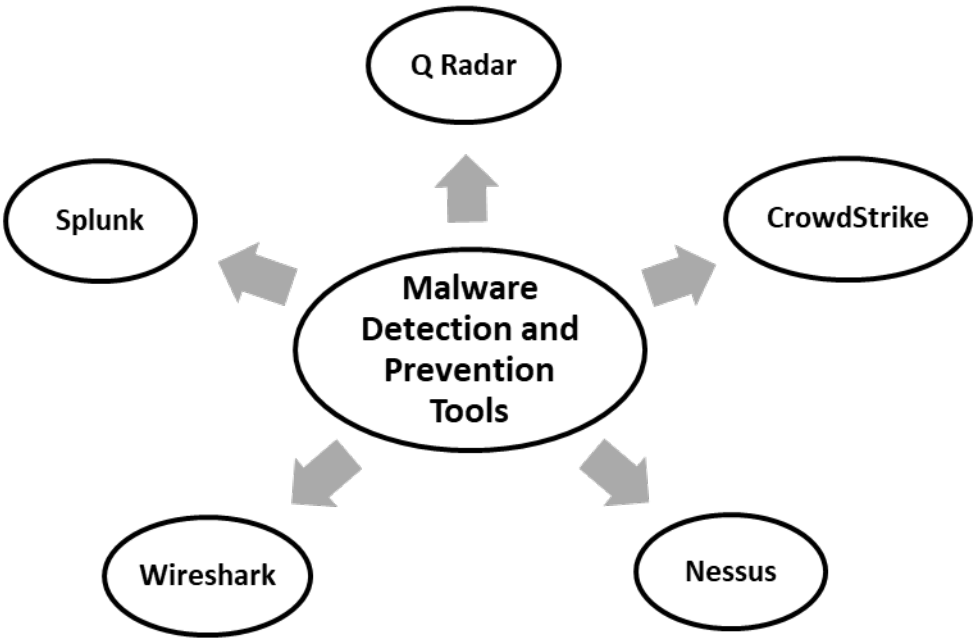
According to the answers to the interview questions that addressed the malware detection question, behavior-based detection is a significant aspect of ML in malware detection. It represents a shift from traditional perimeter security methods to a more proactive approach that focuses on monitoring and responding to threats in real-time. Instead of simply trying to prevent breaches, this approach observes and understands the behavior of potential threats, allowing for rapid intervention and mitigation. However, participants noted that behavior-based detection is typically employed after malware has already infiltrated a system, making it a post-breach strategy rather than a

preventive one. This approach aims to contain and neutralize threats as soon as they are identified, reducing the potential damage they can cause.

Participant 4 indicated that some ML techniques are specifically designed to address email phishing scams, a common attack vector. Software solutions like MEMA CAS (Mail Exchange Malware Classification and Scanning) are capable of detecting targeted email attacks and preventing data leaks, providing a layer of defense against phishing attempts. In addition to behavior-based detection, the participants mentioned several commercially available tools and platforms used for malware detection and prevention. Figure 10 shows some commercially available AI tools used for malware detection and prevention. These tools include:

Figure 10

Commercially available tools used for malware detection and prevention.



Q Radar. It is a threat detection and response platform mentioned in the interview responses. It leverages ML and AI to detect and respond to cybersecurity threats in real-time. Q radar enhances an organization's capability to monitor and analyze network traffic, detect

anomalies, and identify potential security breaches. The platform's rules-based detection system, coupled with ML capabilities, empowers organizations to proactively address threats and respond swiftly to cyber-attacks.

CrowdStrike. CrowdStrike is another notable tool discussed by participants, known for its ML algorithms and behavioral analytics. It offers a platform that identifies and stops threats by analyzing the behavior of processes and entities within a network. CrowdStrike's advanced tools use predictive analytics, ML, and anomaly detection to classify and mitigate potential threats effectively. The platform enables organizations to detect and respond to cyber threats, including malware, in real-time, enhancing their overall cybersecurity posture. CrowdStrike's approach focuses on post-breach intervention, identifying threats after they've entered the network and stopping them before they can cause significant damage.

Splunk. Participants 2, 3, and 14 identified Splunk as a pivotal tool in cybersecurity, they mentioned that it is known for its prowess in collecting, monitoring, and analyzing machine-generated data. It offers real-time visibility into network activities and system logs, enabling security professionals to rapidly identify and respond to threats. By aggregating data from diverse sources, including servers and security appliances, Splunk provides a comprehensive overview of an organization's digital environment. This platform's robust search and analytics capabilities empower security teams to spot anomalies, correlate events, and delve into incidents effectively. It facilitates customized dashboards and alerts, making it indispensable for proactive threat management and swift incident resolution.

Nessus. Nessus assumes a central role in cybersecurity through its proficiency in vulnerability scanning, a process that uncovers potential security weaknesses within networks and systems. While primarily focused on vulnerability assessment, Nessus indirectly contributes to

malware detection by pinpointing vulnerabilities that could be exploited by malicious software. It conducts comprehensive scans of an organization's infrastructure, highlighting issues like outdated software, misconfigurations, or open ports. This empowers security teams to prioritize and address vulnerabilities before cyber adversaries can capitalize on them. With an extensive database of known vulnerabilities and the capability to execute custom scans, Nessus bolsters a network's defenses against malware and other threats, enhancing overall cybersecurity resilience.

Wireshark. Participant 14 described Wireshark as a well-known network protocol analyzer used for monitoring and analyzing network traffic and packet data, while its primary function is network troubleshooting and analysis, it can also be instrumental in malware detection. By scrutinizing network traffic, Wireshark can reveal suspicious or anomalous patterns that may indicate malware activity. It enables cybersecurity professionals to monitor and analyze data packets, aiding in the identification of unusual or unauthorized network behavior. Wireshark serves as an essential tool for network administrators and security experts, helping identify potential threats and security breaches by inspecting data flows within a network.

These tools employ various techniques, including rule-based detection, Yara rules, and anomaly detection, to identify potential threats and protect systems from malware. ML techniques, when combined with tools like Splunk, Nessus, and Wireshark, contribute significantly to improving cybersecurity by enhancing the detection and response capabilities of organizations, thus helping them stay ahead of evolving cyber threats. While ML plays a crucial role in improving cybersecurity, its adoption can vary among technology organizations. Some companies, like storage-focused ones, may not heavily utilize ML for cybersecurity purposes. However, they often partner with companies specializing in computer and security, such as Cisco, to enhance their cybersecurity capabilities.

Vulnerabilities Prediction. Several participants offer their insights on whether AI and ML technology can be utilized to predict vulnerabilities in computer systems (P2, P3, P4, P5, P6, P7, P8, P10, P11, & P12). Participants 4, 6, 10, 12, and 14 discussed the role of AI in cybersecurity, particularly in scanning emails and incoming data for potential cyber threats. They mention that AI can help identify possible attacks before users interact with malicious content, enhancing preventive measures. The participants highlighted the potential of AI-powered defense mechanisms, such as user entity behavior analytics. They suggested that AI can help identify abnormal user behavior and trigger alerts, contributing to system security.

Participant 2 shared an example related to changes in system configurations. They explain that AI can be used to detect changes in the environment, such as modifications to password requirements. When such changes occur, AI can recognize vulnerabilities, like weak password policies, that could make the system susceptible to attacks. Participant 3 believes that AI can predict vulnerabilities through dynamic code testing. They emphasize the importance of integrating dynamic code testing into the software development pipeline to identify vulnerabilities. However, they also acknowledge that predicting vulnerabilities beyond the code level may be challenging. One participant expresses skepticism about the immediate ability of AI to predict vulnerabilities effectively. They highlight the challenge of predicting threats due to the chaotic and unpredictable nature of human behavior, while they believe AI can help detect threats sooner and possibly prevent some vulnerabilities. They are hesitant about using the term “predict” and emphasize the importance of pattern recognition.

The answers to the interview question “can AI/ML be used to predict vulnerability in the system?” took a cautious stance on AI’s role in predicting vulnerabilities. Some participants express concerns about rushing into AI implementation without proper governance, potentially

creating security risks. They emphasize the need for careful consideration and human oversight in AI applications for cybersecurity. The research participants shared specific AI-based tools and startups claiming to predict vulnerabilities. While some participants express interest in these tools, they remain cautious and acknowledge the importance of human intelligence alongside AI.

No Code Low Code Benefits. The interviews addressed the benefits of no-code and low-code applications, primarily focusing on their advantages in the context of cybersecurity and AI-based applications. It was agreed among Participants 2, 4, 5, 7, 9, and 10 that No-code and low-code applications are user-friendly, making it easier for individuals who are not coding experts to use and benefit from them. These apps are especially valuable for smaller organizations that may not have extensive cybersecurity expertise. They enable faster application development and deployment. Applications can be conceptualized and launched more quickly without being bogged down by extensive coding and security concerns. In the context of AI-based applications, no-code and low-code platforms reduce the need for extensive coding, which allows users to spend more time on designing experiments, models, or applications and less time on writing code. These tools are valuable for individuals who have knowledge of development principles and DevOps but may not be proficient coders. No-code and low-code platforms allow them to quickly design and assemble tools without extensive coding efforts.

Vulnerability Patching. The use of AI in enhancing the vulnerability patching process has emerged as a significant technological advancement with numerous benefits. In this research, IT and cybersecurity experts from various backgrounds provided insights into how AI can streamline and improve vulnerability patching procedures. The majority of participants agreed on AI's primary advantage in vulnerability patching lies in its ability to accelerate the process (P1, P2, P3, P4, P6, P7, P9, P10, P11, P12, P14, & P15). Traditional methods often require human intervention

to identify vulnerabilities, check for patches, and apply them. With AI, these tasks can be automated, reducing the time between the discovery of a vulnerability and its patch application. The automation allows for faster response times and a reduced window of vulnerability. AI can comprehensively monitor and manage vulnerabilities across large networks, something that would be extremely time-consuming for humans. AI models can detect when patches are available, immediately initiate the patching process, and even perform regression testing to ensure that new updates do not reintroduce old vulnerabilities.

Participants acknowledges that AI's role in vulnerability patching extends beyond automation. It can assist in prioritizing patches by identifying critical vulnerabilities specific to a network. This helps organizations allocate resources effectively, focusing on the most urgent patches first. Additionally, AI can predict high-risk activities and vulnerabilities, making it a proactive defense against potential breaches. One of the key advantages of AI in this context is its ability to reduce human error. AI-driven systems can execute patching tasks with a high degree of accuracy, minimizing the chances of mistakes that can lead to system failures or security breaches. This enhanced reliability is especially crucial in critical environments where downtime can be costly. Participants emphasized that AI should work in tandem with human experts, complementing their abilities rather than replacing them. AI can make skilled coders exponentially more efficient, enabling them to identify and patch vulnerabilities faster while also conducting more comprehensive testing.

Some participants cautioned that the reliance on AI may lead to a reduction in the use of manual quality assurance (QA) processes. They argue that QA teams are vital for ensuring the effectiveness of patches, as AI might not catch certain issues. Human QA testers can provide the critical human judgment and creativity needed to identify vulnerabilities that AI might overlook.

Participant 14 indicated that the impact on AI on vulnerability patching also extends to network access control (NAC) systems. NAC systems can use AI to detect anomalies in user behavior, such as accessing the network from foreign locations, and flag potential vulnerabilities. This proactive approach helps organizations maintain compliance and security.

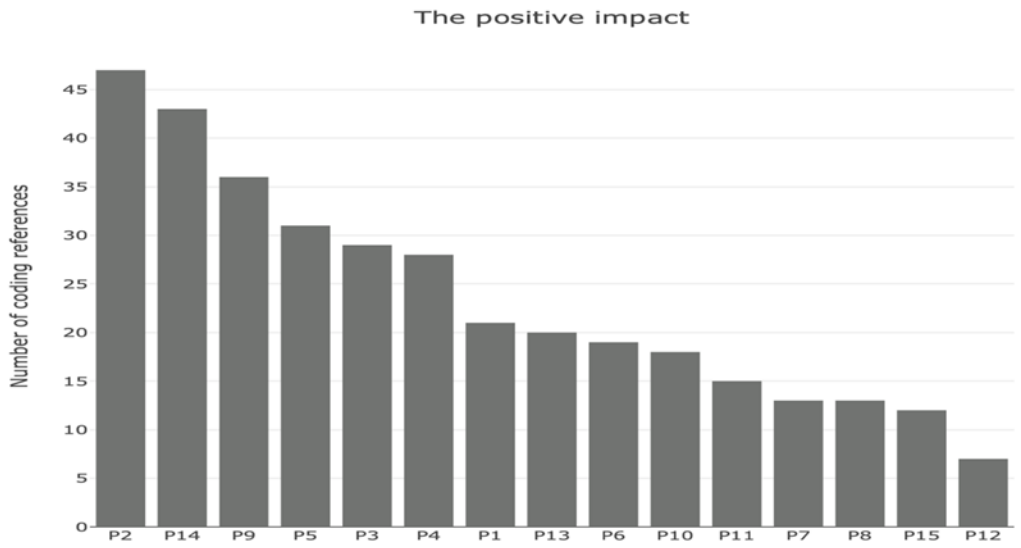
Prevention and Risk Mitigation. The participants' insights helped discovering various strategies and considerations for organizations' decision makers to minimize AI-related cyber-attacks and secure their networks from malicious activities. According to Participants 1, 2, 3, 4, 6, 7, 8, 9, 10, 11, and 15, decision makers need to ensure that their organization's security teams are well-informed and up to date on the latest cybersecurity trends and technologies. Staying current with industry developments is crucial to proactively defend against evolving threats. Participants stressed that organizations should develop a comprehensive security strategy that includes AI-related cybersecurity measures. This strategy should guide the Security Operations Center (SOC) and SOC managers in implementing security plans and workflows. Decision makers must invest in data and analytics tools to foster a learning environment within their organizations. This includes managing expectations, anticipating threats, and implementing realistic technology solutions. Organizations should have well-defined incident response plans in place to react quickly in the event of a cyber-attack. While it may not be possible to prevent all attacks, having effective response plans can mitigate the damage.

It was mentioned that outdated systems are vulnerable to cyber-attacks. Decision makers should allocate resources to invest in innovative systems and technologies with built-in security features to ensure their networks are protected against modern threats. Participants stressed the importance of investing in training programs to educate employees about AI-related cybersecurity risks and best practices. Employee awareness is critical in preventing cyber-attacks. Participants

emphasized the effectiveness of utilizing AI Defenses, leveraging AI technologies for defense is becoming increasingly important. AI can help detect and respond to threats faster and more accurately than humans. Organizations should consider using AI-based security tools and systems. Figure 11 illustrate the number of coding references by each of the 15 participants.

Figure 11

Theme 2 number of coding references by participants.



Theme 3: Investment in AI Technology.

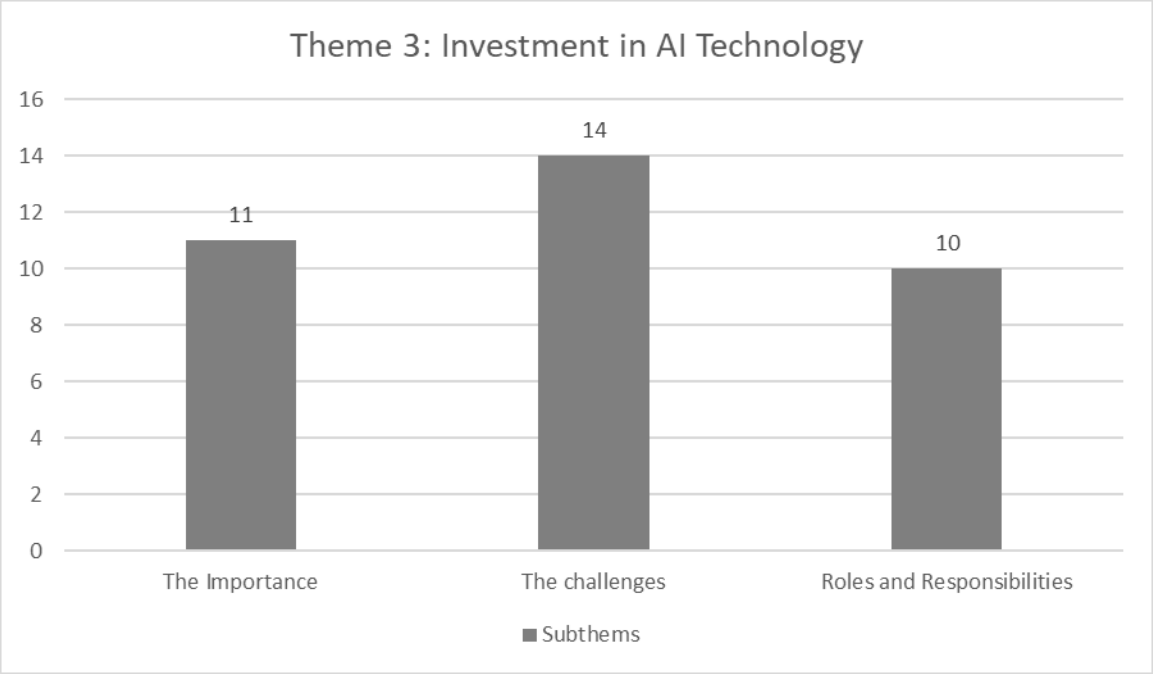
The Importance. Participants highlighted the importance of investing in AI technology to enhance cybersecurity in the high-tech industry in the United States. While the responses vary in detail, there is a consensus that AI is not only the future but also a critical tool for safeguarding businesses, organizations, and the nation as a whole against cyber threats. Participants 1, 2, 3, 4, 5, 7, 8, 9, 10, 11, and 12 stressed the inevitability of AI's role in cybersecurity. They argued that ignoring this shift is a mistake, as it is bound to change the dynamics of cybersecurity in a significant way. It is not just an option but a necessity. Investing in AI for cybersecurity is imperative. AI's ability to adapt, learn, and swiftly detect threats is a game-changer. Shaukat et al. (2020) highlighted the necessity of AI investments to stay ahead of evolving cyber threats and

safeguard sensitive data effectively. In the context of cyber warfare, AI is considered a critical tool. As adversaries use AI for attacks, investing in AI for defense and potentially offensive measures is seen as a logical step to maintain security. Participants shared critical insights regarding the counter AI and legislation challenges, and counter AI is identified as a significant concern, as attackers may employ AI techniques. Participants believe that legislation is seen as slow to catch up with the rapid advancements in AI technology, leaving businesses and organizations in a vulnerable position. The importance of holistic cybersecurity is emphasized in the answers. It is not just about firewalls and traps. It is about protecting all layers of an organization's data and operations.

Participants 4, 7, and 12 emphasized the need for more research, development, and testing of AI solutions for cybersecurity. This includes breaking down AI into layers and components to create robust security measures. Participant 4 suggested that the COVID-19 pandemic has highlighted the critical role of technology, making it imperative for the United States to stay at the forefront of technological advancements, including AI in cybersecurity. The consensus is that investment in AI for cybersecurity should be among the top priorities for organizations. It should not be relegated to a lower position but recognized as a crucial element of overall security strategies. Data volume and cloud migration was highlighted by participants as a good strategy, the high-tech industry deals with massive volumes of data, often in the petabytes. As organizations transition to the cloud, the need for AI becomes even more apparent. AI can efficiently process and correlate large datasets, enhancing network defense in an effective manner. Figure 12 demonstrates the subthemes related to theme 3.

Figure 12

Subthemes of theme 3 based on the responses gathered from participants.



The Challenges. The challenges that technology organizations in the United States face when it comes to building secure systems are complex. The challenges emerged as a sub theme in this study, these challenges are not unique to the United States and are shared by organizations globally. One of the fundamental challenges technology organizations faces is the sheer complexity and scale of their systems (Participants 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, & 14). As organizations grow, they accumulate an increasing number of technologies and endpoints that require robust security measures (Participant 1). The larger an organization becomes, the more challenging it becomes to oversee and manage every component effectively. This complexity can leave organizations vulnerable to security breaches, as any overlooked vulnerability can be exploited.

A critical challenge that resonates with technology organizations in the United States is patch management (Participant 2). Ensuring that systems are consistently updated with the latest

security patches is essential to mitigating vulnerabilities. However, organizations often grapple with this aspect, especially when they lack a dedicated vulnerability management team, and engineers responsible for patching systems fail to carry out their tasks promptly. The consequences of a single unpatched system can be dire, as it can serve as an entry point for attackers into an entire network. A significant shift in perception is currently taking place regarding the importance of security. Historically, security was often perceived as a business inhibitor rather than an enhancer. However, the rising tide of ransomware attacks has forced organizations to reevaluate their stance on security. Small businesses, in particular, may find it challenging to adapt to this evolving technology.

Participant 5 shared that legacy systems pose formidable challenge. Industries like healthcare often rely on outdated systems and software that are susceptible to vulnerabilities. Upgrading these legacy systems is not only expensive but also time-consuming. This challenge underscores the need for technology organizations to strike a balance between modernization and security. Lack of awareness, knowledge, and education in cybersecurity and emerging technologies like AI poses a significant challenge for many organizations. Participant 9 suggested that bridging this knowledge gap is crucial for the effective implementation of secure practices.

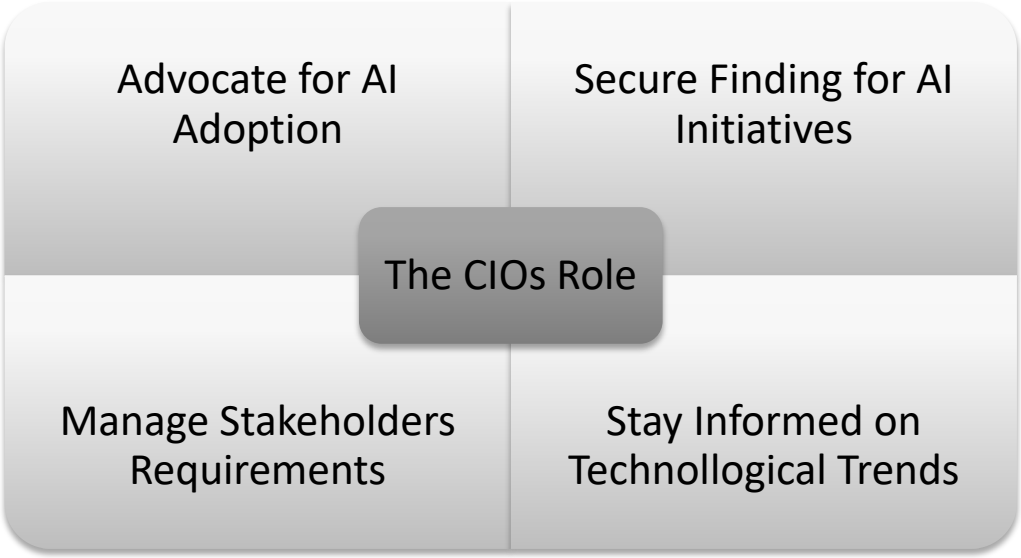
Participant 10 highlighted ethical considerations as another challenge, especially with AI and ML. These technologies can introduce bias into decision-making processes, necessitating a careful examination of the ethical implications of technology choices. Cyber threats are a global concern, with attackers becoming increasingly sophisticated worldwide. Organizations must continually enhance their security measures to keep up with these evolving threats. The United States, as a global technology hub, holds a dominant position in technology development and adoption. While this provides American organizations with access to cutting-edge technologies, it

also makes them attractive targets for cyber-attacks.

