FLORIDA INTERNATIONAL UNIVERSITY

Miami, Florida

CYBERSECURITY PROTECTION BEHAVIOR AMONG US MILITARY VETERANS IN WHITE-COLLAR JOBS

A dissertation submitted in partial fulfillment of

the requirements for the degree of

DOCTOR OF BUSINESS ADMINISTRATION

by

Alex A. Djahankhah

2024

To: Dean William G. Hardin
College of Business

This dissertation, written by Alex A. Djahankhah, and entitled Cybersecurity Protection Behavior among US Military Veterans in White Collar Jobs, having been approved in respect to style and intellectual content, is referred to you for judgment.

We have read this dissertation and recommend that it be approved.

Manjul Gupta

Mark Thibodeau

Mido Chang

Amin Shoja, Major Professor

Date of Defense: May 10, 2024

The dissertation of Alex A. Djahankhah is approved.

Dean William G. Hardin
College of Business

Andrés G. Gil
Senior Vice President for Research and Economic Development
and Dean of the University Graduate School

Florida International University, 2024

DEDICATION

I dedicate this research to my wife for supporting me through my journeys and being a strong mother to our children.

… To my daughters Celeste and Charlotte, for being a part of every decision I make, Daddy loves you, you are my strength...

… To all the US Servicemembers and their families overseas away from home, risking their lives, protecting national interests, and keeping the American spirit alive and well.

ACKNOWLEDGMENTS

The FIU professors and staff that inspired me every day in every engagement and worked with me through this advancement in life.

ABSTRACT OF THE DISSERTATION

CYBERSECURITY PROTECTION BEHAVIOR AMONG US MILITARY VETERANS IN WHITE-COLLAR JOBS

by

Alex A. Djahankhah

Florida International University, 2024

Miami, Florida

Professor Amin Shoja, Major Professor

The rapid growth of cyber threats and attacks necessitates an in-depth examination of individuals' intentions and behaviors regarding cybersecurity. Despite increasing awareness and education about the potential risks, many individuals fail to engage in secure online practices. As veterans enter the job market, they bring in a unique set of experiences and attitudes that may be applied to the cybersecurity stance of an organization. Veterans' perceived ability to communicate and respond to incidents from working environments where risk tolerance is low and security from state actors is a high priority transfer to their behaviors on their organization's network.

An online survey study with a quasi-experimental design was used to observe the units of analysis under natural conditions, without deliberate manipulation, a control group, or random assignment, to explore the strength of the variances for the population.

The results showed that the model was a proper fit; thus, its findings could be relied upon. Of the (7) proposed hypotheses, (4) were supported. Primarily, a military veteran has a significant ability to conduct a threat appraisal. They know how vulnerable they are and can understand how severe a cyber attack can be. Dealing with adversarial threats daily and training in general cyber security awareness while serving has helped them better understand their environment.

A veteran employee’s response efficacy (compliance with IS security policies) and self-efficacy (belief that they can successfully comply with IS security policies) do not contribute to their cybersecurity intentions to protect the information and technology resources of the organization from potential security breaches. Veterans, particularly those who have served in combat roles, have faced real and immediate threats. This exposure might alter their perception of coping in civilian contexts, making theoretical or less immediate threats seem less significant or urgent.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

FIGURE PAGE

CHAPTER I: INTRODUCTION

Problem Statement

The rapid growth of cyber threats and attacks necessitates an in-depth examination of individuals' intentions and behaviors regarding cybersecurity. Despite increasing awareness and education about the potential risks, many individuals fail to engage in secure online practices. This intention-behavior gap poses a significant challenge for organizations and individuals seeking to protect themselves from cyber threats. This problem statement aims to identify the factors contributing to the intention-behavior gap and propose strategies to mitigate this critical cybersecurity challenge.

On April 29, 2021, hackers entered the networks of Colonial Pipeline Co., the largest fuel pipeline in the U.S. The Colonial Pipeline, spanning 5,500 miles, is a critical infrastructure that transports gasoline, diesel, and jet fuel, supplying approximately 45% of the East Coast's fuel needs. Hackers shut it down for six days through a virtual private network account (VPN), which allowed employees to access the company's computer network remotely. The VPN account did not use multifactor authentication. Hackers discovered the account's password inside a batch of leaked passwords on the dark web; this means a Colonial employee may have used the same password on another previously hacked account.

Bloomberg reported that Colonial paid the hackers, affiliates of a Russia-linked cybercrime group known as DarkSide, 75 Bitcoin (valued at approximately $4.4 million at the time) to the attackers to regain access to their systems. This decision was controversial, raising concerns about encouraging future ransomware attacks. Colonial

Pipeline was forced to shut down its entire pipeline system to contain the breach. This precaution was to prevent the spread of ransomware and safeguard critical operational systems. The shutdown lasted several days, causing widespread fuel shortages and panic buying in several states. The hackers also stole nearly 100 gigabytes of data from Colonial Pipeline and threatened to leak it if Colonial Pipeline did not pay the ransom. The shutdown led to panic buying of gasoline, resulting in fuel shortages and long lines at gas stations across the affected regions. This event highlighted the vulnerability of critical infrastructure to cyberattacks and raised awareness about the need for improved cybersecurity measures in such sectors. The attack had international implications, demonstrating how cybercriminals could disrupt critical infrastructure and economies. It also increased global dialogue on cybersecurity and the need for international cooperation to combat cyber threats.

In 2009, AT&T's Ed Amoroso testified before the U.S. Congress that global cybercrime profits topped $1 trillion, 1.6% of the world GDP. (Anderson et al., 2013). The figure does not include the cost of cybersecurity defense, which companies plan at or below the cost of an incident. Private companies are susceptible to cybercrime due to competing resources between core business functions and cyber defense. According to CyberSeek, an initiative funded by the National Initiative for Cybersecurity Education (NICE), the United States faced a shortfall of almost 314,000 cybersecurity professionals as of January 2019, while the current workforce sits at ~716,000 (Crumpler & Lewis, 2019). The Colonial Pipeline incident served as a wake-up call for many organizations, emphasizing the importance of robust cybersecurity practices, regular backups, employee training on cyber threats, and having a response plan for cyber incidents.