Roles and Responsibilities. The researcher was able to get valuable insights from 15 participants discussing the roles and responsibilities of decision-makers in the context of investing in AI technology and making critical cybersecurity decisions within their respective organizations. Participants 1, 3, 4, 5, 8, 9, 10, 11, 13, and 15 emphasized the pivotal role of the Chief Information Officer (CIO) in both investing in AI technology and making cybersecurity-related decisions. The CIO is expected to stay informed about technological trends, advocate for AI adoption, and ensure alignment with organizational goals. Their role also includes securing funding for AI initiatives and managing stakeholder requirements. Figure 13 illustrates the role of the CIO in investing in AI technology.

Figure 13

The role of the CIOs in investing in AI technology.



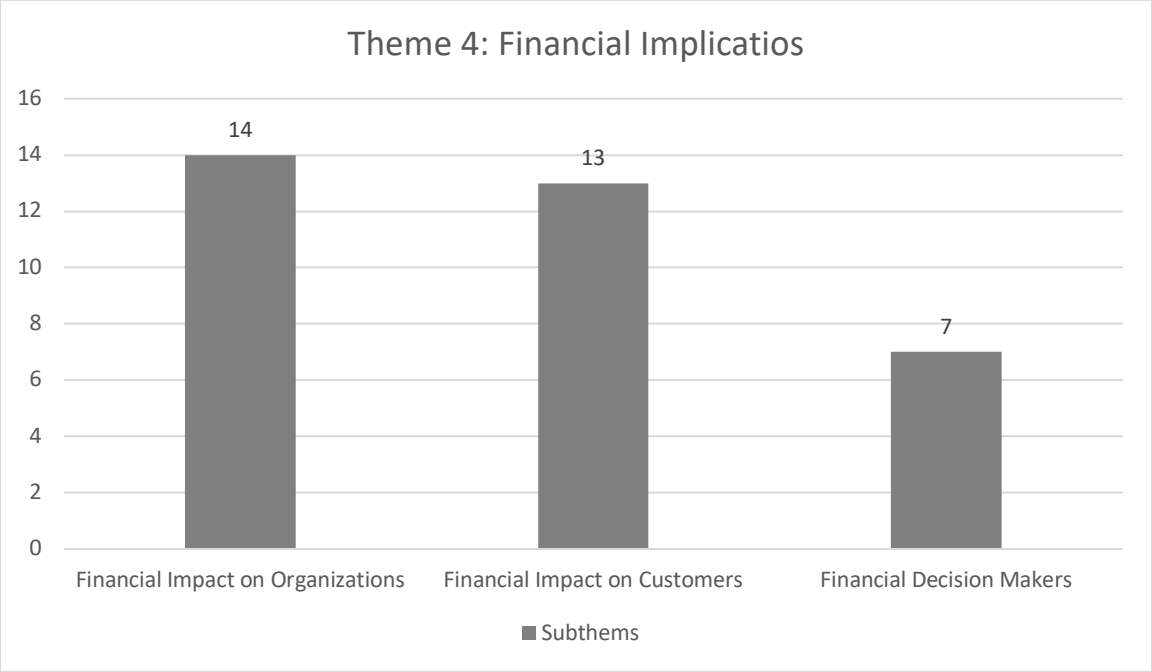
Collaboration emerged as a recurring theme, with participants highlighting the importance of teamwork among various stakeholders. Decision-making often involves a hierarchy, starting from IT managers and department heads, and ascending to CIOs or Chief Technology Officers (CTOs). In critical cybersecurity decisions, directors of cybersecurity and network security play

pivotal roles. Ultimately, CEOs and boards are responsible for overarching strategic decisions. The influence of business executives, including CEOs and boards, was acknowledged in investment decisions related to AI technology. These executives often play a strategic role in approving budgets and investments. Their perspective is shaped by considerations of the organization's long-term vision and its readiness to adapt to technological changes. Participants recognized that the specific titles and roles responsible for decision-making might vary based on the organization's size and industry. Some participants mentioned the involvement of CEOs and boards in critical decisions, while others highlighted the role of specific titles like CISO, CTO, or IT managers. Government agencies and large corporations may have distinct decision-making structures and processes.

Theme 4: Financial Implications. The financial impact of cyber-attacks and data breaches was a recurring theme. Organizations often face financial losses from data breaches, lawsuits, and damage to their reputation, which can run into millions or even billions of dollars. Customers also suffer, facing identity theft, fraud, and loss of trust in the organization. The cost of dealing with these consequences adds to the financial burden. As AI-driven attacks continue to evolve, organizations need to invest in AI-based cybersecurity to mitigate these financial risks and protect their clients' interests (Tufail et al., 2021). Participants asserted that inadequate investments in cybersecurity can lead to significant financial losses, making it imperative for organizations to allocate resources wisely. Several participants provided insights into the potential consequences of such incidents, and common sub themes emerged including the financial implications on organizations, customers, and the key individuals responsible for making critical financial decisions regarding their organization's cybersecurity and AI (AI) technology. *Figure 14* represent the subthemes of themes 4 bases of participants responses.

Figure 14

Subthemes of theme 4 based on the responses gathered from participants.



Financial Impact on Organizations. Organizations face significant financial repercussions due to cyber-attacks. The consequences include the cost of repairing systems, implementing security measures, and potentially paying ransoms to attackers. Loss of revenue is a common theme. Attacks can disrupt operations, leading to financial losses, especially in industries like utilities or healthcare. Legal ramifications, including potential fines and lawsuits, can impose additional financial burdens on organizations. Reputational damage and intellectual property damage are key concerns. Organizations may lose customer trust and loyalty, impacting their brand image and long-term financial prospects (See Figure 15 that shows the financial impact on organizations). The financial impact varies depending on the industry and the specific nature of the attack. Responding to cyber incidents, especially in the case of zero-day vulnerabilities, can consume significant time and resources, leading to financial burdens. Implementing security patches and updates across systems can be a time-sensitive and costly process. The concept of "no

trust environments," was mentioned by participants in this research, where organizations become more cautious and restrictive in their network access. This can create financial challenges as it affects employees' ability to perform their tasks efficiently. The cost of cybersecurity measures is seen as a necessary expense to protect against potential financial devastation caused by cyber-attacks. Participants emphasized the importance of organizations investing in cybersecurity to mitigate financial risks. This includes training staff, adopting advanced technologies like AI and ML, and establishing robust security measures.

Figure 15

The financial effects of automated cyber-attacks on organizations.

Financial Impact on Customers. Customers can suffer financially from cyber-attacks, primarily due to identity theft and fraud. Stolen personal information, such as Social Security numbers and credit card details, can be misused, resulting in financial losses for individuals. Customers may experience stress and inconvenience in dealing with the aftermath of a breach, such as monitoring their accounts and resolving fraudulent transactions. Loss of trust in the affected

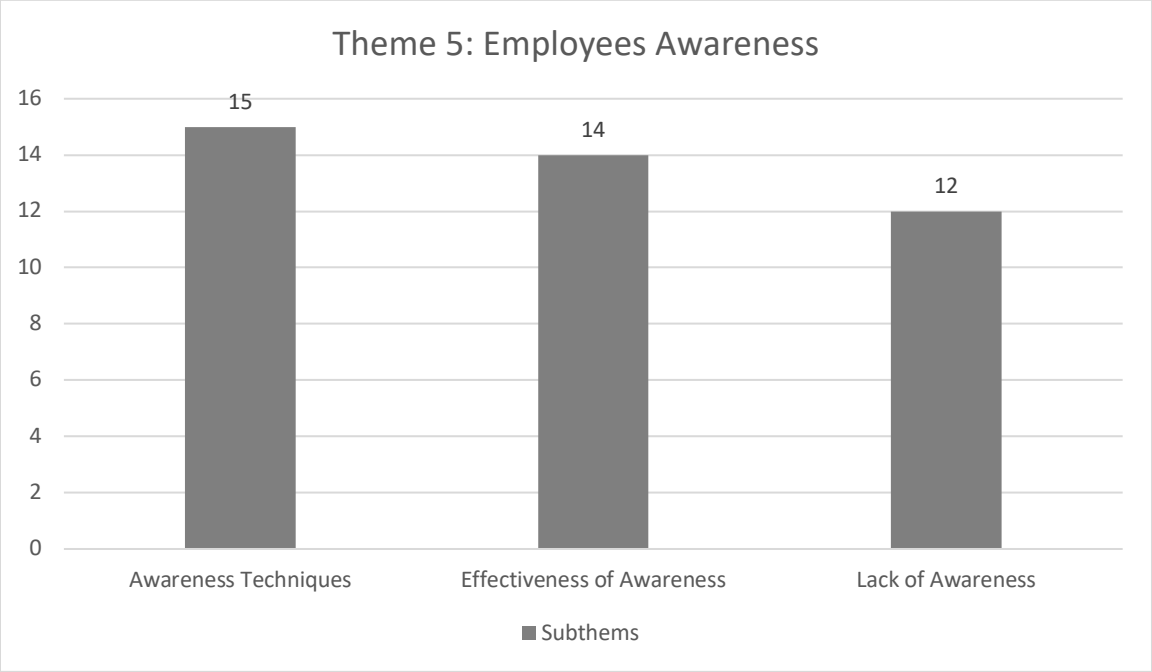
organization can prompt customers to switch to other service providers, potentially affecting their financial stability.

Financial Decision Makers. The interview questions addressed the key individuals responsible for making critical financial decisions regarding their organization's cybersecurity and AI technology. Several common patterns emerged from the participants' answers. One of the prominent patterns in the responses is the varying levels of decision-making authority within organizations. Participants highlighted that the ultimate decision-makers for financial matters related to cybersecurity and AI technology can differ based on factors such as the organization's size and the specific circumstances surrounding the decision. Participant 1 stated that the head of the division responsible for cybersecurity and AI technology is the one making these critical decisions. Participants 2, 3, 4, 8, and 15 indicated that the decision-making process involves the Chief Information Security Officer (CISO), product managers, and the CIO. The involvement of the CEO or board members may also be necessary, particularly for decisions exceeding certain thresholds. Participant 5 suggests that the Chief Financial Officer (CFO) plays a role in financial decisions. While not a consistent theme across all responses, several participants mention the CFO's role in providing financial data, recommendations, or support to the CEO and board members. Participants frequently acknowledge the potential involvement of the CEO and board members in making significant financial decisions. This suggests that, in many cases, ultimate decision-making authority may rest with these high-level executives.

Theme 5: Employees Awareness. This theme revolves around the importance of employee awareness and compliance in enhancing cybersecurity within their organizations. Several key findings emerged from participants' responses to the interview questions. Figure 16 shows the subthemes emerged from theme 5 based on the participants answers to the interview questions.

Figure 16

Subthemes of theme 5 based on the responses gathered from participants.



Awareness Techniques. Various techniques employed by different participants' organizations to enhance employee awareness and compliance against cyber attacks. The primary theme that emerges from the answers is the emphasis on training and education (P1, P2, P3, P4, P5, P7, P8, P9, P10, P11, P12, P13, P14, & P15). Many organizations conduct annual training sessions as a foundational method to improve employee awareness and compliance. These sessions cover various aspects of cybersecurity and are mandatory for all employees. According to Participant 6, some organizations use simulated phishing campaigns to test employee responses. These campaigns involve sending fake phishing emails to employees to gauge their susceptibility. Those who fail may undergo additional training. Other organizations implement comprehensive security awareness programs, which may include tabletop exercises and other practical activities. These programs aim to educate employees on cybersecurity best practices and real-life scenarios.

Many participants highlighted that newsletters and emails are used to disseminate

information and reminders about cybersecurity best practices. Regular communication ensures that the topic remains at the forefront of employees' minds. New employees are often required to complete cybersecurity training during their onboarding process. This ensures that all staff members, regardless of their tenure, are aware of security protocols. Participants suggest implementing accountability systems to monitor employee compliance. This includes periodic audits and monitoring of employee workstations to ensure adherence to cybersecurity guidelines. Continuous learning is promoted through periodic updates and refresher courses. Participants stress the importance of keeping employees informed about evolving threats and developments in cybersecurity. Participants suggest exploring the potential of AI for creating more dynamic and personalized training experiences in the future.

Effectiveness of Awareness. All participants except for participant 12 emphasized that employees are often the first line of defense against cybersecurity threats. They stressed that employees who are aware of potential risks and trained to identify them can significantly reduce the organization's vulnerability. This includes recognizing and avoiding suspicious links, phishing attempts, and other common attack vectors. A well-informed workforce can serve as the first line of defense. Alrobaian et al. (2023) emphasized that a significant percentage of cyber incidents result from human error or negligence. Employees need to recognize the signs of phishing, social engineering, and other cyber threats. Many organizations conduct regular cybersecurity training and education programs for their employees. These programs cover topics such as phishing attacks, cyber threats, and confidentiality. Regular training is seen as a vital component of building a security-conscious culture within the organization. This proactive approach can reduce the likelihood of successful AI-driven attacks, safeguard sensitive data, and protect an organization's reputation, financial well-being, and client trust (Kweon et al., 2021). Phishing attacks are

highlighted as one of the most prevalent and effective methods of cyber-attacks. Participants discussed how their organizations simulate phishing scams to test employee awareness and response. Employees who fail these tests may face warnings or potential consequences, highlighting the seriousness of the issue. Some participants expressed concerns about the evolving threat landscape, particularly with the integration of AI and ML into cyber-attacks. They mentioned the need for specialized training to address these emerging challenges, indicating that cybersecurity education must keep pace with technological advancements. Participant 10 suggests that training alone is not sufficient and that there should be a system of accountability tied to employee performance appraisals. Holding employees accountable for practicing good cyber awareness and security practices is seen as a way to ensure compliance.

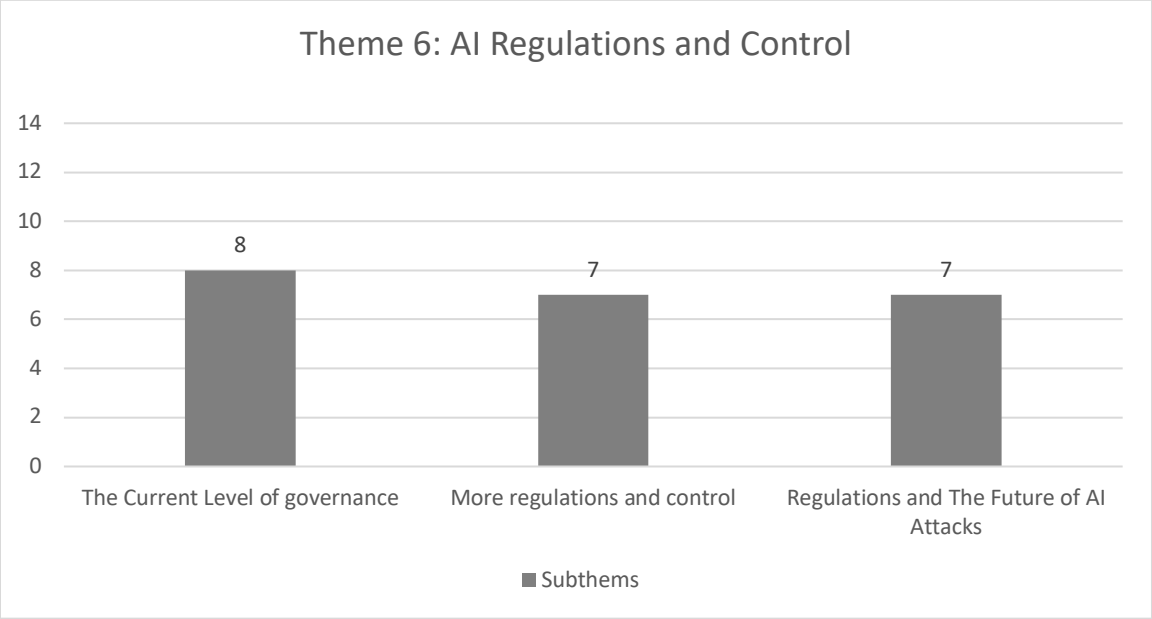
Lack of Awareness. Participants 2, 3, 4, 5, 6, 7, 8, 9, 11, 13, 14, and 15 provided insights into their experiences and perspectives regarding cybersecurity incidents, employee awareness, and compliance in their respective organizations. Several participants mentioned incidents where a lack of employee awareness led to security breaches. These incidents ranged from employees clicking on suspicious links in emails to downloading and installing unauthorized software. In one case, a compromised admin's lack of awareness resulted in a cyber-attack. Phishing attacks were a common thread in the responses. Participants highlighted the importance of recognizing phishing attempts and the tactics used by cybercriminals to trick employees. They emphasized the need for employees to scrutinize email links and verify the legitimacy of messages, especially those related to job offers or sensitive information. Many participants noted that their organizations encouraged employees to report suspicious emails or incidents promptly. Reporting was seen as a crucial step in preventing cyber incidents. Some organizations had systems in place to notify others when a potential threat was identified, such as the automatic notification system in Google.

One participant highlighted a security vulnerability related to convenience in their organization, where sensitive documents left unattended at a shared printer could be accessed by unauthorized personnel. Employee awareness and compliance with security protocols were instrumental in reducing this vulnerability. Social engineering attacks were discussed as a common threat, with employees trained to question unfamiliar requests and verify the identity of individuals making such requests. Education and awareness played a significant role in mitigating the risks associated with social engineering. Some participants acknowledged that employees actively engaged in identifying and reporting security threats. They mentioned instances where employees took proactive steps to prevent cyber incidents, such as questioning suspicious phone calls or emails.

Theme 6: AI Regulations and Control. This theme addressed the current state of governance and regulations related to open-source AI-based tools in the United States. The research participants held diverse viewpoints on the need for governance and regulations in the AI field. Figure 17 shows the subthemes emerged for theme 6. The subthemes include the current level of governance on publicly available AI tools, the need for more regulations and control on these tools and how regulating these tools will affect future automated cyber-attacks.

Figure 17

Subthemes of theme 6 based on the responses gathered from participants.



While some emphasize the need for stricter controls to prevent misuse and protect privacy, others are cautious about overregulation and emphasize the importance of individual and organizational responsibility. The theme highlighted the complexity of AI governance and the ongoing need for dialogue and coordination in this rapidly evolving field. Brundage et al. (2018) argued for increased scrutiny of open-source AI systems to address ethical and safety concerns.

The current level of Governance. Participants 1, 2, 5, 7, 12, 10, 11, and 15 expressed that the current regulations on AI in the United States are insufficient and that they need more comprehensive governance, emphasized the need for stricter governance, particularly in situations where employees use AI tools like Chat GPT to access sensitive company information. They emphasize the importance of protecting against data breaches and maintaining confidentiality within organizations. Almeida et al. (2023) discussed the importance of governance mechanisms to monitor, audit, and control open-source AI, preventing misuse and maintaining public trust. Open-

source AI regulation must strike a balance, ensuring responsible use and avoiding stifling innovation. However, establishing effective control mechanisms is crucial (Almeida et al., 2023). When asked about open-source AI tools that could automate cyberattacks, Participant 2 mentions Chat GPT as a potential tool that could be exploited for malicious purposes. Participant 10 highlights the lack of governance in place for AI tools, particularly regarding the information they handle and the need for more regulation to protect privacy and organizational data.

Participants 7, 12, and 15 suggested that the current level of governance varies depending on the government department involved. The participants expressed concern that the government has too much control over this technology and should not restrict access. They expressed a preference for minimal government control, citing concerns about taking away freedoms, suggesting the importance of individual companies implementing their own internal governance. They also pointed out the challenge of regulating AI without impeding freedom and innovation, suggesting that regulations should be implemented within AI-generated content rather than restricting access to AI.

More Regulations and Control. Participants 1, 2, 3, 5, 10, 11, and 14 emphasized the need for more governance and the impact of regulation on future cyberattacks. The responses highlighted different perspectives and concerns regarding the rapidly evolving field of AI and its potential consequences. Participant 14 discussed the strict regulations within their organization, particularly regarding third-party applications. Acknowledging the need for more talks and discussions about AI governance. Participant 3 acknowledged the need for some form of regulation but highlights the challenge of enforcing regulations effectively when individuals or organizations can simply move to jurisdictions with lax rules. Participant 5 discussed the need for regulating AI use within their organization, particularly in the workplace, mentioning concerns about legalities

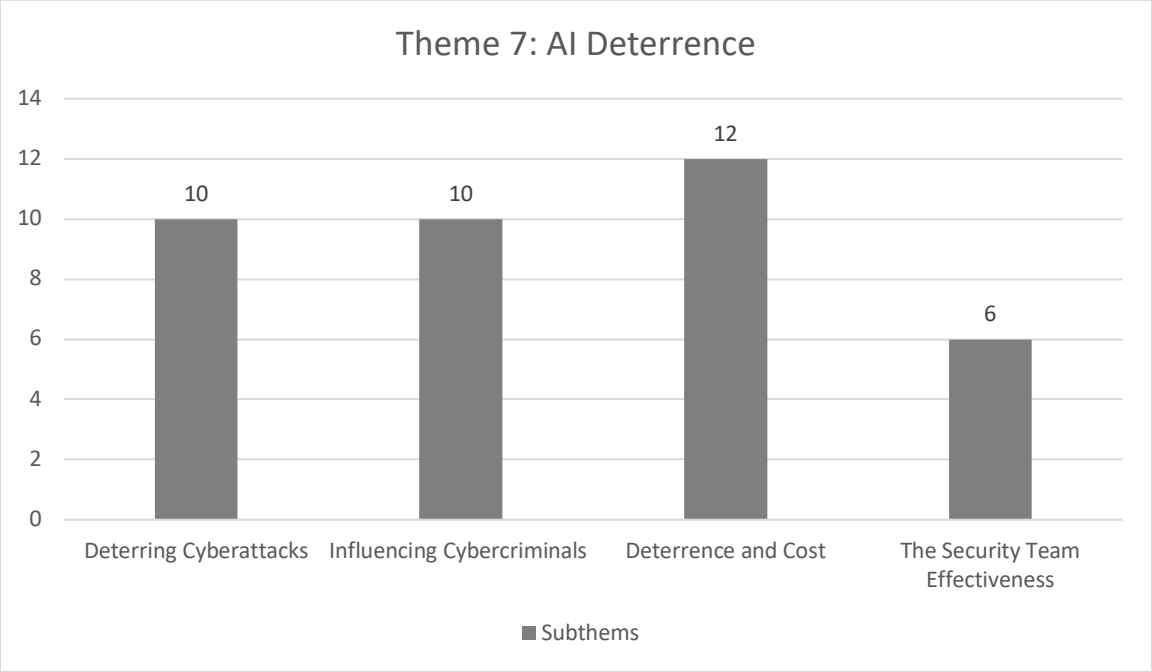
and the necessity of standard operating procedures when dealing with AI.

Regulations and The Future of Cyber-attacks. Participant 6 suggested that there is currently no government legislation regarding open-source AI tools in the United States and there is a need for future regulations. They point out that while privacy laws may exist, they do little to prevent misuse of open-source AI tools. They also anticipate that larger companies like Google, Azure, and Amazon may be the first to address these issues. Participant 8 indicated the governance within their school district, which blocks certain AI applications, expressing the need for government regulations to prevent individuals from making unwise decisions due to a lack of awareness about AI. Participant 9 noted the absence of government regulations in the United States but mentioned Italy's ban on open AI access. The participant also pointed out the potential for AI to replace certain professions and suggested that regulations may be needed to prevent complete AI substitution. Participant 13 discussed the complexity of governance and suggested that unifying bodies should be established to regulate the use of AI tools. The participant anticipated that regulations will be needed to prevent potential damage.

Theme 7: AI Deterrence. The theme of AI deterrence was the result of 15 participants' answers to the interview questions. The participants identified several effective ways to deter cyberattacks. Figure 18 below shows four subthemes that emerged from AI deterrence theme based on the interviews' outcomes.

Figure 18

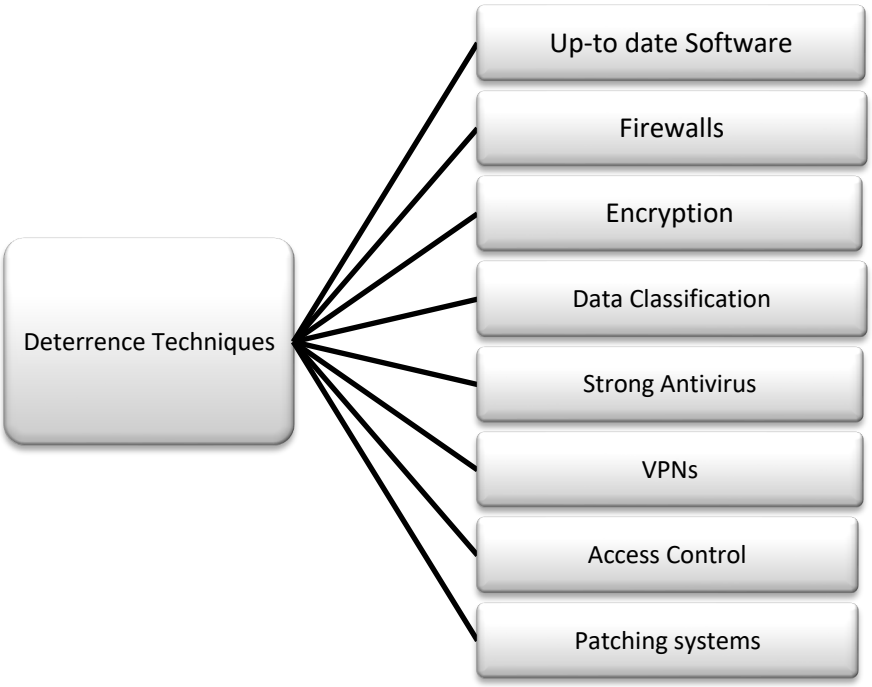
Subthemes of theme 7 based on the responses gathered from participants.



Deterring Cyber-attacks. Participants 1, 2, 4, 6, 7, 8, 9, 10, 14, and 15 emphasized the importance of awareness, education, and training as effective ways to deter cyberattacks. Participants mention the need for up-to-date software, strong antivirus programs, VPNs, firewalls, and other technological safeguards to protect against cyber-attacks. They emphasize the need for regularly patching systems and ensuring software is current. Some participants highlighted the significance of data classification, access control, and encryption as deterrents against cyber-attacks. By effectively managing and securing sensitive data, organizations can make it harder for hackers to access valuable information (See Figure 19).

Figure 19

Effective ways to deter cyberattacks according to the research participants.



Participant 6 identified the three key elements for deterring cyberattacks as securing systems, training people, and effective password management. Education and awareness are key components of cyber-attack deterrence. Participants expressed the value of educating employees to recognize and avoid phishing attempts and other cyber threats. Proactive measures, such as continuous training and phishing simulations, are seen as essential in preventing attacks. Cyber deterrence is a critical concept in today's interconnected world, aiming to dissuade potential cyber adversaries from launching attacks through the threat of severe consequences. Libicki (2009) emphasized the need for clear cyber deterrence strategies, as vague policies can lead to ambiguity and increased risk. Effective cyber deterrence combines a mix of capabilities, including law enforcement, intelligence, diplomacy, and military options.

Influencing Cybercriminals. Ten participants agreed about the possibility to influence cybercriminals not to initiate cyber-attacks through implementing different techniques, these

techniques include being a stronger target and less attractive to the hackers, done good patching to the system, reputation of the organization, invest in training and awareness, punishment and strong antivirus and VPN (P1, P2, P3, P4, P6, P7, P8, P11, P13, & 14). The concept of defense in depth is mentioned which is related to the nine D's of cybersecurity mentioned in Section 1. The participant emphasized the deployment of multiple layers of security measures, such as firewalls, IDS/IPS, and bastion hosts, to slow down or deter attackers. Several participants stress that the weakest link in cybersecurity is often the human element. Participant 1 emphasized the importance to be less attractive and hard target for the cybercriminals, Participant 1 stated "It's about being harder to rob than someone else I mean part of it you just don't want to be the attractive one." Social engineering and phishing attacks are common tactics used by cybercriminals, making employee training and awareness crucial. Monitoring network traffic and system behavior is crucial to detecting anomalies that may indicate a cyberattack. Being vigilant and responsive to unusual activities is a key theme. Some participants suggest that holding cybercriminals accountable through stricter regulations and harsher punishments can influence cybercriminals and serve as a deterrent.

Deterrence and Cost. The participants discussed the cost-effectiveness of deterring cyber-attacks before they occur versus dealing with them after they happen. One of the interview questions focused on prevention versus reaction, Participants 1, 2, 5, 6, 7, 8, 9, 11, 12, 13, 14, and 15 expressed a preference for prevention over reaction. They argue that investing in proactive measures to deter cyber-attacks is more cost-effective than dealing with the consequences after an attack has occurred. Prevention is seen as a way to avoid the potentially high costs associated with damage control, data breaches, and reputational damage.

The Security Team's Effectiveness. The effectiveness of a security team is considered critical in both deterring and preventing cyber-attacks. A skilled and proactive security team can

contribute significantly to an organization's ability to detect and prevent cyber threats. The participants stress the importance of thinking outside the box and being vigilant in monitoring and responding to potential security issues. The reputation of an organization's cybersecurity practices, and perceived strength can influence whether it becomes a target. Demonstrating a commitment to security can deter potential attackers (Participants 1, 2, 4, 6, 7, & 9). Some participants pointed out that learning from the experiences of others can be valuable in cyber-attack deterrence. They suggested that studying past incidents and understanding vulnerabilities can help organizations enhance their security posture.

Theme 8: The Cloud and Internet of Things (IOT).

The Cloud. The interviews featured similar responses among several participants on the topic of enhancing cloud security using AI and ML (ML) technology, as well as the potential threats posed by AI to cloud security. Participants 2, 3, 8, 9, 10, 11, 12, 13, and 15 highlighted the importance of AI in providing real-time monitoring and threat detection, especially in the dynamic and fast-paced cloud environment. Sreedevi et al. (2022) indicated that AI systems can analyze vast datasets to identify anomalies, predict potential breaches, and enhance access control, reducing the attack surface in the cloud. While AI can quickly identify threats and vulnerabilities, human expertise is still essential for decision-making and strategy. There is a consensus among participants that AI should complement human intelligence rather than replace it. Participants emphasized the need of understanding where data are located in the cloud and classifying it appropriately. AI tools can help in data classification, allowing cybersecurity analysts to focus on high-risk areas. Best practices like using multi-factor authentication and strong passwords are crucial for cloud security. Participants pointed out that AI can also pose threats to cloud security due to the dynamic nature of AI attacks, which can adapt quickly, and is seen as a challenge. There

is concern about attackers using AI to imitate identities or gain unauthorized access to cloud resources. Cloud services are expected to provide high availability, and data can be geographically distributed globally. Participants discuss the need to defend against attacks like bots that generate a high volume of requests, which can strain cloud resources. While AI augments cloud security, it is essential to address concerns about adversarial attacks on AI systems (Biggio, 2010).

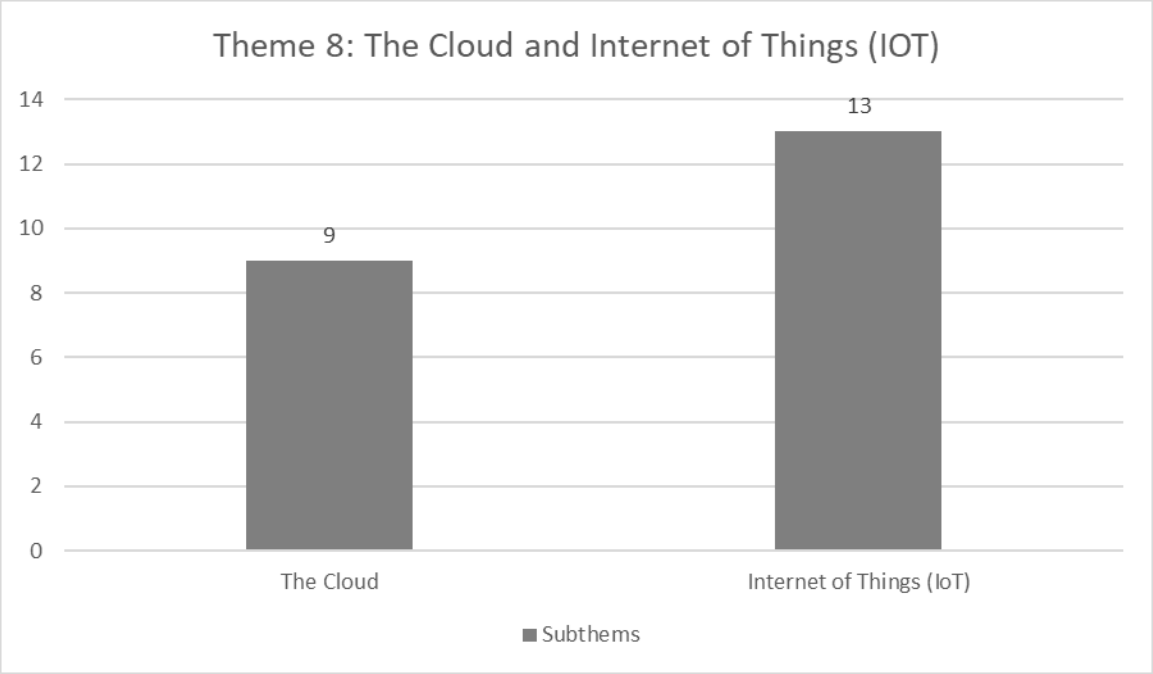
Internet of Things (IOT). AI-powered systems can detect unusual behavior and potential threats in IoT networks, enabling swift response (Abdel-Basset et al., 2018). The interviews covered the security and privacy challenges associated with Internet of Things (IoT) devices, as well as the potential role of AI and ML in addressing these issues. Participant 2, 4 acknowledges the vulnerabilities of IoT devices and expresses concern about guests connecting their devices to their network. Sharma et al. (2020) mentioned that ML aid in anomaly detection and threat prediction, emphasizing the importance of balancing innovation with safeguarding IoT ecosystems. Participants 3 and 5 highlight the insecurity of IoT due to a lack of updates and accountability from manufacturers. They propose the need for a governance strategy and governmental intervention to ensure the security of IoT devices. Participants 4 and 5 asserted the importance of changing internet passwords regularly to minimize vulnerabilities, emphasized that most residential users fail to change their network passwords frequently, leaving their IoT devices at risk. They suggested strategies to reduce the attack surface of IoT, including regular updates and patches, monitoring IoT assets, and network segmentation for IoT devices. They also pointed out the readily available information on IoT devices through tools like Shodan. One participant specializes in governance and compliance, indicated the importance of AI in ensuring cloud services meet regulatory requirements. Participants 7, 14, and 15 predicted that malicious actors will use AI to exploit IoT devices, potentially causing disruption, privacy breaches, or unauthorized control over appliances.

They highlighted the wide range of IoT devices, from trash cans and refrigerators to security cameras, and the susceptibility of these devices to hacking if not properly secured. Participant 6 confirmed IoT vulnerability to cyber-attacks, with the participant highlighted the challenge of patching and updating IoT devices, especially those that do not do so automatically, stressing the need for security measures as IoT becomes more prevalent, even in biological applications. Participant 7 indicated a preference for manual control over technology and expresses concern about the growing number of access points in networks, which increase security risks. Participant 8 proposed using AI to determine when IoT devices are not in use and disconnect them from the internet to prevent potential attacks during idle periods. They also mention the risk of AI-powered listening devices.

Participant 10 stressed the importance of securing IoT devices, particularly those like Alexa and Siri, is underscored. The participant mentioned the potential for malicious intent and data gathering if security is not robustly implemented. Participant 11 expressed optimism about using AI to predict and prevent threats to IoT devices, citing AI's ability to analyze data and improve security measures. They acknowledge the inherent vulnerabilities in IoT devices. While Participant 12 expressed concern about privacy breaches through IoT devices, citing examples of devices like Facebook apps recording conversations. They worry about companies having control over household appliances connected to the internet. Participant 13 raised concerns about the potential for nefarious individuals to exploit AI and ML to hack into IoT devices, emphasizing the vulnerability of IoT appliances connected to the internet. Figure 20 below shows the advantages and threats of AI technology on the cloud and IoT as two subthemes of theme 8.

Figure 20

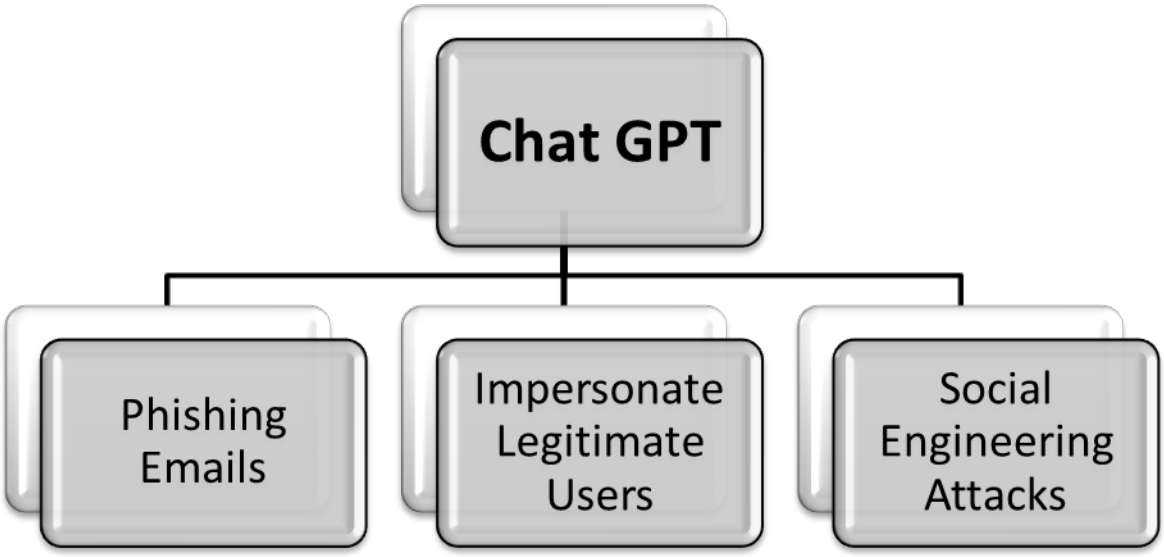
Subthemes of theme 8 based on the responses gathered from participants.



Theme 9: Chat GPT and Cybersecurity. The participants contemplated the potential for Chat GPT or similar models to generate malware. They envisioned a scenario where such AI-driven systems might interact with individuals, attempting to coax them into executing malicious code. While the plausibility of this scenario remains uncertain, the participants entertained the notion of AI being leveraged for social engineering purposes, potentially leading to the execution of harmful actions. Chat GPT can be exploited for malicious purposes. These systems can generate convincing phishing emails, impersonate legitimate users, and engage in social engineering attacks. AI-driven chatbots can amplify the scale and sophistication of cyber-attacks (Blauth et al., 2022). Figure 21 below illustrate the potential use of Chat GPT to conduct automated cyber-attacks.

Figure 21

The potential use of Chat GPT to conduct automated cyber-attacks.



Participant 15 stated,

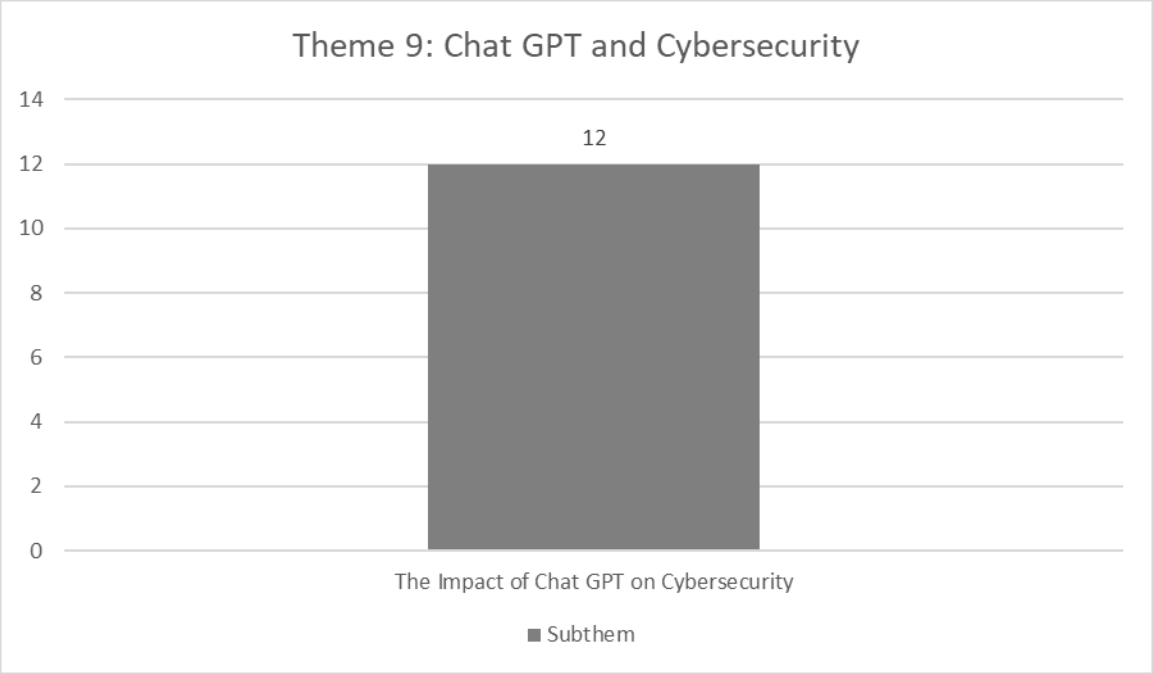
> There are some people who are using some AI mechanics right now (i.e., chat GPT and the Google BARD system to generate programs to go through and try and find holes in firewalls or to go against Linux systems or Apple systems to try and find a way in).

The participants discussed the use of AI, specifically Chat GPT, in both cyber-attacks and cybersecurity. Participants 1, 2, 3, 5, 6, 7, 8, 9, 10, 13, 14, and 15 highlighted concerns about the potential misuse of AI for malicious purposes, such as writing malware and conducting phishing attacks. Some of the participants also discussed the need for governance and regulations to address these concerns. Participant 14 indicated that while AI models like Chat GPT will not directly respond to requests to write malware, attackers can manipulate the system by changing the prompts to reflect normal behavior. This means that attackers can use AI models to generate code or instructions that can be used for malicious purposes. Figure 22 illustrate the impact of Chat GPT on

cybersecurity based on the responses to the interview questions.

Figure 22

Subtheme of theme 9 based on the responses gathered from participants.



Multiple participants expressed concerns about the misuse of AI, particularly Chat GPT, in cyber-attacks. They mentioned that hackers can manipulate AI systems to generate code, create phishing emails, and potentially write malware. Participant 13 stated that "to use Chat GPT as an example, they can literally automate the chats, you can get just like random emails, phishing links, you click on it and bam, you're hooked the entire organization is hooked." This pattern highlights the adaptability of AI tools for malicious purposes. Participants emphasized the role of AI in social engineering and phishing attacks. They mentioned that AI-powered chatbots can engage with victims via email or chat, leading them to click on malicious links or divulge sensitive information. Some participants acknowledged the benefits of AI in cybersecurity, acknowledged that AI tools can automate security processes, strengthen firewalls, and simplify business processes. Several participants argued that there is a need for more governance and regulations concerning AI,

especially in critical areas like tax filing and professional services. They suggested that regulations should ensure privacy protection and prevent AI from replacing licensed professionals entirely. Participants recognized some AI tools like Chat GPT are accessible globally, not limited to specific regions or countries. This global accessibility raises concerns about potential information leakage and misuse of AI on a global scale. The need for international governance and standards is implied. While Chat GPT is highlighted as a potential tool for cyber-attacks, participants do not mention other specific AI tools used by cybercriminals. This suggests that Chat GPT is a prominent example in their responses.