Significance of the Problem

With the proliferation of technology and the increasing reliance on digital systems, the significance of cybersecurity has become paramount. While technological advancements have facilitated various aspects of our lives, they have also given rise to new vulnerabilities and cyber threats. Poor cybersecurity intentions among individuals can have far-reaching implications, compromising personal privacy, organizational security, and national interests.

As societies and economies increasingly digitalized, the reliance on technology in everyday life and business operations has skyrocketed. This makes cybersecurity crucial for protecting sensitive information, ensuring the smooth functioning of systems, and maintaining public trust in digital services. Cyber threats are becoming more sophisticated, with attackers using advanced techniques to exploit vulnerabilities. This includes the rise of state-sponsored attacks, advanced persistent threats (APTs), ransomware, and phishing attacks. The complexity of these threats requires robust and evolving cybersecurity measures. Vital sectors such as energy, healthcare, finance, and transportation rely heavily on digital systems. Cyberattacks on these sectors can have severe consequences, including service disruptions, financial loss, and threats to national security and public safety, as exemplified by incidents like the Colonial Pipeline ransomware attack.

In an interconnected world, cybersecurity is not just a local or national concern but a global one. Cyberattacks can easily cross borders, and nations increasingly recognize cyber warfare as a significant component of national security strategies. With the increasing amount of personal data being collected and stored by organizations, there is a heightened focus on data privacy. Regulations such as the EU's General Data Protection Regulation (GDPR) and various data protection laws globally make cybersecurity a legal requirement to protect consumer data.

Cybersecurity incidents can have a significant economic impact, from the direct costs of responding to breaches to the indirect costs such as reputational damage and loss of consumer trust. Companies are increasingly investing in cybersecurity to mitigate these risks. Emerging technologies like the Internet of Things (IoT), artificial intelligence (AI), and 5G networks create new opportunities and introduce new vulnerabilities and attack surfaces. Ensuring the security of these technologies is critical.

The shift to remote work, accelerated by the COVID-19 pandemic, has expanded the cybersecurity perimeter for many organizations. This has led to increased challenges in securing remote access, managing bring-your-own-device (BYOD) policies, and protecting against threats that target remote workers. As cyber threats become more prevalent, there is a growing recognition of the importance of cybersecurity awareness and education at all levels – from individual users to high-level decision-makers in organizations. The demand for skilled cybersecurity professionals continues to outpace supply, highlighting the need for education and training to address this critical skills gap.

At the individual level, poor cybersecurity intentions can lead to devastating consequences. Negligent behavior, such as weak password management, clicking on suspicious links, or falling victim to phishing attempts, can result in identity theft, financial loss, and personal privacy breaches. Research suggests that individuals with low cybersecurity intentions are more susceptible to cyber-attacks and are less likely to adopt preventive measures (Safa & Von Solms, 2016). Understanding the motivations and attitudes underpinning poor cybersecurity intentions is crucial for designing effective awareness campaigns and interventions to promote safe online practices among individuals.

Large and small organizations are frequent targets of cyber-attacks due to the potential financial gain and the value of their sensitive data. Poor cybersecurity intentions within an organization can result in data breaches, intellectual property theft, and reputational damage. Literature indicates that employees' lack of intent to comply with security policies, such as sharing passwords or downloading unauthorized software, significantly increases the organization's vulnerability to cyber threats (Doherty & Tajuddin, 2018). Fostering a security-conscious culture and providing robust training programs are essential to mitigate the risk of poor cybersecurity intentions among employees.

In addition to individual and organizational consequences, poor cybersecurity intentions have implications for national security. Governments and nations increasingly rely on interconnected digital systems for critical infrastructure, defense networks, and communication channels. The emergence of state-sponsored cyber warfare and espionage underscores the importance of ensuring robust cybersecurity practices at a national level. McCombie, S. (2020) emphasizes that citizens' intentions to engage in secure online behavior and support national cybersecurity initiatives are vital for safeguarding a nation's interests in cyberspace (McCombie et al., 2020).

In 2012, the Nextgov newsletter reported that the Pentagon and the National Nuclear Security Administration each received approximately ten million attempted network intrusions or cyber-attacks per day (Armitage et al., 2016). Job demand in cybersecurity is so high that applicants with just one completed cybersecurity certification have been known to get jobs there. Under the IT umbrella, working in cybersecurity can be physically demanding and stressful based on how much risk the organization is willing to assume. Military veterans, especially combat veterans, are fond of stressful environments and make excellent candidates for high job demands. Cybersecurity investment must be worth the liability and be less than the assets it is meant to protect. Unfortunately, cybersecurity and IT are typically the first budget-cut targets, and organizational leadership assumes more risk. Therefore, companies should avoid a high turnover rate in cybersecurity because seasoned employees tend to understand better the organization's network architecture and how to protect it.

The significance of poor cybersecurity intentions must be addressed in today's interconnected world. Individual-level implications, organizational consequences, and national security considerations emphasize the urgency of addressing this issue. By understanding the underlying motivations and challenges associated with poor cybersecurity intentions, policymakers, educators, and cybersecurity professionals can develop targeted interventions to promote secure online practices. Ultimately, fostering a culture of cybersecurity consciousness and will is crucial for ensuring a safer digital environment for individuals, organizations, and nations. Cybersecurity today is not just a technical issue but a fundamental aspect of how modern societies and economies operate and protect themselves. It is a field that demands continuous innovation, awareness, and collaboration to stay ahead of emerging threats.

Research Gap

There seems to be limited direct academic research explicitly addressing the gap between military veterans and cybersecurity behavior. This could be due to the novelty of this specific research area or the limited public availability of such studies. As veterans transition from military to civilian life, many start new businesses and seek new career opportunities in various sectors. The field of cybersecurity presents a promising avenue for veterans, given their strong backgrounds in discipline, leadership, and problem-solving. However, despite their potential aptitude, there is a noticeable research gap in understanding veterans' intentions and motivations in pursuing careers with cybersecurity in mind.