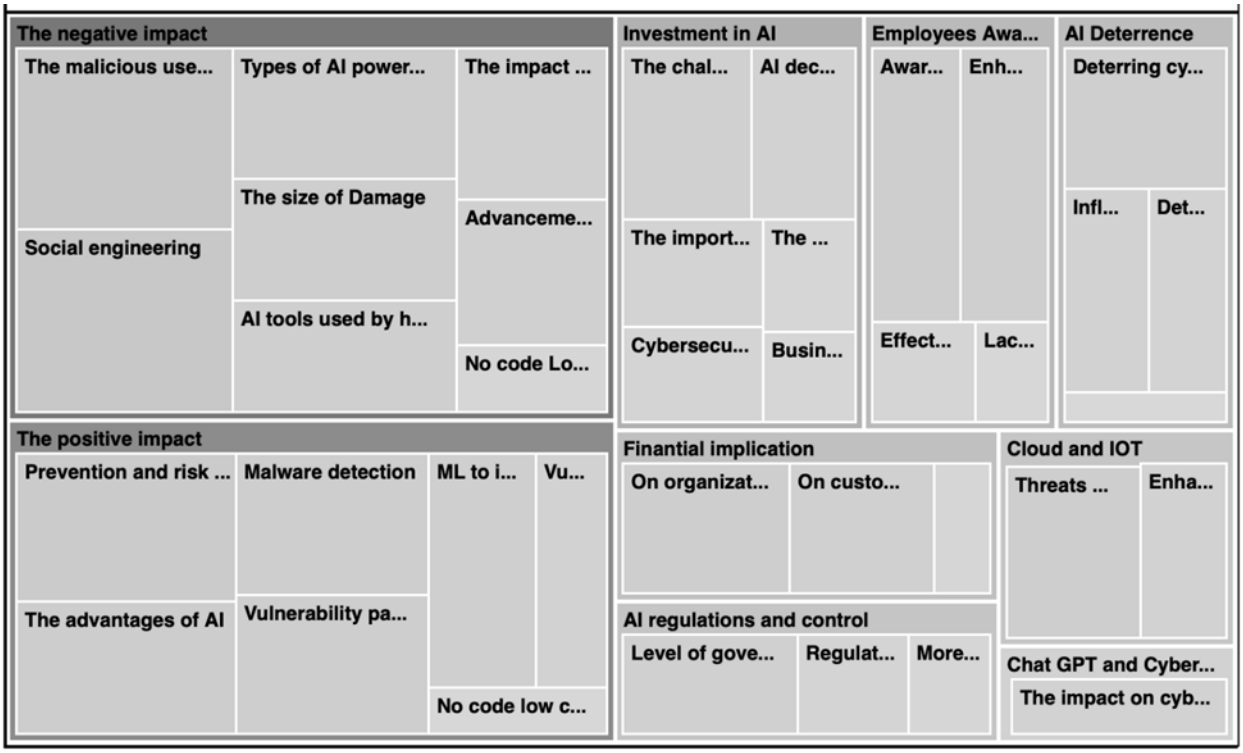
Representation and Visualization of the Data

Data representation and visualization offer researchers powerful tools to communicate findings, identify patterns, and gain insights from complex datasets. Effective representation and visualization are critical not only for comprehending information but also for conveying it to diverse audiences. One fundamental aspect of data representation is the selection of appropriate formats and structures to capture the inherent characteristics of the data. The researcher chose methods that accurately and faithfully depict the underlying information. Visualization, on the other hand, went beyond mere representation by translating data into visual elements such as charts, graphs, and diagrams. It offers a means to grasp complex relationships, trends, and anomalies that may be obscured in raw data. The researcher incorporated NVivo into the research process to enhance the quality of data representation and visualization by streamlining data management, coding, and analysis. Data visualization in this research included bar charts, hierarchy charts, graphs, tables, and diagrams based on the insights derived from the research data. Bar charts included the subthemes emerged from each theme based on interviews outcomes and participants responses. These visualizations not only aid in presenting findings to a wider audience

but also offer a deeper understanding of the research results. Data representation and visualization in this research serves to enhance the accessibility of research. They enable the researcher to convey the findings to a broader audience, fostering comprehension among non-specialists and stakeholders. It is imperative in ensuring the transparency and reproducibility of research findings. Well-designed visuals not only improve the clarity of data but also help in maintaining rigor in the research process. Figure 23 is a tree map of the emerging themes and subthemes. It shows the nine themes emerged from data analysis that was conducted using NVIVO qualitative data analysis tool.

Figure 23

Tree map of the emerging themes and subthemes.



Tufte (2001) advocated for the principle of data-ink ratio, suggesting that good visualization should maximize data ink while minimizing non-essential ink. He argues that less ink dedicated to embellishments results in a clearer communication of information. While Ware (2008) expounded on the concept of data visualization as a means of leveraging human visual perception for data

analysis, stressing the importance of encoding data using visual variables like color, size, and position. Data representation and visualization are indispensable tools in modern research. They enable researchers to effectively communicate their findings, uncover hidden insights, and maintain transparency in their work. By adhering to the principles outlined in the peer-reviewed literature, researchers can harness the full potential of data representation and visualization in advancing scientific knowledge.

Relationship of the Findings

The results of this study, stemmed from answers to the interview questions and data gathering, align closely with the central aspects of the research proposal, especially the aspects discussed in Section 1 of the dissertation. Nearly all the concepts presented in the peer-reviewed articles referenced, previous dissertations, and the information outlined in Section 1 of this research project corresponded with the findings obtained through data collection and interviews. These findings exhibited strong correlations with the research questions that addressed the research problem, the conceptual framework that include the two concepts and one theory along with the research actors and constructs, the expected themes, the literature that referenced peer-reviewed articles, and the research problem.

Research Questions. The researcher crafted specific research questions in the initial research process in Section 1, the questions is designed to address the research problem and contribute to generate good findings through data collection. The research findings provided comprehensive insights into the complex interplay between AI, cybersecurity, and cybercrime, addressing the research questions with real-world examples and diverse perspectives. They highlighted both the opportunities and challenges that AI presents in the context of cybersecurity, making it clear that organizations and cybersecurity professionals must adapt to this evolving

technology to protect sensitive information and systems effectively. The research findings are highly relevant to the research questions, providing valuable insights into the complex relationship between AI, cybersecurity, and cybercrime. Below is a breakdown of how these findings relate to each of the research questions:

Research question one is “How does the growth of AI contribute to the increase of cyberattacks and data breaches against organizations?” The findings illustrated that the growth of AI has indeed contributed to an increase in cyberattacks. AI enables automated attacks, personalized phishing, rapid password cracking, and other sophisticated tactics. It allows cybercriminals to conduct more extensive and rapid damage compared to traditional methods. The consensus among participants is that automated cyber-attacks are a significant threat due to their scale, efficiency, and adaptability. Sub question one is “what are the negative effects of AI on Cybersecurity?” The negative effects of AI on cybersecurity are well-documented in the findings. While AI has the potential to enhance cybersecurity, it also poses challenges. Hackers leverage AI tools such as Chat GPT, Pin Schema, Domo, and Google BARD for malicious activities. Additionally, AI enables social engineering attacks and deep fakes, making it harder to detect and prevent cyber threats. The findings emphasized the ongoing challenges in safeguarding sensitive information and systems as AI continues to evolve. Sub question two and three are “what are some AI and ML tools Cybercriminals use to conduct Cyber-attacks?” and “how do hackers take advantage of AI to conduct cybercrime-related activities?” The findings explicitly addressed these questions by listing AI and ML tools used by cybercriminals, including specific examples. They highlighted how hackers exploit AI for various purposes, from generating malicious code to conducting social engineering attacks. The findings also stressed the importance of adapting security measures to counter evolving AI-driven tactics.

Research question two and sub question one is “how does AI contribute to enhancing cybersecurity within organizations? What are the positive effects of AI on cybersecurity?” The findings highlighted the positive contributions of AI to cybersecurity. AI improves response times, automates tasks, enhances threat detection, and streamlines processes. It empowers cybersecurity professionals to protect systems and data more effectively, leading to faster threat detection, mitigation, and fraud prevention. The consensus is that AI can significantly enhance cybersecurity measures if implemented carefully. Sub question two is “what are some AI and ML tools organizations use to detect and counter cyber-attacks?” The findings mentioned that organizations are increasingly leveraging ML algorithms and AI to improve cybersecurity. These technologies are used for modeling attack patterns, automating responses, monitoring network behavior, and enhancing overall security measures. Collaboration and partnerships are also crucial in strengthening cybersecurity posture. Sub question three is “what can leaders do to avoid cyberattacks and secure their networks from data breaches and malicious activities?” The findings provided guidance for leaders by emphasizing the importance of staying informed, proactive planning, investing in technology, and educating employees. They stressed the need for strong access controls, disaster recovery preparedness, and recognizing AI and ML's potential in enhancing cybersecurity.

Research question three is “how important is it for the high-tech industry in the United States to invest more in AI?” The findings confirmed the necessity for the high-tech industry in the United States to invest in AI-driven cybersecurity. They emphasized the potential financial rewards, improved decision-making, and effective defense against cyber threats that AI offers. However, they also acknowledged the challenges and need for addressing legislative lag and counter AI. Sub question one is “What are the challenges for businesses to build a reliable security

system that cannot be compromised by hackers?" The findings explored various challenges businesses face in building reliable security systems. They highlighted technical, financial, educational, and cultural challenges that organizations must adapt to in the ever-changing threat nature.

Research Question four and sub question one are "what are the financial impacts that organizations face as a result of cybersecurity threats? "what are the financial implications of cyber-attacks and data breaches on customers?" The findings discussed the substantial financial impacts of cyber-attacks and data breaches on organizations and customers. These impacts include operational disruptions, legal penalties, reputational damage, and individual financial losses. They emphasized the importance of investing in cybersecurity measures to mitigate these risks.

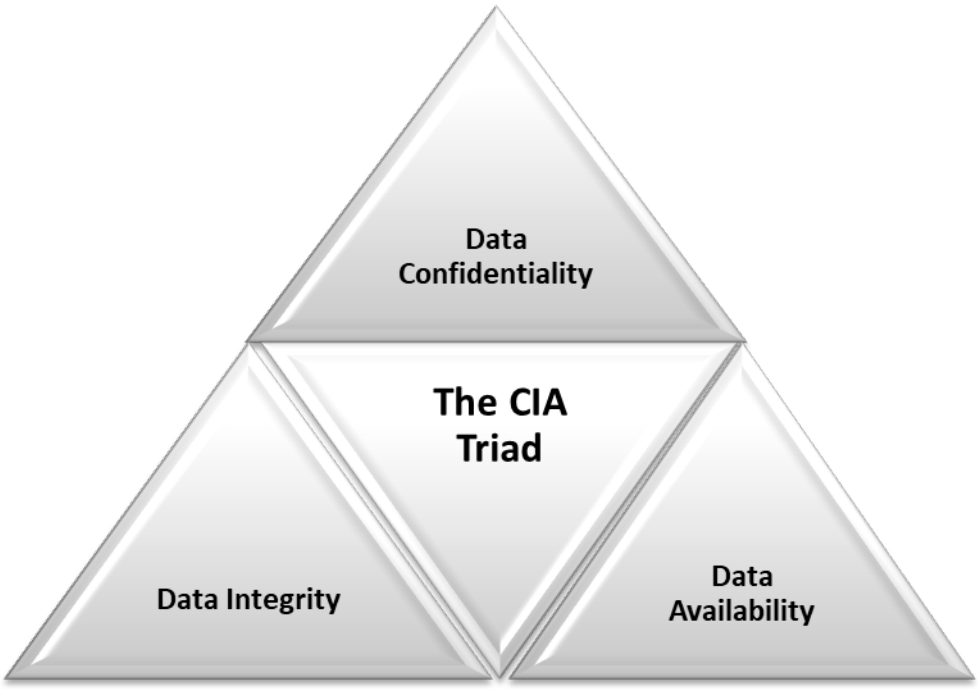
Conceptual Framework.

The CIA Triad Concept. The findings discussed in the research are closely related to the CIA Triad Concept. They highlighted the importance of maintaining confidentiality, integrity, and availability of data and systems to address evolving cyber threats in a disciplined and determined manner. When it comes to confidentiality, the findings highlighted how AI and ML are used by cybercriminals for various purposes, including data breaches and social engineering campaigns. These activities compromise the confidentiality of sensitive information held by individuals and organizations. For instance, the findings mentioned the effectiveness of AI in creating convincing fake content, which can deceive individuals and lead to data breaches. In terms of integrity, automated cyber-attacks, as discussed in the findings, can manipulate data and system configurations. Techniques such as DNS poisoning and polymorphic malware can compromise the integrity of data and systems, making them unreliable and potentially leading to incorrect decisions based on compromised information. Lastly the effect on availability, AI-powered attacks, as

emphasized in the research, have the potential to disrupt operations significantly. The scale and efficiency of these attacks can lead to downtime, affecting the availability of critical systems and services. Organizations must invest in cybersecurity measures to ensure the availability of their systems and data. Figure 24 illustrates the CIA triad.

Figure 24

The CIA Triad.



The Nine D's Concept. The research findings align with the Nine D's of Cybersecurity by emphasizing the importance of taking proactive measures to deter, detect, drive up difficulty, differentiate protections, dig beneath threats, diffuse protection, distract attackers, divert attackers, and create depth in defense strategies to address the automated cyber-attacks, the following is a detailed discussion of how the research findings related to the Nine D's concept:

The findings discussed the need for organizations to stay vigilant and adapt their defenses to counter evolving cyber threats. This relates to the concept of deterrence, where proactive measures are taken to discourage cybercriminals from attempting attacks. AI and ML technologies

are increasingly employed for threat detection, as mentioned in the findings. They enhance the speed and accuracy of identifying cyber threats, aligning with the detection aspect of the Nine D's of cybersecurity. AI related cyber-attacks, as discussed in the research findings, can manipulate data and system configurations. Implementing complicated security measures and defenses can drive up the difficulty for cybercriminals by making it harder for them to compromise data and systems.

The participants mentioned various AI and ML tools used by cybercriminals, including Chat GPT and Google BARD. Differentiating protections involves tailoring cybersecurity measures to address specific threats and vulnerabilities. The findings about AI's role in cybersecurity demonstrated the importance of going beyond surface-level defenses and delving into the intricacies of cyber threats. This aligns with the concept of digging beneath the threat to understand its underlying mechanisms. The emphasis on employee awareness, compliance, and training in the findings reflected the need to diffuse protection measures throughout an organization. Creating a security-conscious culture and promoting cybersecurity education are key elements of this approach.

The data collected from the research participants about cyber threats and attacks highlighted the importance of diverting attackers' attention and distracting them with decoy systems or data. This diversion tactic can buy valuable time for organizations to respond effectively. The findings emphasized the need for organizations to adapt their defenses and collaborate to enhance their defense mechanisms. This collaboration can divert attackers to other, less secure targets. The discussions about the financial impact of cyber-attacks and the responsibility of decision-makers confirmed the importance of creating a multi-layered, deep defense strategy to address cybersecurity challenges effectively. Participant 3 stated,

> We always had perimeter security and we had defense in depth, we're blocking you from coming in period versus we want you to do something so we can see it happen, then we can close it down within a microsecond.

The Cyber Deterrence Theory. The findings shed light on the complex relationship between AI and ML-driven cyber threats and the deterrence theory in the context of cybersecurity. The findings highlighted that AI and ML enable automated cyber-attacks with significant potential for rapid and extensive damage. In the context of deterrence theory, this ensures the importance of a strong defense. Organizations must invest in robust cybersecurity measures to make attacks exceedingly difficult. This aligns with the first essential factor of deterrence theory, where a formidable defense acts as a deterrent by raising the cost and risk for potential attackers. The concept of retaliation in deterrence theory is critical. The findings emphasized that the financial impact of cyber-attacks can be substantial. This aligns with the second essential factor of deterrence theory, where the threat of severe retribution acts as a deterrent. The potential for legal penalties and sever punishments serve as a consequence that should outweigh the benefits of cybercriminal activities.

The findings emphasized that deterring cyber-attacks is generally more cost-effective than reacting to them after they occur. This aligns with the core principle of deterrence theory, which seeks to make attacks costly. Organizations investing in robust cybersecurity defenses can potentially deter attackers by raising the difficulty associated with breaching their systems. The findings highlighted the significance of well-trained security teams and ongoing education efforts. These proactive measures align with the first objective of deterrence theory, which emphasizes a strong defense. A well-prepared security team can make cyber-attacks exceedingly difficult, serving as a deterrent to potential aggressors. The emphasis on investing in technology to prevent

AI-related cyber-attacks resonates with the concept of a strong defense in deterrence theory. Implementing cutting-edge security technologies can bolster an organization's cybersecurity posture and discourage attackers who seek easy targets. The critical role of employee awareness and compliance in bolstering cybersecurity aligns with the second objective of deterrence theory: the threat of retaliation. If employees are vigilant and aware, they can contribute to identifying and reporting potential threats, which in turn can lead to retaliation against malicious actors.

The participants discussed the complex nature of governance and regulation in the AI and cybersecurity domains. This is relevant to the broader context of deterrence theory, where governments and regulatory bodies play a role in defining and enforcing consequences for cyber-attacks. Effective regulation can contribute to the overall deterrence strategy. The participants recommended employing a multi-layered defense strategy and having robust response plans. This aligns with deterrence theory's emphasis on both defense and retaliation. A well-prepared response strategy can act as a deterrent by making potential aggressors think twice about the consequences of their actions. Some participants acknowledged the inevitability of cyber-attacks and advocated for robust response strategies. This perspective supports the understanding in deterrence theory that not all attacks can be prevented, but the threat of retaliation can still serve as a deterrent. The findings resonate strongly with deterrence theory's principles of creating a strong defense and the threat of retaliation to deter cyber-attacks. The strategies and practices outlined in the findings are essential components of a comprehensive cyber deterrence approach, especially in the context of AI-related cybersecurity threats. Organizations must continue to adapt and evolve their cybersecurity strategies to stay ahead of the future threats, ultimately working toward the goal of deterring potential cyber adversaries.

Anticipated Themes. The findings provided offer valuable insights into the relationship

between AI and cybersecurity, highlighting both the potential benefits and risks associated with the integration of AI and ML in securing IT infrastructure. Several key themes emerged from the findings, which align with the anticipated themes outlined in the research. The participants emphasize that AI and ML have empowered cybercriminals with advanced tools for conducting malicious activities. This aligns with the anticipated theme of the potential risks and challenges posed by the misuse of AI in cybersecurity. The research participants unanimously agreed that automated cyber-attacks are more extensive and rapid compared to traditional cyber-attacks. This corresponds with the expected theme of the growing attack surface due to the increasing sophistication and automation of cyber threats. The participants mentioned specific AI and ML tools used by cybercriminals, highlighting their potential to automate and enhance the effectiveness of attacks. This resonates with the idea that malicious AI can have a significant impact on organizations' infrastructure and security strategies. The participants also recognized the advantages of AI and ML in cybersecurity, including improved response times, enhanced threat detection, and streamlined processes, which mirrored the anticipated theme of technology organizations investing in AI-based technology to enhance IT infrastructure security. The findings emphasized that AI and ML play a pivotal role in malware detection and prevention efforts, participants shared some names of tools used for this purpose. The detection part was anticipated as one of the themes of technology organizations incorporating AI tools and ML models to enhance malware detection. The participants recognized the use of AI models to predict, detect, and respond to potential cyber-attacks, illustrating the theme of leveraging AI to counteract AI-driven threats. The anticipated theme of the continuous growth of attack surface within the large organizations was validated in the findings by highlighting that as organizations grow, they accumulate more data assets, which in turn enlarges their attack surface. Participants stressed the importance of effective

strategies to reduce this attack surface and minimize vulnerabilities.

The research findings corroborated the anticipated themes, highlighting the complex and dynamic nature of the relationship between AI and cybersecurity. While AI offers significant advantages in enhancing security measures, it also introduces new challenges that organizations must address. The consensus among participants confirmed the need for proactive measures, continuous education, and strategic investments in cybersecurity to effectively navigate this evolving issue. The findings largely align with the anticipated themes, providing validation of the text's expectations. However, there are also differences, unanticipated themes, and missing themes that enrich the understanding of AI's role in cybersecurity and highlight the evolving nature of this complex field. The differences between the themes discovered in the findings and the anticipated themes is addressed in this study. While the findings emphasized AI's role in malware detection, the original text anticipated a broader theme of AI's use in overall cybersecurity. The findings focus more on detection and less on prevention.

The missing theme discovered in this study is the findings did not extensively cover the theme of using AI for mitigation of cyber threats. The anticipated themes mentioned the importance of AI in automating responses, but this is not a prominent aspect of the findings. The second missing theme is the findings did not delve deeply into ethical considerations related to AI in cybersecurity. The anticipated themes anticipated potential ethical challenges; these challenges were not the main focus of the findings. There are few unanticipated Themes, the first one is the findings introduce a theme of collaboration and partnerships in strengthening cybersecurity posture. While the anticipated themes did not explicitly mention this, it emerges as a valuable aspect in the findings. The second unanticipated theme is, the findings touch on the financial impact of automated cyber-attacks and data breaches, providing insights into the costs associated

with cyber incidents. This theme was not explicitly anticipated in the anticipated themes. the last unanticipated theme is, the findings mentioned the role of AI in governance and regulation, particularly in open-source AI tools. While not anticipated in section 1, this theme highlights the evolving nature of AI governance.