One prominent reason for the research gap is the need for more comprehensive studies focusing on veterans' cybersecurity intentions. While research on cybersecurity and career intentions exists, it often fails to address veterans' unique experiences, skill sets, and motivations. Consequently, this gap limits our understanding of veterans' attitudes and inhibits the development of targeted strategies to engage them effectively in cybersecurity careers.

Veterans have an inherent cybersecurity preparedness, especially combat veterans, who have experience with risk and adapting to tricky situations and unknown threats, and are believed to be better suited than the civilian population to deal with the threat landscape of cybersecurity (Dupuis & Weiss, 2019). Veterans excel in the soft skills required in cybersecurity; Julian Meyrick, head of IBM's Security Division in Europe, stated, "Anybody who has worked in the operations center in a warship, in a military unit, or an RAF station is going to have much experience in both dealing with incidents and training to deal with incidents. I think for me taking veterans and turning them into cyber operators is typically something relatively easy to do. They frequently have many soft skills that are essentially difficult to train people for." (Guenole et al., 2018).

Transitioning from military to civilian life can be daunting, and veterans face numerous challenges. While there is existing research on veterans' transition experiences, there needs to be more focus on the specific hurdles they encounter in pursuing cybersecurity careers. Factors such as a lack of awareness about available opportunities, limited access to relevant information and resources, and the absence of tailored support programs may contribute to the research gap in understanding veterans' cybersecurity intentions.

According to the Department of Labor, there are 8,918,000 military veterans in the US civilian workforce, making up 5.6% of the total workforce. Military veterans understand risk management, and many hold or have held security clearances that include background checks and security training, making them desirable cybersecurity workers. Veterans possess various valuable skills gained during their military service, such as problem-solving, teamwork, and adaptability. However, translating these skills into the civilian job market, particularly in the context of cybersecurity, may need to be revised.

The research gap exists in understanding how veterans perceive and articulate their skills in the cybersecurity domain.

Additionally, the need for clarity regarding certifications and qualifications required for cybersecurity roles may deter veterans from pursuing careers in this field. However, many service members are still afforded cybersecurity training; complimentary free training in industry-recognized IT certifications is still available. Veteran status means they have ongoing access to continuing education and training. (Merritt, 2020). Servicemembers must undergo transition programs to help them transition from the military to the general workforce. The transition programs help them translate their military experience to looked-for civilian work skills.

Veterans often face mental health challenges stemming from their military experiences. Issues such as post-traumatic stress disorder (PTSD), depression, and anxiety can impact their career choices and intentions. While mental health research within the veteran population is well-established, there is a lack of research investigating the relationship between mental health and veterans' cybersecurity intentions. Understanding how cognitive health factors influence veterans' decisions regarding cybersecurity careers could help develop targeted interventions and support systems.

Research Questions

As veterans enter the job market, they bring a unique set of experiences and attitudes that may be applied to an organization's cybersecurity stance. Veterans' perceived ability to communicate and respond to incidents from working environments where risk tolerance is low and security from state actors is a high priority transfer to their behaviors on their organization's network. *What are the contributing factors toward cybersecurity protection behaviors among US military veterans in white-collar jobs?*

Research Contributions

Applying PMT within the context of cybersecurity intention among veterans presents a promising avenue for research. This study can provide insights into veterans' threat perceptions in the digital domain. Examining their perceptions of the severity and vulnerability of cyber threats can help tailor interventions and educational programs to address specific concerns. Veterans are often driven by their support for a shared “mission” and are instilled with solid values and ethics (Merritt, 2020). Veteran networks and groups provide a pool of employable individuals. Organizations with cybersecurity positions experience high turnover, while veterans prefer team environments and are “company loyal” (Merritt, 2020). Some veterans may experience post-traumatic stress disorder (PTSD) from military service. Understanding the impact of PTSD on veterans' cybersecurity intentions is crucial for designing tailored interventions and support systems that account for their unique needs.

Investigating veterans' self-efficacy beliefs regarding cybersecurity practices can contribute to understanding their intention to engage in protective behaviors. By identifying the factors that enhance or hinder self-efficacy, researchers can design interventions to boost veterans' confidence in their ability to protect themselves and others from cyber threats.

Studying veterans' beliefs in the effectiveness of various cybersecurity measures can shed light on the role of response efficacy in their intention to adopt protective behaviors. Understanding the perceived effectiveness of different security measures can guide the development of interventions that align with veterans' preferences and promote their engagement in cybersecurity practices.

The findings from this study can inform the design of tailored interventions. By considering veterans' threat perceptions, self-efficacy beliefs, and the perceived effectiveness of cybersecurity measures, interventions can be customized to address their unique needs and motivations.

The intersection of veterans and cybersecurity intention presents a unique research area with significant implications for the military community and cybersecurity. The values and sense of mission instilled in veterans can motivate them to contribute to national security even after leaving the military. This dedication can translate into a solid intention to engage in cybersecurity practices to safeguard critical infrastructure and sensitive information.

CHAPTER II: BACKGROUND LITERATURE REVIEW AND THEORY

Cybersecurity Environment

Cybersecurity encompasses various technical and social considerations for safeguarding networked information systems. The significance of this concept has grown substantially due to the widespread transition of governmental, business, and day-to-day activities into the online realm. Since 2003, it has gained prominence across various academic and mainstream domains, including software engineering, international relations, crisis management, and public safety. This prominence has gradually supplanted more technical terms like computer/system/data security (prevailing in the 1970s/1980s) and information security (prevalent since the mid-1990s). However, despite its expanding influence, concerns have emerged regarding its strong association with national security and defense agencies, raising questions about the potential inappropriate securitization of government programs.

In the information age, accelerated by the COVID-19 pandemic, more work is occurring on connected devices, which has created opportunities for malicious actors to intrude on the company's networks for malicious reasons. Malicious actors, including state actors and cyber terrorists, make large organizations a prime target. A cybersecurity threat is the threat of a malicious attack by an individual or organization attempting to access a network to corrupt data or steal confidential information (Li et al., 2022). Organizations initiate cybersecurity awareness and training programs to disseminate information that all organization users need and communicate security requirements and appropriate behavior (Bada et al., 2019). The United States faces numerous challenges in safeguarding its digital infrastructure from cyber threats in today's interconnected world. Cybersecurity has become a critical concern due to cyberattacks' increasing frequency, sophistication, and impact.