The Literature. The findings addressed various aspects of the relationship between AI and cybersecurity. They encompassed both the negative implications and advantages of AI and ML technologies in the context of cybersecurity. These findings are closely related to the literature review, which serves as a foundational understanding of this relationship. The researcher explored the key connections, similarities, and differences. While the literature review identified specific cyber-attacks to include man in the middle, DDOS, and Zero day attacks, the findings highlighted several negative implications which showed that both the findings and the literature review emphasized the growing threat posed by AI and ML-powered cyber-attacks. These technologies empower cybercriminals to execute automated attacks, sophisticated phishing scams, rapid password cracking, and personalized social engineering campaigns. The findings mentioned the dark web's involvement in developing unregulated AI models, intensifying the threat landscape. This aligns with the literature's focus on the malicious use of AI by adversaries. Both the literature and the findings agreed that automated cyber-attacks have the potential to cause more extensive and rapid damage compared to traditional cyber-attacks. The efficiency and adaptability of these attacks pose significant threats. The findings dove deep into the technical aspects of AI-powered cyber-attacks, such as DNS poisoning, MAC address table manipulation, and polymorphic malware. These details complement the literature review's exploration of AI's role in cybersecurity. The literature's discussed some AI tools employed by adversaries that are aligned with specific AI and ML tools identified in the findings, including Chat GPT, Pin Schema, Domo, and Google

BARD, used by cybercriminals.

The findings and literature review highlighted how AI and ML streamline cybersecurity processes, improving efficiency, and enabling proactive threat detection. They agreed that AI and ML technologies enhance threat detection capabilities. They automate responses, monitor network behavior, and model attack patterns, contributing to faster threat detection. The findings mention that behavior-based detection is increasingly important in modern cybersecurity strategies. This aligns with the literature's emphasis on AI's role in modeling attack patterns. The finding complements the literature's focus on AI's role in cybersecurity by acknowledging the role of AI in vulnerability patching. It can automate repetitive tasks, prioritize critical vulnerabilities, and enhance proactive threat detection. While the literature review suggested ongoing exploration of AI's potential to predict vulnerabilities, the findings highlighted varying opinions among participants. This indicated the dynamic nature of this area of research and development.

The literature addressed employees awareness and compliance as a business practice and included several peer reviewed sources to support the importance of employees awareness in avoiding AI- powered cyber-attacks, the literature also emphasized that employees are the first line of defense and that the human is the weakest link in cybersecurity. The findings recognized the critical role of employee awareness and compliance in bolstering cybersecurity. It emphasized the importance of regular training and vigilance among employees, aligning with the literature's focus on education and awareness. The findings discussed decision-making in AI technology investments and cybersecurity to support the research actors and constructs in the literature review and its emphasis on advising technology organizations regarding AI investments. They explored various roles and functions of stakeholders like CIOs, CISOs, CEOs, and board members. Financial implications on organizations and customers are important part of the research literature, the

researcher emphasized on the financial impact of automated cyber-attacks on organizations' operations and strategy, as well as the impact on customers and their trust in the service provided by organizations. The findings addressed the substantial financial impacts of cyber-attacks, including operational disruptions, legal penalties, and reputational damage. This aligns with the literature's mention of financial risks associated with AI and ML cyber threats.

The governance and control of AI technology was part of the literature review focus. The findings addressed the governance and regulation of open-source AI tools through different interview questions, reflecting the evolving nature of AI governance and the necessity of AI's responsible use. While the literature review addressed No Code/Low Code platforms and the adoption of AI in the cloud computing as well as the threats, and vulnerabilities in Internet of Things, the findings highlighted concerns about security and privacy risks associated with IoT devices, suggesting that AI and ML could play a role in addressing these challenges. This complements the literature's focus on AI's role in safeguarding sensitive information and systems in and out of the cloud. The findings align with the literature review by emphasizing the negative implications and advantages of AI and ML in cybersecurity. The interviews revealed valuable information about technical details, tools used, and specific challenges, providing a more granular perspective on AI's role in cyber threats and defense. The literature along with the findings both touched on the evolving nature of contemporary cyber threats, where AI plays a significant role, and the importance of continuous adaptation and vigilance in cybersecurity practices.

The Problem. The research findings shed light on the complex relationship between AI, ML, and cybersecurity. The problem being studied revolves around the nature of AI and ML in cybersecurity – on one hand, these technologies offer significant advantages for defending against cyber threats, but on the other hand, they pose substantial risks when leveraged by cybercriminals.

The findings presented in the responses provide a comprehensive overview of the intricate relationship between AI, ML, and cybersecurity. They addressed the challenges and opportunities that technology organizations in the United States face in addressing the dual nature of AI in the context of cybersecurity. These findings highlighted the urgent need for proactive measures and responsible AI use to mitigate the risks posed by malicious AI-driven cyber-attacks and protect critical sectors in the United States.

The research focused on the disadvantages of AI on cybersecurity and addressed the research problem by navigating into the negative implications of AI and ML on cybersecurity. Participants discussed how these technologies have empowered cybercriminals with potent tools for conducting malicious activities. Automated attacks, phishing scams, rapid password cracking, and personalized social engineering campaigns are mentioned as examples. This emphasizes the growing threat where AI and ML facilitate the creation and execution of cyber-attacks. Additionally, the involvement of the dark web in developing unregulated AI models amplifies these threats. The findings directly relate to the problem being studied. They emphasized that AI and ML are not only tools for defenders but also weapons in the hands of attackers. This dual nature of AI and ML intensifies the challenges faced by technology organizations in the United States, especially those providing critical services, as they need to be prepared to counteract these malicious AI-driven cyber-attacks.

To have a complete understanding of the problem under study, the researcher explored the advantages of AI and ML in cybersecurity. Participants pointed out that these technologies can significantly enhance response times, automate tasks, improve threat detection, and streamline processes for cybersecurity professionals. They also mentioned that AI and ML can model attack patterns, automate responses, monitor network behavior, and contribute to faster threat detection

and mitigation. The findings illustrated that AI and ML are indispensable for organizations in their efforts to strengthen cybersecurity defenses. However, they also emphasized the importance of responsible and careful implementation, as well as collaboration and continuous improvement in algorithms. The findings also identified the means in whish cybercriminal conduct AI-powered attacks using specific AI and ML tools, including Chat GPT, Pin Schema, Domo, and Google BARD. These tools are used for various purposes, from generating malicious code to social engineering attacks. The participants stressed that these tools could automate and enhance the effectiveness of cybercriminal activities. The information provided by research participants is crucial as it highlighted the real-world application of AI and ML by malicious actors. Technology organizations need to be aware of the tools and techniques used by cybercriminals to develop effective countermeasures.

Another aspect highlighted in the findings is the increase in data breaches in the United States due to AI-driven cyber-attacks. It indicated the ongoing challenges faced by cybersecurity professionals in safeguarding sensitive information and systems. As AI continues to evolve, organizations must remain vigilant and adapt their security measures. The research findings directly relate to the problem at hand, as they emphasized the urgent need for technology organizations to address the growing risk of data breaches and vulnerabilities caused by malicious AI and ML applications. The findings also touched upon the varying opinions regarding the vulnerability of no-code and low-code applications to cyber-attacks. While some expressed concerns due to limited security measures and reliance on AI, others see them as secure depending on third-party providers. This highlights the complexity of evaluating the security of emerging technologies and the need for careful consideration. On the other hand, it explored how these applications offer improved accessibility, faster development, and reduced coding effort, which can

be valuable for technology organizations. The research concluded that it is important to assess the security of new technologies, including AI-driven applications, which is directly relevant to technology organizations providing critical services.

The findings discussed the role of AI and ML in malware detection, prevention, and vulnerability patching. ML techniques are highlighted as crucial for analyzing and responding to threats, especially in the face of rapidly evolving malware. Participants emphasized the importance of keeping systems updated and employing the latest ML technologies. The findings offered insights into how technology organizations can utilize AI and ML to stay ahead of cyber threats, a crucial aspect of the problem being studied. The findings also touched upon AI's potential to predict vulnerabilities in computer systems. While recognizing AI's capabilities in detecting anomalies and changes in system configurations, there is consensus that human intelligence and careful implementation are crucial in cybersecurity. The research highlighted the ongoing exploration of AI's role in predicting vulnerabilities and the potential benefits and challenges associated with it.

The findings consistently emphasized the critical role of employee awareness, compliance, and training in bolstering cybersecurity. Regular training, testing, and accountability are seen as essential components of creating a security-conscious culture. The need to adapt training programs to address evolving threats is also stressed to defend against AI-driven cyber threats. The findings also touched upon the governance and regulation of open-source AI-based tools. Participants recognized the need for increased governance while balancing innovation, freedom, and security in the rapidly advancing field of AI. They emphasized the importance of responsible AI use and oversight, which is relevant to the problem of malicious AI in cybersecurity. Lastly, the exploration of the research problem led to the fact that the rapid progress of AI and ML technologies has

garnered significant attention from information technology experts and the U.S. government. These technologies have the potential to revolutionize various industries, including cybersecurity.

Summary of the Findings

The research findings emphasized the growing impact of AI and ML on cybersecurity, both in terms of threats and advantages. On the negative side, the findings concluded that it is evident that cybercriminals increasingly exploit AI and ML to conduct malicious activities. The dark web's involvement in unregulated AI models intensifies the threat on cyberspace. Automated cyber-attacks, in particular, are viewed as highly damaging due to their scale and efficiency. On the positive side, AI and ML offer significant benefits to cybersecurity. They improve response times, automate tasks, enhance threat detection, and streamline processes. ML techniques are vital in malware detection and prevention, while AI has the potential to significantly improve vulnerability patching. However, the findings emphasized that careful integration and human oversight are required to ensure effectiveness. The financial impact of automated cyber-attacks and data breaches is substantial, with costs ranging from operational disruptions to reputational damage. Organizations are encouraged to invest in cybersecurity measures to minimize these risks. Employee awareness and compliance are essential for bolstering cybersecurity. Regular training, testing, and accountability are crucial in creating a security-conscious culture. Regulating open-source AI-based tools remains a challenge, with the need for governance and responsible AI use. The importance of education, awareness, and training in deterring cyber-attacks is widely recognized, along with multi-layered defense strategies, system updates, and network monitoring. In the context of cloud and IoT, AI and ML can enhance security, but vigilance and cooperation with human intelligence are necessary. The findings revealed that the security and privacy risks associated with IoT devices are a growing concern, with the need for manufacturers to be

accountable for device security.

Application to Professional Practice

The results of this qualitative multiple case study on the dark side of AI in cybersecurity and strategies for mitigation have the potential to significantly improve general business practices across a wide range of industries. As AI and ML continue to play a critical role in business, understanding the implications of AI in cybersecurity and adopting the recommended strategies can enhance overall business resilience, security, and decision-making. The results of this study offer valuable insights into the evolving technology of AI and cybersecurity. These insights can be applied across general business practice to enhance cybersecurity measures, decision-making, employee awareness, and collaboration. By proactively addressing the challenges and opportunities presented by AI in cybersecurity, businesses can better protect their operations and financial well-being in an increasingly digitized world.

Improving General Business Practice

The study highlighted the growing threat of AI-powered cyber-attacks and the need for robust cybersecurity practices. General business practice can greatly benefit from implementing these enhanced cybersecurity measures, such as leveraging AI and ML for threat detection, investing in AI and ML tools and software, and prioritizing employee awareness and compliance. By doing so, organizations can better protect their data, operations, and reputation, reducing the risk of financial losses due to cyber incidents.

The study focused on the necessity of investing in AI and ML technologies for both cybersecurity and business operations. General business practice can learn from this and strategically invest in AI to improve decision-making, optimize operations, and remain competitive. Organizations that embrace AI will likely have an advantage in terms of efficiency

and effectiveness, ultimately leading to better financial outcomes (Gudigantala et al., 2023). The research findings point out the substantial financial risks associated with automated cyber-attacks. These insights can be applied to business practice for businesses to assess their own financial vulnerability to cyber threats and invest in the necessary cybersecurity measures to mitigate such risks (Dearden et al., 2023). A proactive approach to cybersecurity can prevent operational disruptions, legal penalties, and reputational damage. The study addressed the nature of decision-making in AI technology investments and cybersecurity. Business can learn from this by promoting a culture of adaptive decision-making. This involves staying informed about emerging threats, collaborating with decision-makers across different departments, and remaining adaptable to evolving risks and technological solutions.

Employee awareness and compliance is one of the most important business practices addressed in this research and findings. The findings highlighted the importance of employee training and awareness in preventing cybersecurity incidents. This business practice can improve employee cybersecurity education and training, ensuring that staff is equipped to recognize and respond to emerging threats. A well-informed and vigilant workforce is a critical line of defense against cyber-attacks (Miranda, 2018). The research findings raised the need for stronger governance and regulations in the context of AI use. The results advocate for responsible AI use and proactively engage with policymakers to ensure that AI technologies are developed and deployed in a manner that prioritizes security and ethical considerations. This can improve the general business practices and help create a safer and more predictable environment for AI adoption. The study emphasized the significance of collaboration and partnerships in strengthening cybersecurity. General business practice can explore collaboration with cybersecurity experts, AI technology providers, and other organizations to enhance their collective defense against cyber

threats. Collaboration can lead to shared threat intelligence and more robust cybersecurity measures (Amanowicz, 2021).

With the growing concerns around IoT device security, general business practice can adopt a proactive approach by implementing security-conscious cultures and strategies for securing IoT devices. Integrating AI and ML solutions to monitor and protect IoT networks can be a beneficial approach for many industries (Xu et al., 2020). The ever-evolving nature of AI and cybersecurity requires businesses to adopt a culture of continuous learning and adaptation. Organizations must adapt good business practices by implementing mechanisms to stay updated about the latest cybersecurity threats, AI developments, and regulatory changes. Continuous learning is essential for remaining at the forefront of cybersecurity (Kam et al., 2020). The study emphasized the importance of building resilience in the face of evolving cyber threats. This can be applied to businesses by adopting a proactive and adaptive approach to cybersecurity, ensuring that they have strategies and resources in place to respond effectively to any cyber incident.

Potential Application Strategies

Leveraging the findings of the study on the malicious side of AI in cybersecurity and strategies for mitigation requires organizations to adopt proactive application strategies. These strategies can help businesses implement the study's recommendations effectively, improve their cybersecurity posture, and remain competitive in the evolving nature of AI-powered threats. Organizations can apply the study's findings by incorporating AI-driven cybersecurity solutions into their existing infrastructure. These solutions include AI-based threat detection systems, anomaly detection tools, and ML algorithms (Zhang et al., 2022). By automating the identification and mitigation of cyber threats, businesses can enhance their overall security measures.

The study emphasized the significance of employee training and awareness. Organizations

can apply this finding by investing in continuous training programs that keep employees informed about emerging cyber threats and best practices. Regular cybersecurity awareness training helps employees recognize and respond to potential threats, reducing the risk of successful cyber-attacks (Sasse et al., 2001). To mitigate the risk of unauthorized access to sensitive data and systems, organizations can implement MFA. This strategy is in line with the study's recommendations for strong access controls. MFA adds an extra layer of security by requiring users to provide multiple forms of identification, making it more challenging for cybercriminals to breach accounts. Organizations should actively monitor and stay informed about AI-related cyber threats, which is a key recommendation from the study. This includes subscribing to threat intelligence feeds, participating in industry-specific cybersecurity forums, and collaborating with cybersecurity experts. By doing so, businesses can proactively identify emerging threats and adapt their defenses accordingly. Building on the study's emphasis on collaboration and partnerships, organizations can form collaborative alliances with peers, industry associations, and government agencies to share threat intelligence. Collaborative threat sharing can enhance the collective ability to detect and respond to cyber threats more effectively. Given the growing concerns around IoT device security, organizations can apply the study's findings by adopting AI-driven solutions for securing IoT networks. AI can be used to monitor and protect IoT devices, identify abnormal behavior, and respond to potential threats in real time.

In light of the study's focus on resilience in the face of threats, organizations should develop robust incident response plans. These plans should outline the steps to take when a cyber incident occurs, including communication strategies, containment measures, and recovery processes. Having a well-defined incident response plan can help organizations minimize the impact of cyber-attacks (Garcia-Perez et al., 2023). The nature of decision-making in AI technology investments

and cybersecurity, as discussed in the study, can be addressed by applying strategic decision-making processes. Organizations can establish cybersecurity governance frameworks, involving various stakeholders, to ensure that decisions related to AI technology investments are aligned with cybersecurity priorities. Organizations can leverage the findings to invest in AI-driven solutions that enhance data privacy and compliance. AI can assist in data encryption, access control, and monitoring to ensure that organizations comply with data protection regulations, such as GDPR and HIPAA. To address the recommendation of patch management to reduce the attack surface, organizations should establish a proactive patch management process. Regularly updating software, systems, and security patches is crucial for mitigating vulnerabilities that cybercriminals may exploit. The study highlights the importance of responsible AI use and oversight. Organizations can apply this finding by promoting ethical AI practices within their AI development and deployment processes. This includes conducting ethical impact assessments, ensuring transparency, and adhering to responsible AI guidelines. Businesses can actively engage with policymakers and industry groups to advocate for stronger governance and regulations in AI use. By participating in the development of regulatory frameworks and best practices, organizations can help shape a secure and responsible AI ecosystem (Brundage et al., 2018). To enhance cybersecurity, organizations can apply AI-driven predictive analytics to anticipate and proactively address cyber threats. Predictive algorithms can analyze historical data and identify potential vulnerabilities, enabling businesses to strengthen their defenses before an attack occurs.

Summary

This qualitative study provided valuable insights into the complex relationship between AI and cybersecurity, emphasizing the need for organizations to strike a delicate balance between leveraging AI for defense and guarding against its exploitation for malicious purposes. As AI

continues to advance, the cybersecurity community must remain vigilant and adaptive, ensuring that they are always one step ahead of cybercriminals. It illuminated the dark side of AI in cybersecurity, highlighting the substantial threats posed by AI-powered cyber-attacks and the potential consequences for organizations. At the same time, it highlighted the advantages of AI and ML in enhancing cybersecurity and the critical role of these technologies in defending against evolving threats. Applying the findings of the study to improve cybersecurity practices and overall business resilience is essential in today's digital landscape. By adopting these application strategies, organizations can effectively navigate the evolving challenges and opportunities presented by AI in cybersecurity. These strategies not only enhance security measures but also promote responsible AI use and collaboration, contributing to a more secure and competitive business environment.

Recommendations for Further Study

The findings of this qualitative multiple case study have unveiled various aspects of AI's impact on cybersecurity. These areas for further study are justified by the research findings as they address specific aspects of AI in cybersecurity that were highlighted in the study. Investigating these areas can contribute to a deeper understanding of the impact of AI in cybersecurity, the development of effective countermeasures, and the ethical and regulatory considerations surrounding AI use in this field. Additionally, this research can help organizations make informed decisions about adopting AI-driven cybersecurity solutions and developing strategies to protect their digital assets. These findings suggest several areas for further study, as follows:

Regulations and Governance for AI in Cybersecurity

The research addressed the need for stronger regulations and governance in AI use. Further study could focus on the development of regulatory frameworks specific to AI in cybersecurity. Specifically implementing more control on open-source AI tools without compromising freedom of

access to the public, and the way regulatory frameworks can be designed to control open-source AI tools in cybersecurity while still ensuring public access and collaboration. Further research could also explore the ethical and legal implications of AI use in cybersecurity by addressing the specific ethical concerns related to the use of AI in cybersecurity, and how can they be addressed in regulatory frameworks, addressing the design of legal frameworks to provide clarity on liability and accountability in cases of AI-related cybersecurity incidents, and focusing on the potential unintended consequences of regulatory measures, and how can these be mitigated. The research emphasized the importance of responsible AI use. Further study could explore the development of guidelines and standards for responsible AI use in cybersecurity and how organizations can be incentivized to adopt and adhere to responsible AI practices in cybersecurity. Additional research could also explore mechanisms for ensuring AI ethics and accountability in cybersecurity practices.

AI-Powered Threat Detection and Response Algorithms

The research highlighted the importance of AI in threat detection. Additional research could investigate the effectiveness of different AI-powered threat detection algorithms and their ability to detect emerging threats in real-time. Further research also needed to address how AI can enhance incident response processes and explore the use of AI chatbots for immediate response, AI-driven forensic analysis, and automation in post-incident recovery. Additionally, it is necessary to examine the application of AI and ML in predictive cybersecurity analytics. Further research in this area will help organizations identify the most efficient algorithms for their specific cybersecurity needs and could investigate the accuracy of predictive models in identifying vulnerabilities and predicting cyber threats.

Human Factors in Cybersecurity

The study emphasized the role of employee awareness and compliance in cybersecurity.

Future research could further explore the human factors that contribute to cybersecurity effectiveness. This could include studying the impact of various training methods, the psychology of phishing attacks, studying methods to detect AI-driven cyber-attacks and developing countermeasures, the development of AI-driven cybersecurity training solutions, and the specific impact of AI language models in crafting and disseminating customized messages for social engineering attacks, as well as the evolution of AI-powered cyber threats. Further studies could explore the psychological aspects of phishing attacks, such as the factors that make individuals susceptible to phishing attempts, assess the effectiveness of AI-driven simulations and scenarios in enhancing employees' practical cybersecurity skills, and propose proactive measures and defensive strategies to stay ahead of emerging AI-driven cyber threats. By exploring these research areas, scholars and practitioners can contribute to a deeper understanding of the human and technological aspects of cybersecurity, leading to more effective strategies for securing organizational assets against evolving cyber threats.

AI in IoT Security

The findings acknowledged the security challenges associated with IoT devices. Future research could focus on AI-driven solutions for securing IoT networks, including the development of AI-based intrusion detection systems (IDS) specifically tailored for IoT environments, developing ML models for IoT device behavior analysis, and AI-enhanced IoT device management. It is necessary to conduct more study about different areas within the IoT security and take advantage of AI’s detection and monitoring capabilities. New studies could explore the utilization of ML algorithms to analyze network traffic and identify anomalous patterns that may indicate potential security threats, the use anomaly detection techniques to identify deviations from expected behavior, signaling potential security breaches. and the implementation of real-time

monitoring capabilities to detect and respond to security incidents promptly. This future study can contribute significantly to addressing the evolving security challenges associated with the proliferation of IoT devices, ensuring a more robust and resilient IoT ecosystem.

Reflections

Researching this problem has significantly contributed to both personal and professional growth, offering me valuable insights and opportunities for development in several ways. The research has been instrumental in my personal and professional growth by broadening my knowledge, enhancing my decision-making skills, promoting ethical AI use, and fostering a culture of continuous learning and collaboration. It has not only enriched my professional capabilities but also contributed to my personal awareness and engagement with the evolving landscape of AI in cybersecurity. These learnings are invaluable assets that will continue to shape my personal and professional growth in the years to come. The study expanded my knowledge and expertise in the field of cybersecurity and AI. By focusing on the intricacies of AI-driven cyber threats, I gained a deeper understanding of the evolving landscape of cybersecurity, including emerging risks, threat detection, and mitigation strategies. This knowledge has allowed me to become a more informed and effective professional in the field.

Personal & Professional Growth

The study's focus on decision-making in the context of AI technology investments and cybersecurity has enhanced my ability to make informed, strategic decisions. I have learned to consider a multifaceted approach to decision-making, involving various stakeholders and adapting to evolving risks and technology solutions. This skill is invaluable in both personal and professional contexts. The study's emphasis on employee awareness and compliance has encouraged me to advocate for cybersecurity awareness within my professional environment. I

have been able to contribute to the development of training programs and raise awareness among colleagues, fostering a culture of security-consciousness within my organization. The study's focus on responsible AI use and oversight has strengthened my commitment to promoting ethical AI practices. This extends beyond the professional sphere and has influenced my personal perspective on AI technology.

I am now more conscious of the ethical considerations and implications of AI in various contexts. The ever-evolving nature of AI and cybersecurity has instilled in me a culture of continuous learning and adaptation. This has not only enhanced my professional growth but also encouraged me to stay updated on technological advancements and emerging threats in my personal life. The study's emphasis on collaboration and threat intelligence sharing has facilitated networking opportunities with peers, experts, and organizations in the field. Interviewing IT professionals and experts in the cybersecurity field had expanded my professional network and allowed me to collaborate on various initiatives related to AI in cybersecurity. The knowledge and insights gained from the study have boosted my confidence in addressing cyber threats both personally and professionally. I feel more equipped to identify potential threats, respond to incidents, and contribute to the development of robust cybersecurity strategies.

Biblical Perspective

The exploration of business functions, particularly in the context of AI-driven cybersecurity and the study's findings, can be viewed through the lens of a Christian worldview. Christianity emphasizes principles of ethics, stewardship, responsibility, and love for one's neighbor. These principles align with and relate to the business functions explored in the study. The ethical use of AI in cybersecurity is a central concern in the study. A Christian worldview aligns with ethical business practices, emphasizing honesty, integrity, and respect for others. Scripture, such as

Ephesians 4:25, reinforces the importance of truthfulness: "Therefore each of you must put off falsehood and speak truthfully to your neighbor, for we are all members of one body." This verse highlights the Christian value of honesty in business operations, which includes the responsible and ethical use of AI technologies to protect data and networks.

The responsible stewardship of technology, including AI, is another key aspect of the study. A Christian worldview emphasizes the responsibility of individuals and organizations to use their resources wisely and for the greater good. The Parable of the Talents in Matthew 25:14-30 illustrates the concept of stewardship, where individuals are entrusted with resources and are expected to use them wisely. In the context of AI, businesses are entrusted with advanced technology, and they are called to use it responsibly to protect their assets and the data of their customers and partners. The research emphasized the importance of protecting sensitive information in the face of AI-driven threats. This aligns with the Christian principle of loving one's neighbor, which includes safeguarding the interests and well-being of others. Leviticus 19:18 states, "Love your neighbor as yourself." This commandment extends to business operations, where organizations have a responsibility to protect sensitive information, such as customer data, in a manner that reflects love and care for those they serve.

The study addressed the necessity of collaboration and partnership in cybersecurity. A Christian worldview encourages the idea of community and working together for the common good. Scripture, such as 1 Corinthians 12:12-27, illustrates the concept of the body of Christ, where each part has a role to play in harmony. Similarly, in the business context, organizations collaborate and partner with others to strengthen their cybersecurity defenses. This reflects the Christian value of working together for a common purpose. The nature of decision-making was indicated in the study, particularly in the context of AI technology investments and cybersecurity.

A Christian worldview emphasizes the need for wise and discerning decision-making. Proverbs 3:5-6 advises, "Trust in the Lord with all your heart and lean not on your own understanding; in all your ways submit to him, and he will make your paths straight." This verse highlights the importance of seeking guidance and making decisions with wisdom, which applies to the ethical and strategic decision-making in business. Keller and Alsdorf (2012) discussed responsible decision-making in the context of work. They acknowledged the importance of approaching decision-making with wisdom and discernment, considering the ethical implications of their choices. The authors emphasized the need for individuals to seek guidance, make decisions with integrity, and align their choices with Christian values (Keller & Alsdorf, 2012).

The research promoted a culture of continuous learning and adaptation in the face of evolving cybersecurity challenges. Continuous learning aligns with the Christian value of growth and transformation. Romans 12:2 encourages believers to be transformed by the renewal of their minds. Similarly, in the business context, organizations are called to adapt, learn, and grow in their cybersecurity practices to protect their assets and serve their stakeholders effectively. The study emphasizes the need for accountability and compliance with cybersecurity regulations. A Christian worldview values accountability and responsibility. In Galatians 6:5, it is written, "For each will have to bear his own load." This verse highlights the principle of individual responsibility. In business, organizations are accountable for complying with cybersecurity regulations and ensuring the security of their systems and data.

Summary of Reflections

In summary, engaging with the study on AI's dark side in cybersecurity significantly advanced my expertise, decision-making skills, and ethical awareness. It empowered me to enhance cybersecurity awareness at work, foster ethical AI practices, and build a robust

professional network. The study instilled a commitment to continuous learning, boosting my confidence in addressing cyber threats personally and professionally. Overall, it has shaped a well-rounded growth, enriching both my personal awareness and professional capabilities in the evolving realm of AI in cybersecurity. The business functions explored in this study can align with a Christian worldview through the application of ethical practices, responsible stewardship, the protection of sensitive information, collaboration and partnership, responsible decision-making, continuous learning and adaptation, and accountability and compliance. These principles are consistent with the teachings of Christianity, which emphasizes love, integrity, and the responsible use of resources for the greater good. The scriptures referenced illustrate the relationships between these business functions and the values inherent in a Christian worldview. By integrating these principles, businesses can not only enhance their cybersecurity but also align their operations with a Christian ethical framework.

Summary of Section 3

Section 3 is the last section of this qualitative multiple case study, in this section the researcher provided an overview of the study, that includes comprehensive details on the overall study. the researcher reported the research findings in the presentation of findings part of the section. The research findings are presented the discovered themes and sub themes that emerged from the participants responses to the interview questions. Each theme was interpreted and based of the data collected from participants during the data collection phase of the study. This section completed the first two sections and is related to them, it explored the relationship of the findings with the research questions, the problem and the conceptual framework that was addressed in Section 1, along with the relationship of the findings with the literature and the anticipated themes that was addressed in Section 2. This section identified the application to professional practices by

explaining how this research contributed to improve general business practices and the potential application strategies. It also suggested new areas for future study by providing four recommendations of future study topics related to the use of AI in the cybersecurity field. The researcher concluded this section with reflections on personal and professional growth and a discussion of the relationship between business functions addressed in this research and its integration with a Christian worldview by providing specific scripture references to support the integration.

Summary and Study Conclusion

The qualitative multiple case study explored the dark side of AI in cybersecurity, focusing on defensive tactics for organizations. It focused on the dual nature of AI in cyber threats and defenses, emphasizing the necessity of AI as a core component of cybersecurity strategies. The study aimed to identify harmful AI and ML applications in cyber-attacks while highlighting effective strategies for preventing and mitigating these risks. The research explored the evolving landscape of AI-powered cyber threats, where adversaries leverage AI for social engineering, developing mutating malware, and identifying network vulnerabilities. Simultaneously, organizations deploy AI in robust defense systems to detect and respond to cyber threats. The study's flexible design and qualitative approach, rooted in pragmatism, sought to explore the impact of AI on cybersecurity in technology organizations across the United States.

Key findings revealed the increasing use of AI by cybercriminals for automated attacks, posing substantial risks to organizations. The study emphasized the urgency for technology firms to counter malicious AI, advocating for the responsible use of AI to enhance cybersecurity. The research identified specific business practices, including improving employee cybersecurity awareness, utilizing ML algorithms, and adopting AI in cloud computing, as effective strategies for

mitigating AI-driven cyber threats. The literature review provided a baseline understanding of the relationship between AI and cybersecurity, emphasizing the need for increased investment in AI and ML solutions for IT infrastructure security. The conceptual framework incorporated key concepts such as the CIA Triad, Nine Ds of cybersecurity, and cyber deterrence theory.

The research findings showcase the role of AI and ML in cyber threats and defenses, addressing the potential financial, operational, and reputational risks associated with automated cyber-attacks. The study underscores the necessity for technology organizations to invest in AI technology to stay competitive and secure in an evolving technological landscape. Comprehensive discussion on how the study's results can improve general business practices emphasizes the importance of ethical AI use, responsible decision-making, employee awareness, and collaboration. Potential application strategies include implementing AI-powered threat detection algorithms, enhancing incident response with AI, and focusing on AI in predictive analytics. The study's significance for personal and professional growth lies in its contribution to knowledge, decision-making skills, and a heightened awareness of ethical AI use. Finally, the integration with a Christian worldview highlights the alignment of business functions with Christian principles such as ethical conduct, responsible stewardship, love for one's neighbor, collaboration, responsible decision-making, continuous learning, and accountability. The study provides a framework for businesses to navigate the challenges of AI in cybersecurity while adhering to Christian values.

References

Abdel-Basset, M., Manogaran, G., & Mohamed, M. (2018). Internet of Things (IoT) and its impact on supply chain: A framework for building smart, secure and efficient systems. *Future Generation Computer Systems*, *86*(9), 614–628. https://doi.org/10.1016/j.future.2018.04.051

Abdullahi, M., Baashar, Y., Alhussian, H., Alwadain, A., Aziz, N., Capretz, L. F., & Abdulkadir, S. J. (2022). Detecting cybersecurity attacks in internet of things using artificial intelligence methods: A systematic literature review. *Electronics*, *11*(2), 198. https://doi.org/10.3390/electronics11020198

Ahsan, M., Nygard, K. E., Gomes, R., Chowdhury, M. M., Rifat, N., & Connolly, J. F. (2022). *Cybersecurity threats and their mitigation approaches using ML—*A review. *Journal of Cybersecurity and Privacy*, *2*(3), 527–555. https://doi.org/10.3390/jcp2030027

Akhtar, M., & Feng, T. (2021). An overview of the applications of AI in cybersecurity. *EAI Endorsed Transactions on Creative Technologies*, *8*(29), 1–8. https://doi.org/10.4108/eai.23-11-2021.172218

Alhassan, M., & Adjei-Quaye, A. (2017). Information security in an organization. *International Journal of Computer (IJC)*, *24*(1), 100–116. https://www.researchgate.net/publication/314086143_Information_Security_in_an_Organization

Alkhudhayr, F., Alfarraj, S., Aljameeli, B., & Elkhdiri, S. (2019, May). Information security: A review of information security issues and techniques. In *2019 2nd International Conference on Computer Applications & Information Security* (ICCAIS) (pp. 1–6). IEEE. https://doi.org/10.1109/CAIS.2019.8769504

Almeida, V., Mendes, L. S., & Doneda, D. (2023). On the development of AI governance frameworks. *IEEE Internet Computing*, *27*(1), 70–74. https://doi.org/10.1109/MIC.2022.3186030

Al-Moshaigeh, A., Dickins, D., & Higgs, J. L. (2019). Cybersecurity risks and controls: Is the AICPA's SOC for Cybersecurity a solution?. *CPA Journal*, *89*(6), 36–41. https://www.proquest.com/openview/72915043b6ca9ac3e25c96c664bccb71/1?pq-origsite=gscholar&cbl=41798

Alothman, B., Alhajraf, A., Alajmi, R., Farraj, R. A., Alshareef, N., & Khan, M. (2022). Developing a Cyber incident exercises model to educate security teams. *Electronics*, *11*(10), 1575. https://doi.org/10.3390/electronics11101575

Alrobaian, S., Alshahrani, S., & Almaleh, A. (2023). Cybersecurity awareness assessment among trainees of the technical and vocational training corporation. *Big Data and Cognitive Computing*, *7*(2), 73. https://doi.org/10.3390/bdcc7020073

Al-Rushdan, H., Shurman, M., & Alnabelsi, S. (2020). On detection and prevention of zero-day attack using Cuckoo Sandbox in software-defined networks. *International Arab Journal of Information Technology*, *17*(4A), 662–670. https://doi.org/10.34028/iajit/17/4A/11

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

Amanowicz, M. (2021). A shared cybersecurity awareness platform. *Journal of Telecommunications and Information Technology*, (3), 32–41. https://doi.org/10.26636/jtit.2021.154421

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

Anderson, K. (2016). *Technology and social trends: A Biblical point of view.* Christian Publishing House, the Bible.

Andress, J. (2014). *The basics of information security: Understanding the fundamentals of InfoSec in theory and practice.* Syngress.

Bada, M., Sasse, A. M., & Nurse, J. R. (2019). *Cyber security awareness campaigns: Why do they fail to change behavior?* arXiv. https://arxiv.org/abs/1901.02672

Baksh, B. (2018). To bracket or not to bracket: Reflections of a novice qualitative researcher. *Reflections: Narratives of Professional Helping*, *24*(3), 45–55. https://reflectionsnarrativesofprofessionalhelping.org/index.php/Reflections/article/view/1637/1556

Balbix. (2022). *Software security solutions – End-to-end code security*. Digicert.

Bansal, P. (2018). New ways of seeing through qualitative research. *Academy of Management Journal*, *61*(4), 1189–1195. https://doi.org/10.5465/amj.2018.4004

Bendiek, A., & Metzger, T. (2015). Deterrence theory in the cyber-century. Lessons from a state-of the-art literature review. *INFORMATIK 2015*. https://dl.gi.de/bitstream/handle/20.500.12116/2216/553.pdf?sequence=1&isAllowed=y

Bengio, Y. (2023). AI and catastrophic risk. *Journal of Democracy*, *34*(4), 111–121. https://doi.org/10.1353/jod.2023.a907692.

Bently, L. (2012). What is “intellectual property”? *The Cambridge Law Journal*, *71*(3), 501–505. https://doi.org/10.1017/S0008197312000797

Berg, B. L., & Lune, H. (2017). *Qualitative research methods for the social sciences* (9th ed.).

Pearson.

Biggio, B. (2010). Adversarial pattern classification. *Proceedings of IEEE*, *106*(2), 230–235. https://www.academia.edu/download/49343472/Adversarial_Pattern_Classification201610 04-25807-guotk3.pdf

Blauth, T. F., Gstrein, O. J., & Zwitter, A. (2022). AI crime: An overview of malicious use and abuse of AI. *IEEE Access*, *10*, 77110–77122. https://doi.org/10.1109/ACCESS.2022.3191790

Bondwe, G. W. (2019). *Strategies to mitigate supply chain disruptions in grocery businesses* (Publication No. 27995866) [Doctoral dissertation, Tennessee State University]. ProQuest Dissertations and Theses Global. https://www.proquest.com/openview/417613d686080501e20d6ed713a8e007/1?pq-origsite=gscholar&cbl=18750&diss=y

Bonell, C., Fletcher, A., Morton, M., Lorenc, T., & Moore, L. (2013). Methods don't make assumptions, researchers do: A response to Marchal et al. S*ocial Science & Medicine (1982)*, *94*, 81–82. https://doi.org/10.1016/j.socscimed.2013.06.026

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Braun, V., & Clarke, V. (2019). Reflecting on reflexive thematic analysis. *Qualitative Research in Sport, Exercise and Health*, *11*(4), 589–597. https://doi.org/10.1080/2159676X.2019.1628806

Brown, A. (2020). *Improving implementation DoD supply chain counterfeit prevention and detection policy: A qualitative multiple case study* (Publication No. 13899809) [Doctoral dissertation, Northcentral University]. ProQuest Dissertations and Theses Global.

https://www.proquest.com/openview/8383ce03fa0a9c9d7951ffd58d054d34/1?pq-origsite=gscholar&cbl=51922&diss=y

Brown, H. (2022). *Low code is revolutionizing the software industry: What type is dominating?* Cyclr. https://cyclr.com/blog/low-code-is-revolutionising-the-software-industry

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Dafoe, A., Scharre, P., Zeitzoff, T., Filar, B., Anderson, H., Roff, H., Allen, G. C., Steinhardt, J., Flynn, C., O hEigeartaigh, S., Beard, S., Belfield, H., Farquhar, S., ... Zeitzoff, T. (2018). The malicious use of AI: Forecasting, prevention, and mitigation. *Nature Machine Intelligence*, *1*(2), 389–396. https://doi.org/10.48550/arXiv.1802.07228

Camélia, R., & Nadia, S. (2022). Board gender diversity and corporate response to cyber risk: Evidence from cybersecurity related disclosure. *Journal of Business Ethics*, *177*(2), 351–374. https://doi.org/10.1007/s10551-020-04717-9

Candela, A. G. (2019). Exploring the function of member checking. *The Qualitative Report*, *24*(3), 619–628. https://doi.org/10.46743/2160-3715/2019.3726

Candelon, F., Courtaux, M., & Nahas, G. (2022, June 7). Is 'A.I. for everyone' A good idea for businesses? *Fortune.* https://fortune.com/2022/06/03/artificial-intelligence-ai-democratization-no-low-code/

Carlini, N., & Wagner, D. (2017, May). Towards evaluating the robustness of neural networks. In *2017 ieee symposium on security and privacy (sp)* (pp. 39–57). Ieee.

Carriço, G. (2018). The EU and AI: A human-centered perspective. *European View*, *17*(1), 29–36. https://doi.org/10.1177/1781685818764821

Carter, N., Bryant-Lukosius, D., DiCenso, A., Blythe, J., & Neville, A. J. (2014). The use of triangulation in qualitative research. *Oncology Nursing Forum*, *41*(5), 545–547.

https://doi.org/10.1188/14.onf.545-547

Castleberry, A., & Nolen, A. (2018). Thematic analysis of qualitative research data: Is it as easy as it sounds? *Currents in Pharmacy Teaching and Learning*, *10*(6), 807–815. https://doi.org/10.1016/j.cptl.2018.03.019

Charmaz, K. (2006). *Constructing grounded theory: A practical guide through qualitative analysis*. Sage.

Chen, Y., Tang, G., Jin, J., Xie, Q., & Li, J. (2014). CEOs' transformational leadership and product innovation performance: The roles of corporate entrepreneurship and technology orientation. *Journal of Product Innovation Management*, *31*(S1), 2–17. https://doi.org/10.1111/jpim.12188

Cisco. (2022, June 6). *What is malware? - definition and examples.* Cisco. https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-malware.html

Copeland, B. (2022, August 24). AI. *In* Encyclopedia Britannica. https://www.britannica.com/technology/artificial-intelligence

Creswell, J. W. (2007). *Qualitative inquiry and research design: Choosing among five approaches* (2nd ed.). Sage.

Creswell, J. W. (2014). *Research design: Qualitative, quantitative and mixed methods approaches* (4th ed.). Sage.

Creswell, J. W., & Miller, D. L. (2000). Determining validity in qualitative inquiry. *Theory Into Practice*, *39*(3), 124–130. https://doi.org/10.1207/s15430421tip3903_2

Creswell, J. W., & Poth, C. N. (2018). *Qualitative inquiry & research design: Choosing among five approaches* (4th ed.). Sage.

Cypress, B. S. (2017). Rigor or reliability and validity in qualitative research: Perspectives, strategies, reconceptualization, and recommendations. *Dimensions of Critical Care Nursing*, *36*(4), 253–263. https://doi.org/10.1097/DCC.0000000000000253

Cypress, B. S. (2019). Data analysis software in qualitative research: Preconceptions, expectations, and adoption. *Dimensions of Critical Care Nursing*, *38*(4), 213–220. https://doi.org/10.1097/DCC.0000000000000363

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

Dearden, T. E., Parti, K., Hawdon, J., Gainey, R., Vandecar-Burdin, T., & Albanese, J. (2023). Differentiating insider and outsider cyber-attacks on businesses. *American Journal of Criminal Justice*, *48*(4), 871–886. https://doi.org/10.1007/s12103-023-09727-7

De Arroyabe, I. F., Arranz, C. F., Arroyabe, M. F., & de Arroyabe, J. C. F. (2023). Cybersecurity capabilities and cyber-attacks as drivers of investment in cybersecurity systems: A UK survey for 2018 and 2019. *Computers & Security*, *124*, 102954. https://doi.org/10.1016/j.cose.2022.102954

Dempsey, L., Dowling, M., Larkin, P., & Murphy, K. (2016). Sensitive interviewing in qualitative research: Sensitive interviewing. *Research in Nursing & Health*, *39*(6), 480–490. https://doi.org/10.1002/nur.21743

Denzin, N. K., & Lincoln, Y. S. (2002). *The qualitative inquiry reader*. Sage.

Denzin, N. K., & Lincoln, Y. S. (2018). *The Sage handbook of qualitative research*. Sage.

DiGaetano, R. (2013). Sample frame and related sample design issues for surveys of physicians and physician practices. *Evaluation & the Health Professions*, *36*(3), 296–329.

https://doi.org/10.1177/0163278713496566

Dilek, S., Çakır, H., & Aydın, M. (2015). *Applications of AI techniques to combating cybercrimes: A review.* arXiv preprint arXiv:1502.03552.

Dissanayake, N., Jayatilaka, A., Zahedi, M., & Babar, M. A. (2022). Software security patch management-A systematic literature review of challenges, approaches, tools and practices. *Information and Software Technology*, *144*, 106771. https://doi.org/10.1016/j.infsof.2021.106771

Dixon, C. S. (2015). Interviewing adolescent females in qualitative research. *The Qualitative Report*, *20*(12), 2067–2077. https://doi.org/10.46743/2160-3715/2015.2436

Dixon, W., & Eagan, N. (2019, June). 3 ways AI will change the nature of cyber-attacks. In *Online World Economic Forum*. https://www.weforum.org/agenda/2019/06/ai-is-powering-a-new-generation-ofcyber-attack-its-also-our-best-defence

Dodgson, J. E. (2019). Reflexivity in qualitative research. *Journal of Human Lactation*, *35*(2), 220–222. https://doi.org/10.1177/0890334419830990

Dojkovski, S., Lichtenstein, S., & Warren, M. (2010, January). Enabling information security culture: Influences and challenges for Australian SMEs. In *ACIS 2010: Proceedings of the 21st Australasian Conference on Information Systems*. ACIS.