The NICE (National Initiative for Cybersecurity Education) framework is a comprehensive resource developed by the National Institute of Standards and Technology (NIST) to enhance the overall cybersecurity posture in the United States. It provides a common language to categorize and describe the different roles and responsibilities within the cybersecurity workforce. The NICE framework is organized into several components, including categories, specialty areas, work roles, knowledge, skills, and abilities (KSAs). Work Roles define specific cybersecurity functions, and each role is associated with a set of KSAs. These roles include analyzing cyber threats, developing secure software, and managing cybersecurity policies.

The framework is a valuable tool for organizations to identify, recruit, develop, and retain a skilled cybersecurity workforce. It helps standardize job descriptions, clarify skills requirements, and promote a common understanding of the various roles in the field of cybersecurity. The NICE framework is widely used by government agencies, private sector organizations, and educational institutions to align their cybersecurity workforce strategies with industry best practices (Petersen et al., 2020).

One key area of investigation is the identification and analysis of the evolving threat landscape. Studies (Smith & Rupp, 2002) and (Johnson et al., 2022) have explored the nature of cyber threats and the tactics employed by cybercriminals. These studies provide valuable insights into attackers' tactics, techniques, and procedures, helping organizations better understand the risks they face. Identifying and analyzing the evolving threat landscape in cybersecurity is critical to maintaining robust digital defense mechanisms. As technology advances, so do the strategies employed by malicious actors, necessitating continuous assessment and adaptation of cybersecurity measures. This comprehensive process involves scrutinizing emerging threats, understanding their characteristics, and implementing effective countermeasures.

Cybersecurity experts develop and implement proactive defense strategies for the identified threats. This involves the creation of robust incident response plans, the deployment of intrusion detection systems, and the continuous updating of security protocols. Additionally, organizations invest in employee training programs to enhance awareness and resilience against social engineering attacks.

Another focus area is the vulnerabilities present in critical systems. Researchers have examined vulnerabilities in various domains, such as healthcare, finance, and transportation. For example, Veale and Brown studied the vulnerabilities in healthcare systems and proposed strategies to enhance cybersecurity in the healthcare industry. Identifying and understanding vulnerabilities in critical systems constitute a paramount aspect of cybersecurity, as these systems underpin essential functions in various sectors, including energy, healthcare, finance, and transportation (Veale & Brown, 2020). A comprehensive exploration of these vulnerabilities reveals the potential weaknesses that malicious actors could exploit, posing significant risks to national security and public safety.

Critical systems encompass various infrastructures, including supervisory control and data acquisition (SCADA) systems, industrial control systems (ICS), and other interconnected networks that manage and control essential processes. One prominent vulnerability lies in their increasing connectivity to the Internet, making them susceptible to cyber threats from various sources (Hentea, 2008). Hentea emphasized the need for robust cybersecurity measures and policies to protect these essential infrastructures.

Older software and hardware are among the vulnerabilities prevalent in critical systems. Many critical infrastructures still rely on legacy systems that may no longer receive security updates, exposing them to known exploits. This challenge is compounded by the reluctance or difficulty in updating these systems due to concerns about operational disruptions or the high costs associated with modernization. Savin found that continued use of outdated software and hardware in essential systems poses significant security risks. They also address the challenges of updating these systems, including operational disruptions and high costs, which deter organizations from modernizing their infrastructure (Savin & Anysz, 2021).

Another vulnerability arises from insufficient security measures in designing and implementing critical systems. In some cases, security considerations might have been secondary during the development phase, leading to weaknesses that adversaries can exploit. Common issues include default passwords, inadequate encryption protocols, and insufficient access controls, which, if not addressed, can compromise the integrity and confidentiality of critical infrastructure. Stamp et. al found that these vulnerabilities often stem from a lack of emphasis on security during the design and implementation phases of these systems, which adversaries can exploit to compromise the integrity and confidentiality of critical infrastructure (Stamp et al., 2003). In addition to unintentional errors, malicious insider threats pose a considerable risk. Employees with access to sensitive data or critical systems may intentionally engage in activities that compromise security, necessitating measures such as access controls, monitoring, and incident response plans to detect and mitigate insider threats effectively.

The convergence of information technology (IT) and operational technology (OT) in critical systems introduces additional vulnerabilities. Traditionally isolated from external networks, critical infrastructure systems are increasingly connected to IT networks for improved efficiency and data analytics. However, this integration poses risks as cyber threats can potentially traverse between IT and OT networks, disrupting operations and causing cascading effects (Ray et al., 2011). Addressing vulnerabilities in critical systems demands a multifaceted approach. Regular security assessments, penetration testing, and vulnerability scans are crucial for identifying weaknesses. Additionally, implementing a robust patch management strategy, updating legacy systems, and enhancing employee cybersecurity awareness are essential to mitigating risks.

Social engineering attacks represent another vector for exploiting vulnerabilities in critical systems. Phishing attempts, for instance, could target personnel with access to critical infrastructure, aiming to gain unauthorized entry or compromise sensitive information. Critical systems are vulnerable due to human errors and insufficient training. Attackers exploit these weaknesses to gain unauthorized access to sensitive information and advocated for comprehensive training programs and awareness campaigns to mitigate these risks, emphasizing the need for robust security measures to design and implement critical infrastructure systems. Employees may resist security measures if they perceive them as cumbersome or hindering productivity. Balancing security requirements with user experience is crucial to ensuring that individuals are more likely to adhere to security protocols.

Studies have examined the role of employees in cybersecurity incidents and the importance of their awareness and behavior. For instance, Nobles explored the impact of employee awareness and training on organizations' cybersecurity posture. His findings emphasize the significance of educating and empowering employees to recognize and respond to cyber threats (Nobles, 2018). The human factor in cybersecurity represents a critical and often unpredictable element in the defense against cyber threats. This multifaceted aspect involves individuals' behavior, actions, and decision-making within an organization, acknowledging that human actions can significantly impact the overall security posture. Understanding and addressing the human factor is essential for creating effective cybersecurity strategies that account for technical vulnerabilities and human behaviors.

Reeves (2021) found that cybersecurity fatigue can result from overexposure to workplace cybersecurity advice (e.g., training) or cybersecurity actions (e.g., forced password updates). He suggests that practitioners should determine whether the advice or cyber security action has tired the employees and whether the disengagement is attitudinal, cognitive, or a combination of both (Reeves et al., 2021).

Moreover, the human factor extends to incident response and recovery. How individuals respond to a cybersecurity incident, communicate within the organization, and collaborate with security teams can impact the effectiveness of resolving and mitigating an attack's consequences (Corman, 2023).

Cultural aspects within an organization contribute to the human factor in cybersecurity. A security-aware culture fosters a collective understanding of the importance of cybersecurity, encouraging employees to prioritize security in their daily activities. Leadership support and a positive security culture can significantly enhance an organization's resilience against cyber threats. Fostering a security-aware culture contributes to a collective understanding of cybersecurity's importance, encouraging employees to embed security practices into their daily routines. Leadership support and promoting a positive security culture are crucial for enhancing an organization's resilience against cyber threats (Triplett, 2021).

The cyber threat landscape in America is marked by a diverse range of adversaries, including nation-states, organized criminal groups, hacktivists, and individual hackers. These actors employ phishing, ransomware, distributed denial-of-service (DDoS) attacks, and advanced persistent threats (APTs) to exploit vulnerabilities and gain unauthorized access to sensitive information. Cyber espionage, intellectual property theft, and disruption of critical infrastructure are among the primary concerns. Research (Chou et al., 2011) emphasizes the association between access to technology (such as the Internet) and vulnerabilities stemming from socio-demographics, health status, and health literacy levels. This research highlights how disparities in access can perpetuate vulnerabilities for specific populations.

The U.S. government has recognized the significance of cybersecurity and has implemented several policies and regulations to mitigate threats. The Cybersecurity and Infrastructure Security Agency (CISA) is crucial in coordinating cybersecurity efforts, sharing information, and facilitating incident response across federal, state, local, tribal, and territorial governments. Implementing frameworks like the National Institute of Standards and Technology (NIST) Cybersecurity Framework guides organizations in enhancing their cybersecurity posture.

Addressing the complex nature of cybersecurity threats requires collaborative efforts between the public and private sectors. Public-private partnerships have emerged as crucial mechanisms for information sharing, threat intelligence exchange, and joint initiatives to enhance resilience. Collaborative initiatives, such as sharing best practices, promoting cybersecurity education, and fostering research and development, contribute to a more robust cybersecurity ecosystem. The cybersecurity environment in America presents significant challenges due to the evolving threat landscape and vulnerabilities in critical systems (He et al., 2018).

R. Banham highlights that mid-sized and small businesses are increasingly targeted due to their often inadequate cybersecurity measures compared to more giant corporations. Banham discusses various types of threats, including malware, phishing, and ransomware, which have become more sophisticated and prevalent (Banham, 2017). His study emphasized the critical need for robust cybersecurity policies tailored to the specific vulnerabilities of smaller businesses. He also outlines key components of effective cybersecurity strategies, such as regular risk assessments, employee training, and the implementation of comprehensive security protocols, arguing that proactive cybersecurity measures are essential for smaller businesses to mitigate risks, protect sensitive data, and ensure business continuity in an increasingly digital economy.

Atkins and Lawson argue that while some sectors, notably those with significant government oversight and military involvement, have developed robust cybersecurity measures, others lag due to insufficient policy enforcement and lack of standardized practices (Atkins & Lawson, 2021). These authors identified vital factors influencing policy effectiveness, including regulatory environment, sector-specific vulnerabilities, and integrating cyber defense strategies with traditional security measures. Their paper concludes by calling for a more cohesive and adaptive policy approach to enhance the resilience of critical infrastructure against cyber threats, stressing the importance of continuous evaluation and updating of cybersecurity policies to keep pace with evolving threats.

Protection Motivation Theory (PMT)

Protection Motivation Theory (PMT) is a psychological framework that explains and predicts individuals' responses to threats and their engagement in protective behaviors (Rogers, 1975). PMT was developed to understand fear appeals in the context of health behaviors. PMT has since been applied to various domains, including cybersecurity, climate change, and public health. PMT suggests that past behavior strongly influences assessing threats and one's ability to cope with them (Vance 2012).

PMT proposes that motivation to self-protect from risks emerges from (1) perceived severity, (2) perceived vulnerability, and (3) perceived response efficacy; and to explain failing to engage in protective behaviors, three cognitive appraisals: (4) self-efficacy, (5) response costs and (6) rewards associated with risky behavior (Maddux & Rogers, 1983). These appraisals collectively shape an individual's motivation to engage in protective actions. PMT can be applied to investigate how veterans' threat perception and response perception regarding cybersecurity impact their compliance behaviors.

PMT has been applied in healthcare, psychology, information technology, and others. The variables of PMT are split between threat and coping appraisals. Threat appraisal measures how someone will perceive a threat, primarily through a subject's perceived vulnerability, perceived severity, and motivation to keep unwanted behavior as rewards or benefits. Higher perceived severity increases individuals' motivation to protect themselves (Floyd et al., 2000). Vulnerability, on the other hand, refers to the perceived likelihood of experiencing the threat. Higher perceived vulnerability enhances the motivation to engage in protective behaviors. Coping appraisal in our context measures the perception of protective responses against cybersecurity threats. Coping appraisal focuses on individuals evaluating their ability to respond to a threat effectively. It includes two main components: response efficacy and self-efficacy. Response efficacy is the belief that the recommended protective actions will effectively reduce or eliminate the threat. Higher response efficacy enhances individuals' motivation to adopt protective behaviors (Milne et al., 2000). Self-efficacy refers to confidence in one's ability to perform the recommended protective actions successfully. Higher self-efficacy increases the likelihood of engaging in protective behaviors.