Edmonds, W. A., & Kennedy, T. D. (2017). *An applied guide to research designs* (2nd ed.). Sage.

Edmonds, W. A., & Kennedy, T. D. (2017). Quantitative methods for experimental and Quasi-experimental research. *An Applied Guide to Research Designs*, 29–34. Sage.

Emmitt, J. (2021). *Patch management: Best practices and why it's important.* Security Boulevard. https://securityboulevard.com/2021/03/patch-management-best-practices-and-why-its-important/

Fambro, I. (2016). Qualities distinctive to Christian researchers: A quest for spiritual significance. *Emerging Leadership Journeys*, *9*(1), 106–112. https://www.regent.edu/acad/global/publications/elj/vol9iss1/6ELJ-Fambro.pdf

Farooq, M. B., & de Villiers, C. (2017). Telephonic qualitative research interviews: When to consider them and how to do them. *Meditari Accountancy Research*, *25*(2), 291–316. https://doi.org/10.1108/MEDAR-10-2016-0083

Ferrag, M. A., Maglaras, L., Janicke, H., & Smith, R. (2019, September). Deep learning techniques for cyber security intrusion detection: A detailed analysis. In *6th International Symposium for ICS & SCADA Cyber Security Research 2019 6* (pp. 126–136).

Finlay, L. (2002). Negotiating the swamp: The opportunity and challenge of reflexivity in research practice. *Qualitative Research*, *2*(2), 209–230. https://doi.org/10.1177/146879410200200205

Fitzgerald, L., & Dopson, S. (2009). Comparative case study designs: Their utility and development in organizational research. In D. A. Buchanan & A. Bryman (Eds.), *The SAGE handbook of organizational research methods* (pp. 465–485). SAGE.

Fletcher, D., De Massis, A., & Nordqvist, M. (2016). Qualitative research practices and family business scholarship: A review and future research agenda. *Journal of Family Business Strategy*, *7*, 8–25. https://doi.org/10.1016/j.jfbs.2015.08.001.

Frank, M. L., Grenier, J. H., & Pyzoha, J. S. (2019). How disclosing a prior cyber-attack influences the efficacy of cybersecurity risk management reporting and independent assurance. *Journal of Information Systems*, *33*(3), 183–200. https://doi.org/10.2308/isys-52374

Frey, B. (2018). *The SAGE encyclopedia of educational research, measurement, and evaluation* (Vols. 1–4). Sage. https://doi.org/10.4135/9781506326139

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

Fusch, P. I., & Ness, L. R. (2015). Are we there yet? Data saturation in qualitative research. *Qualitative Report*, *20*(9), 1408–1420. https://doi.org/10.46743/2160-3715/2015.2281

Gao, L., Calderon, T. G., & Tang, F. (2020). Public companies' cybersecurity risk disclosures. *International Journal of Accounting Information Systems*, *38*, 100468. https://doi.org/10.1016/j.accinf.2020.100468

Garcia-Perez, A., Sallos, M. P., & Tiwasing, P. (2023). Dimensions of cybersecurity performance and crisis response in critical infrastructure organisations: An intellectual capital perspective. *Journal of Intellectual Capital*, *24*(2), 465–486. https://doi.org/10.1108/JIC-06-2021-0166

Geetha, R., & Thilagam, T. (2021). A review on the effectiveness of machine learning and deep learning algorithms for cyber security. *Archives of Computational Methods in Engineering State of the Art Reviews*, *28*(4), 2861–2879. https://doi.org/10.1007/s11831-020-09478-2

Gioulekas, F., Stamatiadis, E., Tzikas, A., Gounaris, K., Georgiadou, A., Michalitsi-Psarrou, A., Doukas, G., Kontoulis, M., Nikoloudakis, Y., Marin, S., Cabecinha, R., & Ntanos, C. (2022). A cybersecurity culture survey targeting healthcare critical infrastructures. *Healthcare (Basel, Switzerland)*, *10*(2), 327. https://doi.org/10.3390/healthcare10020327

Goldkuhl, G. (2012). Pragmatism vs interpretivism in qualitative information systems research. *European Journal of Information Systems*, *21*(2), 135–146. https://doi.org/10.1057/ejis.2011.54

Goodman, D. (2020, January 10). *Infographic: Low-code application development trends.* Mendix.

https://www.mendix.com/blog/infographic-low-code-application-development-trends/

Goodman, W. (2010). Cyber deterrence: Tougher in theory than in practice? *Strategic Studies Quarterly*, *4*(3), 102–135. http://www.jstor.org/stable/26269789

Green, J., Willis, K., Hughes, E., Small, R., Welch, N., Gibbs, L., & Daly, J. (2007). Generating best evidence from qualitative research: The role of data analysis. *Australian and New Zealand Journal of Public Health*, *31*(6), 545–550. https://doi.org/10.1111/j.1753-6405.2007.00141.x

Grey, E. (2016). Cultural beliefs and practices of ethnic Filipinos: An ethnographic study. *Social Sciences*, *3*(3), 2016. https://doi.org/10.21013/jmss.v3.n3.p30

Gudigantala, N., Madhavaram, S., & Bicen, P. (2023). An AI decision-making framework for business value maximization. *AI Magazine*, *44*(1), 67–84. https://doi.org/10.1002/aaai.12076

Guion, L. A. (2002). *Triangulation: Establishing the validity of qualitative studies.* Institute of Food and Agricultural Sciences, University of Florida. https://sites.duke.edu/niou/files/2014/07/W13-Guion-2002-Triangulation-Establishing-the-Validity-of-Qualitative-Research.pdf

Hagendorff, T. (2021). Forbidden knowledge in ML reflections on the limits of research and publication. *AI & Society*, *36*(3), 767–781. https://doi.org/10.1007/s00146- 020-01045-4

Haley, C. (2013). A theory of cyber deterrence*. Georgetown Journal of International Affairs*, 2013.

Hao, K. (2020). *Hackers trick a Tesla into veering into the wrong lane* | MIT Technology Review. MIT Technology Review. https://www.technologyreview.com/2019/04/01/65915/hackers-trick-teslas-autopilot-into-veering-towards-oncoming-traffic

Hegwer, L. R. (2017, January 19). Managing cybersecurity threats. *Healthcare Financial*

Management, *71*(2), 32–40. https://www.hfma.org/legal-and-regulatory-compliance/privacy-and-hipaa/52145/

Hennink, M., & Kaiser, B. N. (2022). Sample sizes for saturation in qualitative research: A systematic review of empirical tests. *Social Science & Medicine*, *292*, 114523. https://doi.org/10.1016/j.socscimed.2021.114523

Hu, Y., Kuang, W., Qin, Z., Li, K., Zhang, J., Gao, Y., Li, W., & Li, K. (2023). AI security: Threats and countermeasures. *ACM Computing Surveys*, *55*(1), 1–36. https://doi.org/10.1145/3487890

Hutchings, T. (2017). Design and the digital Bible: Persuasive technology and religious reading. *Journal of Contemporary Religion*, *32*(2), 205–219. https://doi.org/10.1080/13537903.2017.1298903

Islam, M. S., Wang, T., Farah, N., & Stafford, T. (2021). The spillover effect of focal firms' cybersecurity breaches on rivals and the role of the CIO: Evidence from stock trading volume. *Journal of Accounting and Public Policy*, *41*(2), 106916. https://doi.org/10.1016/j.jaccpubpol.2021.106916

Jakhar, D., & Kaur, I. (2020). Artificial intelligence, machine learning and deep learning: Definitions and differences. *Clinical and Experimental Dermatology*, *45*(1), 131–132. https://doi.org/10.1111/ced.14029

Janiesch, C., Zschech, P., & Heinrich, K. (2021). Machine learning and deep learning. *Electronic Markets*, *31*(2-3), 685–695. https://doi.org/10.1007/s12525-021-00475-2

Jogaratnam, G. (2017). How organizational culture influences market orientation and business performance in the restaurant industry. *Journal of Hospitality and Tourism Management*, *31*, 211–219. https://doi.org/10.1016/j.jhtm.2017.03.002

Johnson, F. (2016). The process of oncology nurse practitioner patient navigation: A pilot study. *Clinical Journal of Oncology Nursing*, *20*(2), 207–210. https://doi.org/10.1188/16.CJON.207-210

Kabbas, A., Alharthi, A., & Munshi, A. (2020). Artificial intelligence applications in cybersecurity. *IJCSNS International Journal of Computer Science and Network Security*, *20*(2), 120–124. http://paper.ijcsns.org/07_book/202002/20200216.pdf

Kaloudi, N., & Li, J. (2020). The AI-based cyber threat landscape: A survey. *ACM Computing Surveys (CSUR)*, *53*(1), 1–34. https://doi.org/10.1145/3372823

Kam, H., Menard, P., Ormond, D., & Crossler, R. E. (2020). Cultivating cybersecurity learning: An integration of self-determination and flow. *Computers & Security*, *96*, 101875. https://doi.org/10.1016/j.cose.2020.101875

Kar Yee, C., & Zolkipli, M. F. (2021). Review on confidentiality, integrity and availability in information security. *Journal of ICT in Education*, *8*(2), 34–42. https://doi.org/10.37134/jictie.vol8.2.4.2021

Keller, T., & Alsdorf, K. L. (2012). *Every good endeavor: connecting your work to God's work.* Dutton.

Kelly, R. (2020). *Almost 90% of cyber-attacks are caused by human error or behavior.* ChiefExecutive.net. https://chiefexecutive.net/almost-90-cyber-attacks-caused-human-error-behavior/

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

Kennedy, J., Holt, T., & Cheng, B. (2019). Automotive cybersecurity: Assessing a new platform for cybercrime and malicious hacking. *Journal of Crime & Justice*, *42*(5), 632–645.

https://doi.org/10.1080/0735648X.2019.1692425

Kessler, S. R., Pindek, S., Kleinman, G., Andel, S. A., & Spector, P. E. (2020). Information security climate and the assessment of information security risk among healthcare employees. *Health Informatics Journal*, *26*(1), 461–473. https://doi.org/10.1177/1460458219832048

Khidzir, N. Z., Daud, K. A. M., Ismail, A. R., Ghani, M. S. A. A., & Ibrahim, M. A. H. (2018). Information security requirement: The relationship between cybersecurity risk confidentiality, integrity and availability in digital social media. In *Regional Conference on Science, Technology and Social Sciences* (RCSTSS 2016) (pp. 229–237). Springer, Singapore.

Kobayashi, A. (2019). *International encyclopedia of human geography.* Elsevier.

Korolov, M. (2017, October 19). *How AI can help you stay ahead of cybersecurity threats.* CSO Online. https://www.csoonline.com/article/3233951/how-ai-can-help-you-stay-ahead-of-cybersecurity-threats.html

Kostyuk, N. (2021). Deterrence in the cyber realm: Public versus private cyber capacity. *International Studies Quarterly*, *65*(4), 1151–1162. https://doi.org/10.1093/isq/sqab039

Kramer, F. D., Starr, S. H., & Wentz, L. K. (2009). *Cyber power and national security.* Center for Technology and National Security Policy. https://doi.org/10.2307/j.ctt1djmhj1

Krathwohl, D. R. (2009). *Methods of educational and social science research: The logic of methods*. Waveland Press.

Kweon, E., Lee, H., Chai, S., & Yoo, K. (2021). The utility of information security training and education on cybersecurity incidents: An empirical evidence. *Information Systems Frontiers*, *23*(2), 361–373. https://doi.org/10.1007/s10796-019-09977-z

Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. *Business*

Horizons, *64*(5), 659–671. https://doi.org/10.1016/j.bushor.2021.02.022

Leedy, P. D., & Ormrod, J. E. (2019). *Practical research*. Macmillan.

Lewis, S. (2015). Qualitative inquiry and research design: Choosing among five approaches. *Health Promotion Practice*, *16*(4), 473–475. https://doi.org/10.1177/1524839915580941

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*, 13–24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Libicki, M. C. (2009). *Cyberdeterrence and Cyberwar*. RAND Corporation.

Lilli, E. (2021). Redefining deterrence in cyberspace: Private sector contribution to national strategies of cyber deterrence. *Contemporary Security Policy*, *42*(2), 163–188. https://doi.org/10.1080/13523260.2021.1882812

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry*. Sage.

Lincoln, Y. S., & Guba, E. E. (1986). Research, evaluation, and policy analysis: Heuristics for disciplined inquiry. *Review of Policy Research*, *5*(3), 546–565. https://doi.org/10.1111/j.1541-1338.1986.tb00429.x

Liu, C., Huang, P., & Lucas, H. C. (2020). Centralized IT decision making and cybersecurity breaches: Evidence from U.S. higher education institutions. *Journal of Management Information Systems*, *37*(3), 758–787. https://doi.org/10.1080/07421222.2020.1790190

Lonergan, E., & Montgomery, M. (2021). What is the future of cyber deterrence? *The SAIS Review of International Affairs*, *41*(2), 61–73. https://doi.org/10.1353/sais.2021.0018

Luo, G. (2020). Research on network security vulnerability detection method based on artificial intelligence. *Journal of Physics: Conference Series*, *1651*(1), 012005.

https://doi.org/10.1088/1742-6596/1651/1/012005

Mangelsdorf, M. E. (2017). What executives get wrong about cybersecurity. *MIT Sloan Management Review*, *58*(2), 22.

Marshall, C., & Rossman, G. B. (2016). *Designing qualitative research*. Sage.

Mason, J. (2006). Mixing methods in a qualitatively driven way. *Qualitative Research*, *6*(1), 9–25. https://doi.org/10.1177/1468794106058866

Mathews, S. L. (2018). *A quantitative examination of the relationship between organizational commitment, work-life balance and voluntary turnover intention of women faculty in the STEM disciplines within the United States* (Publication No. 13424114) [Doctoral dissertation, Liberty University]. ProQuest Dissertations and Theses Global. https://www.proquest.com/openview/35102d6cd298ff8a05baae1818d08095/1?pq-origsite=gscholar&cbl=18750&diss=y

Mazanec, B. M., & Thayer, B. A. (2016). Deterrence theory and the challenge of applying it to cyber warfare. In *Deterring cyber warfare* (pp. 29–43). Palgrave Macmillan UK. https://doi.org/10.1057/9781137476180_3

Mazarr, M. J. (2021). Understanding deterrence. *NL ARMS Netherlands Annual Review of Military Studies 2020: Deterrence in the 21st Century—Insights from Theory and Practice*, 13–28. https://doi.org/10.1007/978-94-6265-419-8_2

McMahon, S. A., & Winch, P. J. (2018). Systematic debriefing after qualitative encounters: An essential analysis step in applied qualitative research. *BMJ Global Health*, *3*(5), e000837. https://doi.org/10.1136/bmjgh-2018-000837

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

Miranda, M. J. (2018). Enhancing cybersecurity awareness training: A comprehensive phishing

exercise approach. *International Management Review*, *14*(2), 5–10. http://www.imrjournal.org/uploads/1/4/2/8/14286482/imr-v14n2art1.pdf

Moed, H. F. (2010). Measuring contextual citation impact of scientific journals. *Journal of Informetrics*, *4*(3), 265–277. https://doi.org/10.1016/j.joi.2010.01.002

Moore, S. (2021, May 17). *Gartner forecasts worldwide security and risk management spending to exceed $150 billion in 2021*. Gartner. https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwide-security-and-risk-managem

Morawski, C. M., & Rottmann, J. (2016, May 16). Multimodal narrative inquiry: Six teacher candidates respond. *International Journal of Education & the Arts*, *17*(14). http://www.ijea.org/v17n14/

Morgan, S. (2019). *Official Annual Cybercrime Report*. A 2019 report from Cybersecurity Ventures sponsored by Herjavec Group. https://www.herjavecgroup.com/wpcontent/uploads/2018/12/CV-HG-2019-Official-AnnualCybercrime-Report.pdf

Morse, J. M. (2015). Critical analysis of strategies for determining rigor in qualitative inquiry. *Qualitative Health Research*, *25*(9), 1212–1222. https://doi.org/10.1177/1049732315588501

Morse, J. M., Barrett, M., Mayan, M., Olson, K., & Spiers, J. (2002). Verification strategies for establishing reliability and validity in qualitative research. *International Journal of Qualitative Methods*, *1*(2), 13–22. https://doi.org/10.1177/160940690200100202

Moustakas, C. E. (1994). *Phenomenological research methods.* Sage.

Mumford, M. D., Hunter, S. T., & Byrne, C. L. (2009). What is the fundamental? The role of cognition in creativity and innovation. *Industrial and Organizational Psychology*, *2*(3),

353–356. https://doi.org/10.1111/j.1754-9434.2009.01158.x

Munk, T. (2022). Cyber attacks, means, and methods. *The Rise of Politically Motivated Cyber Attacks*, 47–77. https://doi.org/10.4324/9781003126676-3

Nightingale, A. J. (2019). Triangulation. In *International encyclopedia of human geography* (pp. 477–480). Elsevier. https://doi.org/10.1016/b978-0-08-102295-5.10437-8

Olenick, D. (2018). *2019 Cybersecurity Predictions: AI.* Haymarket Media Inc. https://www.scmagazine.com/home/security news/2019-cybersecurity-predictions-artificial-intelligence/

Olswang, A., Gonda, T., Puzis, R., Shani, G., Shapira, B., & Tractinsky, N. (2022). Prioritizing vulnerability patches in large networks. *Expert Systems with Applications*, *193*, 116467. https://doi.org/10.1016/j.eswa.2021.116467

O'Neil, K. (2019). How qualitative data analysis happens: Moving beyond "themes emerged". *Forum: Qualitative Social Research*, *20*(3), Art. 35. https://doi.org/10.17169/fqs20.3.3388

Paoli, L., Visschers, J., & Verstraete, C. (2018). The impact of cybercrime on businesses: A novel conceptual framework and its application to Belgium. *Crime, Law and Social Change: An Interdisciplinary Journal*, *70*(4), 397–420. https://doi.org/10.1007/s10611-018-9774-y

Patel, K. K., Patel, S. M., & Scholar, P. (2016). Internet of things-IOT: Definition, characteristics, architecture, enabling technologies, application & future challenges. *International Journal of Engineering Science and Computing*, *6*(5). http://www.opjstamnar.com/download/Worksheet/Day-110/IP-XI.pdf

Patil, A., Holdowsky, J., & Kearns-Manolatos, D. (2020, December 10). *Time, technology, talent1.* Deloitte Insights. https://www2.deloitte.com/us/en/insights/focus/cognitive-technologies/cloud-machine-

learning.html?id=us%3A2em%3A3na%3A4di7015%3A5awa%3A6di%3AMMDDYY%3A%3Aauthor&pkid=1007516

Patton, M. Q. (1999). Enhancing the quality and credibility of qualitative analysis. *Health Services Research*, *34*(5 Pt 2), 1189–1208. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1089059/

Patton, M. Q. (2002). *Qualitative research and evaluation methods.* Sage.

Patton, M. Q. (2014). *Qualitative research & evaluation methods: Integrating theory and practice.* Sage.

Petrova, E., Dewing, J., & Camilleri, M. (2016). Confidentiality in participatory research: Challenges from one study. *Nursing Ethics*, *23*(4), 442–454. https://doi.org/10.1177/0969733014564909.

Price, J. H., & Murnan, J. (2004). Research limitations and the necessity of reporting them. *American Journal of Health Education*, *35*(2), 66–67. https://doi.org/10.1080/19325037.2004.10603611

Quackenbush, S., & Zagare, F. (2016). *Modern deterrence theory: Research trends, policy debates, and methodological controversies.* Oxford.

Rahman, M. T., Rahman, M. S., Wang, H., Tajik, S., Khalil, W., Farahmandi, F., Forte, D., Asadizanjani, N., & Tehranipoor, M. (2020). Defense-in-depth: A recipe for logic locking to prevail. *Integration*, *72*, 39–57. https://doi.org/10.1016/j.vlsi.2019.12.007

Rawindaran, N., Jayal, A., & Prakash, E. (2021). Machine learning cybersecurity adoption in small and medium enterprises in developed countries. *Computers*, *10*(11), 150. https://doi.org/10.3390/computers10110150

Regnault, A., Willgoss, T., & Barbic, S. (2018). Towards the use of mixed methods inquiry as best

practice in health outcomes research. *Journal of Patient-Reported Outcomes*, *2*(1), 1–4. https://doi.org/10.1186/s41687-018-0043-8

Rehman, S. u., Khaliq, M., Imtiaz, S. I., Rasool, A., Shafiq, M., Javed, A. R., Jalil, Z., & Bashir, A. K. (2021). DIDDOS: An approach for detection and identification of distributed denial of service (DDoS) cyber-attacks using gated recurrent units (GRU). *Future Generation Computer Systems*, *118*, 453–466. https://doi.org/10.1016/j.future.2021.01.022

Richardson, L. (2000). Evaluating ethnography. *Qualitative Inquiry*, *6*(2), 253–255. https://doi.org/10.1177/107780040000600207

Robson, C., & McCartan, K. (2016). *Real-world research: A resource for users of social research methods in applied settings.* Wiley.

Ross, C. (2021). Is it time to forget about cyber deterrence? *Air & Space Power Journal*, *35*(1), 69–73. https://www.proquest.com/openview/fdde55fc4b8c8dc93cd9fbd44b2a2d75/1?pq-origsite=gscholar&cbl=26498

Ross, R., Pillitteri, V., Dempsey, K., Riddle, M., & Guissanie, G. (2019). *Protecting controlled unclassified information in nonfederal systems and organizations* (No. NIST Special Publication [SP] 800-171 Rev. 2 [Draft]). National Institute of Standards and Technology.

Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., & McQuaid, R. (2019). *Developing cyber resilient systems: a systems security engineering approach* (No. NIST Special Publication [SP] 800-160 Vol. 2 [Draft]). National Institute of Standards and Technology.

Roumani, Y. (2021). Patching zero-day vulnerabilities: An empirical analysis. *Journal of Cybersecurity*, *7*(1), tyab023. https://doi.org/10.1093/cybsec/tyab023

Rubin, H. J., & Rubin, I. S. (2012). *Qualitative interviewing: The art of hearing data*. Sage.