PMT has been applied in cybersecurity to understand individuals' intentions and behaviors regarding protecting themselves from online threats. Research has shown that threat appraisal factors, such as cyberattacks' perceived severity and vulnerability to online risks, influence individuals' motivation to adopt protective measures (Anderson & Agarwal, 2010). Coping appraisal factors, including perceived response efficacy of security measures and self-efficacy in implementing them, also play a crucial role in shaping individuals' intentions to engage in cybersecurity behaviors (Mathieson, 1991).

Li (2022) found that the coping appraisal process is the most important mediator for employees’ cybersecurity protection action. Li (2022) also notes that employees who are aware of their organization’s cybersecurity policy behave significantly differently than employees who are unaware or employees of organizations with no security policy (Li et al., 2022). A proper information security policy is vigorously developed and creates a process that helps educate and maintain employees’ awareness to implement the existing security policy.

Understanding the components of PMT provides insights into strategies for promoting protective actions. Messages and interventions should focus on enhancing threat appraisal by emphasizing the severity and vulnerability of the threat. Providing clear and effective information about the recommended protective actions can strengthen response efficacy. Additionally, interventions should increase individuals' self-efficacy by providing resources, training, and support to enhance their confidence in executing protective behaviors (Maddux & Rogers, 1983).

Protection Motivation Theory provides a valuable framework for understanding individuals' motivation to engage in protective behaviors in the face of threats. By considering threat appraisal and coping appraisal factors, we can design effective interventions to promote protective actions in various domains, including cybersecurity, public health, and climate change. Understanding human behavior and motivation complexities is essential for developing strategies encouraging individuals to adopt protective behaviors and safeguard their well-being.

How individuals perceive risks in the online environment affects their intentions and subsequent behaviors. Studies have shown that individuals tend to underestimate the severity and likelihood of cyber threats, leading to complacency and a reduced motivation to engage in secure practices (Downs et al., 2022).

Hardiness

Hardiness is a psychological construct encompassing attitudes and personality traits that contribute to an individual's resilience in the face of stress (Kobasa, 1979). Kobasa introduced it in the late 1970s as a framework for understanding how some individuals can better cope with and adapt to stressful situations. Hardiness is characterized by three core components: commitment, control, and challenge. Commitment refers to an individual's tendency to engage fully in activities and have a sense of purpose in life. Control relates to one's belief in their ability to influence and manage their environment. Challenge refers to the perception of stressors as opportunities for growth rather than threats. These components work together to enhance an individual's resilience and coping with stress.

Commitment is a core component of hardiness and involves a deep involvement in activities and a sense of purpose in life. Highly committed individuals strongly believe in the value and significance of their work or other pursuits. They are motivated and dedicated, which helps them maintain a positive outlook and a sense of meaning even in challenging circumstances (Maddi, 2006).

Control refers to an individual's belief in their ability to influence and manage their environment. Hardy individuals have an internal locus of control, perceiving themselves as having control over their actions and outcomes. They view themselves as active agents in their lives, capable of making choices and taking responsibility for their well-being. This sense of control helps them approach stressors with a problem-solving mindset (Kobasa, 1979).

Challenge refers to the perception of stressors as opportunities for growth and learning. Hardy individuals view stressful situations as normal and expect to encounter difficulties in life. Rather than feeling overwhelmed, they embrace challenges and use them as catalysts for personal development. This positive mindset allows them to reframe stressors and maintain a proactive approach to problem-solving (Bartone et al., 2009).

Hardiness has significant implications for stress coping and resilience. Research has shown that individuals high in hardiness are more likely to experience lower levels of stress, anxiety, and burnout, as well as better physical and mental health outcomes (Connor-Smith et al., 2000). Their commitment, control, and challenge mindset enable them to engage in effective coping strategies, such as problem-solving, seeking social support, and reframing stressors in a positive light (Florian et al., 1995).

Although hardiness is considered a personality trait, it is not solely innate and can be cultivated and strengthened. Intervention programs aimed at developing hardiness have shown promising results. These programs involve cognitive restructuring, building self-efficacy, and providing training in stress management and problem-solving skills (Maddi, 2006). Additionally, fostering social support networks and promoting a positive work environment can contribute to developing hardiness.

In a Wong 2014 study, hardy Chinese women consciously integrate commitment, control, and challenge in devoting themselves to strategies to manage difficulties, solve problems, make decisions, and set goals while promptly dealing with stressful events (Wong et al., 2014). Resilience is an important psychological trait contributing to an individual's ability to cope with adversity and maintain mental well-being. The Dispositional Resilience Scale (DRS-15) assessed an individual's dispositional resilience, capturing their inherent capacity to bounce back from challenges.

Wong's study involved a transcultural and psychometric validation process, aiming to ensure the reliability and validity of the DRS-15 when applied to Chinese adult women. The researchers likely conducted a series of assessments and analyses to examine the scale's appropriateness for this specific cultural and demographic group. This process likely included linguistic adaptation, cultural relevance checks, and statistical analyses to confirm the scale's psychometric properties within the Chinese context.

This paper explores how the hardiness construct from veterans applies to cybersecurity behaviors. Aigbefo (2020) explored the impact of two psychological factors, hardiness and habit, on individuals' intentions to engage in security-related behaviors. Hardiness refers to a person's ability to endure and cope effectively with stressful situations; habit represents repeated, automatic behaviors formed through regular practice. The study likely investigates how these two factors influence individuals' intentions to adopt security-related behaviors, such as those related to information security or personal safety. The authors analyzed the collected data to understand the relationships between hardiness, habit, and the intention to engage in security behaviors.

The Aigbefo study found that hardiness significantly affects employee security behavior intention. Employees with high hardiness levels (commitment, control, and challenge) can adjust where necessary to minimize the effect of security threats rather than alienate themselves or submit to the security threat. The study shed light on whether individuals with higher levels of hardiness are more likely to exhibit positive security-related behaviors and whether habitual tendencies contribute to adopting such behaviors. Aigbefo examined the interplay between hardiness, habit, and individuals' intentions to engage in security-related behaviors. Understanding these psychological factors can have implications for designing effective strategies to promote security-conscious behaviors among individuals, whether in cybersecurity, personal safety, or other security-related domains (Aigbefo et al., 2020).

Veterans

Veterans who have served in the military often possess unique attributes and experiences that can contribute to their potential in the cybersecurity field. Military training and experience foster discipline, adaptability, problem-solving skills, and a strong work ethic. These attributes align with the qualities required of cybersecurity professionals, such as attention to detail, resilience, and the ability to work under pressure (Mouloua et al., 2019).

Veterans’ perspectives on cybersecurity risks are often shaped by their military background, where the concept of security extends beyond physical threats to encompass digital vulnerabilities. They are likely to perceive cyber threats as critical to their overall security strategy, recognizing the potential for cyber attacks to disrupt operations and compromise sensitive information. This perception drives a more integrated approach to cybersecurity, where digital defenses are seamlessly aligned with broader security measures.

Shappie (2020) found that personality traits, particularly conscientiousness and openness, were associated with cybersecurity behaviors. Shappie (2020) suggests that personality significantly predicts cybersecurity behavior. People often behave in ways that are discordant with their intentions. Assuming most people intend to comply with safe practices, it is still no surprise that they violate policies and regularly put sensitive data at risk (Shappie et al., 2020).

Hardiness can play a significant role in veterans' success in terms of cybersecurity skills. The commitment component of hardiness reflects a strong sense of purpose and dedication, which can drive individuals to excel in cybersecurity roles that require ongoing learning and adapting to emerging threats. The control component provides veterans with a belief in their ability to handle challenging situations and take proactive measures to protect digital assets. The challenge component allows veterans to view cybersecurity as an opportunity for growth and continuous improvement (Bartone et al., 2009).

Bartone (2009) explored the predictive power of various personality factors on leader performance. The study investigated the influence of the Big Five personality traits (openness, conscientiousness, extraversion, agreeableness, and emotional stability), hardiness, and social judgment in determining the effectiveness of leaders. Bartone's research contributes to the literature on leadership by examining the roles of the Big Five personality factors, hardiness, and social judgment in predicting leader performance and finding that leader performance is predicted by mental abilities. Such insights can be valuable for organizations aiming to identify and cultivate effective leadership qualities in their personnel.

As a population rigorously researched in hardiness studies, the veteran population for this study introduces the hardiness construct as a moderator to PMT. To capitalize on the potential of veterans in cybersecurity, it is crucial to provide support and resources during their transition from military service to the civilian workforce. Initiatives that offer targeted training, certifications, and educational programs tailored to the specific needs of veterans can help bridge the gap between military experience and cybersecurity knowledge. Additionally, mentorship programs and networking opportunities can facilitate the integration of veterans into the cybersecurity community.

By harnessing hardiness's commitment, control, and challenge components, veterans can leverage their skills and mindset to excel in protecting digital systems and information. Providing targeted support and resources during their transition from military service to the cybersecurity workforce is essential for capitalizing on their potential. Understanding and nurturing the relationship between hardiness, veterans, and cybersecurity can contribute to building a robust and resilient cybersecurity workforce (Petersen et al., 2020).

Veterans leverage their military experience to establish and lead tech startups, particularly cybersecurity ones. According to Demsey et al., veteran-founded cybersecurity companies represent a significant portion of the tech entrepreneurial ecosystem, with 45% of these companies led by veterans (Dempsey et al., 2019).

Table 1 Construct Definitions

Construct	Type	Definition	**Source**
Cyber Security Intention	Dependent	An employee's intention to protect the information and technology resources of the organization from potential security breaches.	(Ajzen, 1991)
Fear of Internet Security Threat	Mediator	How fearful an employee is from an internet security threat occurring to them.	(Chen & Qi, 2022)
Hardiness	Moderator	A personality style to differentiate individuals under stress based on commitment towards life, control of life, and willingness to overcome challenges	(Kobasa, 1979)
Perceived Vulnerability	Independent	The probability that an unwanted incident will happen if no actions are taken to prevent it. The chances of receiving a virus	(Vance et al., 2012)
Perceived Severity	Independent	The level of the potential impact of the threat (i.e., its severity and how severe the damage that it can cause). The degree that someone	(Vance et al., 2012)
Response Cost	Independent	The inconvenience incurred in complying with IS security policies.	(Vance et al., 2012)
Response Efficacy	Independent	The efficacy of a recommended coping response (compliance with IS security policy).	(Vance et al., 2012)

Self-efficacy	Independent	The belief that they can successfully comply with IS security policies	(Vance et al., 2012)