Rughani, P. H. (2017). Artificial intelligence-based digital forensics framework. *International*

Journal of Advanced Research in Computer Science, *8*(8), 10–14. https://doi.org/10.26483/ijarcs.v8i8.4571

Saad, S., Briguglio, W., & Elmiligi, H. (2019). *The curious case of ML in malware detection.* arXiv preprint arXiv:1905.07573.

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the 'weakest link'—A human/computer interaction approach to usable and effective security. *BT Technology Journal*, *19*(3), 122–131. https://doi.org/10.1023/A:1011902718709

Sawyer, B. D., & Hancock, P. A. (2018). Hacking the human: The prevalence paradox in cybersecurity. *Human Factors*, *60*(5), 597–609. https://doi.org/10.1177/0018720818780472

Shakeel, I. (2021, April 6). *Use ai to fight AI-powered cyber-attacks*. AT&T Cybersecurity. https://cybersecurity.att.com/blogs/security-essentials/use-ai-to-fight-ai-powered-cyber-attacks

Shamiulla, A. M. (2019). Role of artificial intelligence in cyber security. *International Journal of Innovative Technology and Exploring Engineering*, *9*(1), 4628–4630. https://doi.org/10.35940/ijitee.A6115.119119

Sharma, V., You, I., Andersson, K., Palmieri, F., Rehmani, M. H., & Lim, J. (2020). Security, privacy and trust for smart mobile- internet of things (M-IoT): A survey. *IEEE Access*, *8*, 167123–167163. https://doi.org/10.1109/ACCESS.2020.3022661

Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. A., Chen, S., Liu, D., & Li, J. (2020). Performance comparison and current challenges of using machine learning techniques in cybersecurity. *Energies*, *13*(10), 2509. https://doi.org/10.3390/en13102509

Silverman, D. (2016). Introducing qualitative research. *Qualitative Research*, *3*(3), 14–25. https://methods.sagepub.com/video/david-silverman-discusses-qualitative-research

Simon, M. K. (2011). *Dissertation and scholarly research: Recipes for success*. Dissertation Success, LLC.

Simon, M. K., & Goes, J. (2017). *Dissertation and scholarly research: Recipes for success* (2nd ed.). CreateSpace Independent Publishing Platform.

Soni, V. D. (2019). Role of artificial intelligence in combating cyber threats in banking. *International Engineering Journal for Research & Development*, *4*(1), 7–7. https://www.researchgate.net/publication/343017498_ROLE_OF_ARTIFICIAL_INTELLIGENCE_IN_COMBATING_CYBER_THREATS_IN_BANKING

Sreedevi, A. G., Nitya Harshitha, T., Sugumaran, V., & Shankar, P. (2022). Application of cognitive computing in healthcare, cybersecurity, big data and IoT: A literature review. *Information Processing & Management*, *59*(2), 102888. https://doi.org/10.1016/j.ipm.2022.102888

Stake, R. E. (1995). *The art of case study research*. Sage.

Stake, R. E. (2010). *Qualitative research: Studying how things work.* Guilford Press.

Stevens, T. (2020). Knowledge in the grey zone: AI and cybersecurity. *Digital War*, *1*(1-3), 164–170. https://doi.org/10.1057/s42984-020-00007-w

Stewart, J. (2012). Multiple-case study methods in governance-related research. *Public Management Review*, *14*(1), 67–82. https://doi.org/10.1080/14719037.2011.589618

Stojnic, T., Vatsalan, D., & Arachchilage, N. A. G. (2021). Phishing email strategies: Understanding cybercriminals' strategies of crafting phishing emails. *Security and Privacy*, *4*(5), e165. https://doi.org/10.1002/spy2.165

Sutton, J., & Austin, Z. (2015). Qualitative research: Data collection, analysis, and management. *The Canadian Journal of Hospital Pharmacy*, *68*(3), 226–231.

https://doi.org/10.4212/cjhp.v68i3.1456

Taddeo, M. (2019). Three ethical challenges of applications of artificial intelligence in cybersecurity. *Minds and Machines (Dordrecht)*, *29*(2), 187–191. https://doi.org/10.1007/s11023-019-09504-8

Taddeo, M., & Floridi, L. (2018). Regulate artificial intelligence to avert the cyber arms race. *Nature*, *556*(7701), 296–298. https://doi.org/10.1038/d41586-018-04602-6

Taddeo, M., McCutcheon, T., & Floridi, L. (2019). Trusting artificial intelligence in cybersecurity is a double-edged sword. *Nature Machine Intelligence*, *1*(12), 557–560. https://doi.org/10.1038/s42256-019-0109-1

Tchernykh, A., Schwiegelsohn, U., Talbi, E., & Babenko, M. (2019). Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability. *Journal of Computational Science*, *36*, 100581. https://doi.org/10.1016/j.jocs.2016.11.011

Teherani, A., Martimianakis, T., Stenfors-Hayes, T., Wadhwa, A., & Varpio, L. (2015). Choosing a qualitative research approach. *Journal of Graduate Medical Education*, *7*(4), 669–670. https://doi.org/10.4300/JGME-D-15-00414.1

Theofanidis, D., & Fountouki, A. (2018). Limitations and delimitations in the research process. Perioperative Nursing-Quarterly Scientific. *Online Official Journal of GORNA*, *7*(3 September-December 2018), 155–163. https://doi.org/10.5281/zenodo.2552022

Ting-Toomey, S., & Dorjee, T. (2018). *Communicating across cultures* (2nd ed.). ProQuest Ebook Central.

Tran, V. T., Porcher, R., Falissard, B., & Ravaud, P. (2016). Point of data saturation was assessed using resampling methods in a survey with open-ended questions. *Journal of Clinical Epidemiology*, *80*, 88–96. https://doi.org/10.1016/j.jclinepi.2016.07.014

Truong, T. C., Diep, Q. B., & Zelinka, I. (2020). Artificial intelligence in the cyber domain: Offense and defense. *Symmetry*, *12*(3), 410. https://doi.org/10.3390/sym12030410

Truong, T. C., Zelinka, I., Plucar, J., Čandík, M., & Šulc, V. (2020). *Artificial intelligence and cybersecurity: Past, presence, and future. In AI and evolutionary computations in engineering systems* (pp. 351–363). Springer, Singapore.

Tufail, S., Parvez, I., Batool, S., & Sarwat, A. (2021). A survey on cybersecurity challenges, detection, and mitigation techniques for the smart grid. *Energies (Basel)*, *14*(18), 5894. https://doi.org/10.3390/en14185894

Tufte, E. (2001). *The visual display of quantitative information* (2nd ed.). Graphics Press.

Ullah, F., Edwards, M., Ramdhany, R., Chitchyan, R., Babar, M. A., & Rashid, A. (2018). Data exfiltration: A review of external attack vectors and countermeasures. *Journal of Network and Computer Applications*, *101*, 18–54. https://doi.org/10.1016/j.jnca.2017.10.016

Usman, M., Jan, M., He, X., & Chen, J. (2020). A survey on representation learning efforts in cybersecurity domain. *ACM Computing Surveys*, *52*(6), 1–28. https://doi.org/10.1145/3331174

van Rijnsoever, F. J. (2017). (I can't get no) saturation: A simulation and guidelines for sample sizes in qualitative research. *PLoS One*, *12*(7), 1–17. https://doi.org/10.1371/journal.pone.0181689

Vorobeychik, Y., & Kantarcioglu, M. (2018). Adversarial machine learning. *Synthesis Lectures on Artificial Intelligence and Machine Learning*, *12*(3), 1–169. https://doi.org/10.1007/978-3-031-01580-9

Walkowski, M., Krakowiak, M., Oko, J., & Sujecki, S. (2020). Efficient algorithm for providing live vulnerability assessment in corporate network environment. *Applied Sciences*, *10*(21),

7926. https://doi.org/10.3390/app10217926

Ware, C. (2008). Toward a perceptual theory of flow visualization. *IEEE Computer Graphics and Applications*, *28*(2), 6–11. https://doi.org/10.1109/MCG.2008.39

Wassenaar, D. R., & Singh, S. (2016). Contextualizing the role of the gatekeeper in social science research. *South African Journal of Bioethics and Law*, *9*(1), 42–46. https://doi.org/10.7196/SAJBL.2016.v9i1.465

Weaver, R., Weaver, D., & Farwood, D. (2013). *Guide to network defense and countermeasures.* Cengage Learning.

Wiersma, W. (2000). *Research methods in education: An introduction.* Allyn and Bacon.

Williams, J. B. (2017). *Leading high school students to adopt a biblical worldview through discipleship at First Baptist Church, Lawrenceville, Georgia*. The Southern Baptist Theological Seminary. http://hdl.handle.net/10392/5357

Williamson, K. (2017). *Research methods: Information, systems, and contexts* (2nd ed.). Chandos Publishing.

Willison, R., Warkentin, M., & Johnston, A. C. (2018). Examining employee computer abuse intentions: Insights from justice, deterrence and neutralization perspectives. *Information Systems Journal*, *28*(2), 266–293. https://doi.org/10.1111/isj.12129

Wilner, A. (2017). Cyber deterrence and critical-infrastructure protection: Expectation, application, and limitation. *Comparative Strategy*, *36*(4), 309–318. https://doi.org/10.1080/01495933.2017.1361202

Wilson, K., & Kiy, M. (2014). Some fundamental cybersecurity concepts. *IEEE Access*, *2*, 116–124. https://doi.org/10.1109/ACCESS.2014.2305658

Xu, Z., Liu, W., Huang, J., Yang, C., Lu, J., & Tan, H. (2020). Artificial intelligence for securing

IoT services in edge computing: A survey. *Security and Communication Networks*, *2020*, 1–13. https://doi.org/10.1155/2020/8872586

Yadav, G., Gauravaram, P., Jindal, A. K., & Paul, K. (2022). SmartPatch: A patch prioritization framework. *Computers in Industry*, *137*, 103595. https://doi.org/10.1016/j.compind.2021.103595

Yamin, M. M., Ullah, M., Ullah, H., & Katt, B. (2021). Weaponized AI for cyber attacks. *Journal of Information Security and Applications*, *57*, 102722. https://doi.org/10.1016/j.jisa.2020.102722

Yates, J., & Leggett, T. (2016). Qualitative research: An introduction. *Radiologic Technology*, *88*(2), 225–231. http://www.radiologictechnology.org/content/88/2/225.extract

Yin, D., Zhang, L., & Yang, K. (2018). A DDoS attack detection and mitigation with software-defined Internet of Things framework. *IEEE Access*, *6*, 24694–24705. https://doi.org/10.1109/ACCESS.2018.2831284

Yin, R. K. (2003). Designing case studies. *Qualitative Research Methods*, *5*(14), 359–386.

Yin, R. K. (2014). *Case study research: Design and methods* (5th ed.). Sage.

Yin, R. K. (2018). *Case study research and applications: Design and methods*. Sage.

Zadeh, A. H., Jeyaraj, A., & Biros, D. (2020). Characterizing cybersecurity threats to organizations in support of risk mitigation decisions. *E-Service Journal*, *12*(2), 1–34. https://doi.org/10.2979/eservicej.12.2.01

Zakaria, O., Gani, A., Mohd Nor, M., & Badrul Anuar, N. (2007). Reengineering information security culture formulation through management perspective. In *International Conference on Electrical Engineering and Informatics* (pp. 638–641).

Zeadally, S., Shaikh, F. K., Talpur, A., & Sheng, Q. Z. (2020). Design architectures for energy

harvesting in the Internet of Things. *Renewable and Sustainable Energy Reviews*, *128*, 109901. https://doi.org/10.1016/j.rser.2020.109901

Zhang, F. (2022, February 16). *When bad guys use AI and ML in cyber-attacks, what do you do?* SecurityRoundTable.org. https://www.securityroundtable.org/when-bad-guys-use-ai-and-ml-in-cyber-attacks-what-do-you-do/

Zhang, Z., Ning, H., Shi, F., Farha, F., Xu, Y., Xu, J., Zhang, F., & Choo, K. R. (2022). Artificial intelligence in cyber security: Research advances, challenges, and opportunities. *The AI Review*, *55*(2), 1029–1053. https://doi.org/10.1007/s10462-021-09976-0

Zhu, Q., & Liang, L. (2019, August). *Research on Security Vulnerabilities Based on AI*. In International Conference on Intelligent Computing (pp. 377–387). Springer, Cham.

Appendix A: Interview Questions

The Negative Impact of AI/ML on Cybersecurity.

1. Describe how can AL/ML be used maliciously by cybercriminals? Can you provide me with examples?
2. What is the size of damage an automated cyber-attack can cause compared to a traditional cyber-attack?
3. What are some types of AI/ML–powered cyber-attacks? Provide me with some examples of these attacks against technology organizations in the United States
4. What are the AI/ML tools cybercriminals and hackers employ to conduct cyber-attacks and data breaches against technology organizations?
5. Describe how AI/ML cyber threats impact a business's strategy and decision-making?
6. How did the advancement of AI technology in recent years contribute to increased data breaches in the United States?
7. How vulnerable are "no-code low-code" AI-based applications to cyber-attacks?
8. How effective are ML and deep learning technologies in increasing social engineering attacks? Provide some examples of AI-based social engineering attacks.

The Positive Impact Of AI/ML On Cybersecurity.

1. What are the advantages of AI/ML technology to cybersecurity?
2. How do technology organizations use ML algorithms to improve cybersecurity?
3. What are the ML techniques used for malware detection? Can you name some ML tools used for that purpose?
4. Can AI/ML technology be used to predict vulnerabilities in the system?

5. What are some benefits of no-code low-code AI-based applications, and how secure are these applications?
6. How does the use of AI enhance the process of vulnerability patching?
7. What can an organization's decision-makers do to prevent AI-related cyber-attacks and secure their networks from malicious activities?
8. What effective techniques can organizations implement to mitigate the risk of AI-related cyber-attacks?

Investment in AI/ML-based Technology

1. What is the importance of investing in AI technology to enhance cybersecurity in the High-Tech industry in the United States?
2. What are the challenges for technology organizations in the United States to build secure systems?
3. What is the CIO's role in investing in AI technology and making cybersecurity-related decisions?
4. What are the position titles of the decision-makers responsible for investing in AI technology in your organization?
5. What are the position titles of the decision-makers responsible for critical cybersecurity decisions in your organization?
6. What are business executives' roles in investing in AI technology?

Financial Implications

1. What is the financial impact of automated cyber-attacks and data breaches on organizations*?*
2. What is the financial impact of automated cyber-attacks and data breaches on customer*s?*

3. Who makes critical financial decisions about your organization's cyber-attacks and AI technology?

Employees Awareness

1. How do employees' awareness and compliance enhance cybersecurity in your organization?
2. What techniques does your organization use to improve employees' awareness and compliance against cyber-attacks?
3. Tell me about an example of a security violation or cyber incident in your organization resulting from a lack of employee awareness.
4. Tell me an example of when employee awareness and compliance prevented a security violation or cyber incident in your organization.

AI Governance

1. What is the current level of governance regarding access to open-source AI-based tools in the United States? Do you think there is a need for more governance, and why?
2. What are some open-source AI tools that have the potential to automate cyber-attacks?
3. How will the governance of open-source AI-based tools affect the future of automated cyber-attacks and data breaches against organizations?

AI Deterrence

1. From your experience, describe the most effective ways to deter cyber-attacks?
2. What are some techniques to deter hackers and cybercriminals from initiating a cyber-attack?
3. How do governance and control of the public use of AI can enhance cyber deterrence?
4. How cost-effective it is to deter a cyber-attack before it occurs versus fighting it after its occurrence.

5. How does the security team's effectiveness contribute to deterring and preventing cyber-attacks?

Cloud Computing and IoT

1. How to enhance cloud security using AI/ML technology?
2. What are the threats of AI/ML technology the cloud security?
3. Describe how to reduce the attack surface of IoT using AI/ML technology?
4. What are the threats of AI/ML technology on the internet of things?

Probing Questions

1. Do you mind elaborating more on your answer?
2. That’s interesting; please continue.
3. Would you tell me more about that?
4. Can you provide me some examples?
5. Has it helped? Why or why not?
6. Can you clarify your answer more?

Appendix B: IRB Approval Letter

May 3, 2023

Mustafa Abdulhussein
Dennis Backherms

Re: IRB Exemption - IRB-FY22-23-1300 The impact of AI and ML on Organizations' Cybersecurity

Dear Mustafa Abdulhussein, Dennis Backherms,

The Liberty University Institutional Review Board (IRB) has reviewed your application in accordance with the Office for Human Research Protections (OHRP) and Food and Drug Administration (FDA) regulations and finds your study to be exempt from further IRB review. This means you may begin your research with the data safeguarding methods mentioned in your approved application, and no further IRB oversight is required.
Your study falls under the following exemption category, which identifies specific situations in which human participants research is exempt from the policy set forth in 45 CFR 46:104(d):

Category 2.(iii). Research that only includes interactions involving educational tests (cognitive, diagnostic, aptitude, achievement), survey procedures, interview procedures, or observation of public behavior (including visual or auditory recording) if at one of the following criteria is met: The information obtained is recorded by the investigator in such a manner that the identity of the human subjects can readily be ascertained, directly or through identifiers linked to the subjects, and an IRB conducts a limited IRB review to make the determination required by §46.111(a)(7).

Your stamped consent form(s) and final versions of your study documents can be found under the Attachments tab within the Submission Details section of your study on Cayuse IRB. Your stamped consent form(s) should be copied and used to gain the consent of your research participants. If you plan to provide your consent information electronically, the contents of the attached consent document(s) should be made available without alteration.

Please note that this exemption only applies to your current research application, and any modifications to your protocol must be reported to the Liberty University IRB for verification of continued exemption status. You may report these changes by completing a modification submission through your Cayuse IRB account.

If you have any questions about this exemption or need assistance in determining whether possible modifications to your protocol would change your exemption status, please email us at irb@liberty.edu.

Sincerely,
G. Michele Baker, PhD, CIP
Administrative Chair
Research Ethics Office

Appendix C: Informed Consent

Title of the Project: The impact of AI and ML on Organizations cybersecurity

Principal Investigator: Mustafa Abdulhussein. Doctoral Candidate, School of Business, Liberty University.

Invitation to be Part of a Research Study

You are invited to participate in a research study. To participate, you must be 23 years of age or older, an Information Technology professional with a minimum of two years' experience and have knowledge in cybersecurity and AI technology and trends. Taking part in this research project is voluntary.

Please take time to read this entire form and ask questions before deciding whether to take part in this research.

What is the study about and why is it being done?

The purpose of the study is to explore the malicious use of AI and ML to conduct AI-powered cyber-attacks against the technology organizations in the United States. The study aims to discover the dark side of AI in cybersecurity, and defensive tactics that should be employed by organizations to reduce the risk of automated cyber-attacks.

What will happen if you take part in this study?

If you agree to be in this study, I will ask you to do the following:

1. Participate in a telephonic, audio-recorded interview that will take no more than 45 minutes.
2. Participate in a 15-mins audio-recorded member checking session to review the interview transcripts and check for accuracy and confirm agreement.

How could you or others benefit from this study?

Participants should not expect to receive a direct benefit from taking part in this study. However, your participation will contribute to the benefit of society by helping the researcher to understand the potential risk of misusing AI technology to conduct cyber-attacks on technology organizations that provide various products and services to other sectors in the United States. Which may have implications for securing customers' data from data breaches and saving organizations from potential financial and reputational damages. The insights you provide to this study will add new knowledge to the academic literature in a fairly new – rapidly growing technology like AI and ML. Additionally, by participating in this study, you may have the opportunity to reflect on your own experiences and insights related to the use of AI and ML in the cybersecurity field.

What risks might you experience from being in this study?

The expected risks from participating in this study are minimal, which means they are equal to the risks you would encounter in everyday life.

How will personal information be protected?

The records of this study will be kept private. Published reports will not include any information that will make it possible to identify a subject. Research records will be stored securely, and only the researcher will have access to the records.

- Participant responses to the interview questions will be anonymous. All personal information collected during the study will be kept confidential by replacing names with pseudonyms to protect your identity. The researcher will take measures to ensure that your identity and any personal information you provide will remain anonymous. Any information that could potentially identify you will be removed from the transcripts.
- Interviews will be conducted in a location where others will not easily overhear the conversation.
- Data will be stored on a password locked computer. After three years, all electronic records will be deleted.
- Recordings will be stored on a password-locked computer until participants have reviewed and confirmed the accuracy of the transcripts and then erased. Only the researcher will have access to these recordings.

How will you be compensated for being part of the study?

Participants will not be compensated for participating in this study.

Is study participation voluntary?

Participation in this study is voluntary. Your decision whether to participate will not affect your current or future relations with Liberty University. If you decide to participate, you are free to not answer any question or withdraw at any time without affecting those relationships.

What should you do if you decide to withdraw from the study?

If you choose to withdraw from the study, please contact the researcher at the email address/phone number included in the next paragraph. Should you choose to withdraw, data collected from you will be destroyed immediately and will not be included in this study.

Whom do you contact if you have questions or concerns about the study?

The researcher conducting this study is Mustafa Abdulhussein. You may ask any questions you have now. If you have questions later, **you are encouraged** to contact him at xxx-xxx-xxxx or xxxxxxxxx@liberty.edu. You may also contact the researcher's faculty sponsor, Dr. Dennis Backherms, at email: xxxxxxxx@liberty.edu.

Whom do you contact if you have questions about your rights as a research participant?

If you have any questions or concerns regarding this study and would like to talk to someone other than the researcher, **you are encouraged** to contact the IRB. Our physical address is Institutional Review Board, 1971 University Blvd., Green Hall Ste. 2845, Lynchburg, VA, 24515; our phone number is 434-592-5530, and our email address is irb@liberty.edu.

Disclaimer: The Institutional Review Board (IRB) is tasked with ensuring that human subjects research will be conducted in an ethical manner as defined and required by federal regulations. The topics covered and viewpoints expressed or alluded to by student and faculty researchers are those of the researchers and do not necessarily reflect the official policies or positions of Liberty University.

Your Consent

By signing this document, you are agreeing to be in this study. Make sure you understand what the study is about before you sign. You will be given a copy of this document for your records. The researcher will keep a copy with the study records. If you have any questions about the study after you sign this document, you can contact the study team using the information provided above.

I have read and understood the above information. I have asked questions and have received answers. I consent to participate in the study.

☐ The researcher has my permission to audio-record me as part of my participation in this study.

_____
Printed Subject Name

_____
Signature & Date