CHAPTER III: RESEARCH DESIGN

Conceptual Framework

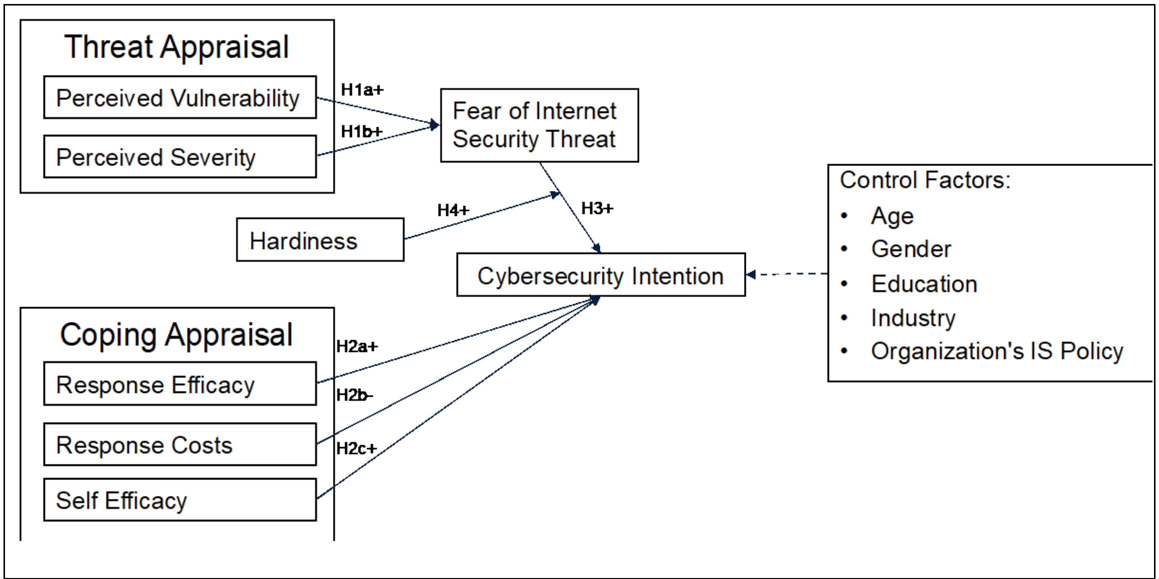


Figure 1 The Conceptual Research Model

Theoretical Development and Hypotheses

How vulnerable you feel to a threat (perceived vulnerability) and imagining the severity of the fallout of a threat or incident occurring to you (perceived severity) may make someone fearful. Perceived vulnerability and severity play a crucial role in shaping individuals' fear of internet security threats in the workplace. Supported by the literature, Chen (2022) found that these two threat appraisal factors: perceived vulnerability and perceived vulnerability, strongly impact fear. Perceived vulnerability acts as an amplifier, intensifying the fear response to internet security threats. When individuals believe they are highly vulnerable, their fear responses become more pronounced, potentially leading to avoidance behaviors, reduced productivity, and compromised decision-making. Fear mediates threat appraisal factors and cybersecurity behavior because fear positively affects adaptive and maladaptive cyber behavior. Users are more likely to seek help if they fear internet threats. When internet users believe they are vulnerable to security attacks and could suffer significant loss or harm, their fear of a threat is raised. Individuals' knowledge gaps and uncertainty regarding internet security threats often influence perceived vulnerability. A limited understanding of cybersecurity practices and the evolving nature of threats can contribute to a heightened sense of vulnerability, fostering employee fear. Their overall threat perception of internet security threats determines how fearful they could become (Chen et al., 2022).

Research consistently demonstrates that higher levels of perceived severity are associated with increased fear responses in the context of internet security threats. Employees who perceive threats as more severe are more likely to experience heightened fear, potentially leading to negative consequences for individuals and organizations. Perceived severity also acts as an amplifier, intensifying fear responses to internet security threats. When individuals believe threats to be highly severe, their fear responses become more pronounced, potentially resulting in avoidance behaviors, reduced productivity, and compromised decision-making. Perceived severity influences employees' trust and confidence in their ability to protect themselves and the organization from internet security threats. Higher perceived severity may erode trust in security measures, leading to increased fear and reduced confidence in mitigating potential threats.

H1a - The employee’s perceived vulnerability increases the employee’s fear of an internet security threat.

H1b -The employee’s perceived severity increases the employee’s fear of an internet security threat.

The PMT coping appraisal constructs: response efficacy, response costs, and self-efficacy, are how employees believe they will deal with or cope with a situation before developing a coping strategy that will lead to their behavior.

Response efficacy is compliance with information security policies (Vance et al., 2012). Research consistently demonstrates that higher levels of response efficacy are associated with increased cybersecurity intention among employees. When employees believe cybersecurity measures effectively safeguard against threats, they are more likely to engage in proactive cybersecurity behaviors, enhancing organizational asset protection. Response efficacy serves as a motivating factor for employees to participate in cybersecurity practices actively. Believing in the effectiveness of cybersecurity measures instills confidence and encourages employees to take ownership of their cybersecurity responsibilities, leading to a stronger intention to engage in protective behaviors. Response efficacy enhances employees' perceived control over cybersecurity outcomes and shapes their expectations of the positive outcomes associated with engaging in cybersecurity behaviors. Employees who believe in the effectiveness of security measures perceive themselves as having greater control over cybersecurity threats and anticipate positive outcomes, reinforcing their intention to engage in protective behaviors.

Response cost is the inconvenience incurred in complying with IS security policies. The usability and convenience of cybersecurity measures significantly influence individuals' intentions and behaviors. Complex and time-consuming security protocols may discourage individuals from adopting secure practices, favoring convenience over security. When the perceived effort, resources, or potential negative consequences of cybersecurity behaviors are high, employees are less likely to exhibit proactive cybersecurity behaviors, compromising organizational security. Response cost is a deterrent, discouraging employees from engaging in cybersecurity behaviors. When employees anticipate significant effort, time, or adverse consequences, they may opt for non-compliance or take shortcuts, undermining cybersecurity practices and increasing vulnerability to cyber threats. Employees who perceive cybersecurity measures as cumbersome or time-consuming are less likely to prioritize these activities, reducing cybersecurity intention. Insufficient resources, inadequate training, or lack of organizational support can amplify response costs. When employees feel ill-equipped or unsupported in executing cybersecurity tasks, the perceived effort and potential negative outcomes increase, hampering their cybersecurity intention (Hu et al., 2012).

Self-efficacy is the employee’s belief that they can successfully comply with IS security policies, which should enhance compliance with policies and procedures. Research consistently demonstrates that higher levels of self-efficacy are associated with increased cybersecurity intention among employees. When employees believe in their capabilities to perform cybersecurity tasks effectively, they are more likely to engage in proactive cybersecurity behaviors, enhancing organizational asset protection. Self-efficacy serves as a motivational factor for employees to participate in cybersecurity practices actively. Believing in their abilities to successfully perform cybersecurity tasks instills confidence. It encourages employees to take ownership of their cybersecurity responsibilities, resulting in a stronger intention to engage in protective behaviors. When employees have opportunities to engage in and accomplish cybersecurity activities, their self-efficacy increases, leading to a higher intention to engage in future cybersecurity behaviors.

The coping appraisal factors lead to employees developing a cognitive coping strategy. It is appropriate to measure the employee's self-belief on how they cope with an incident because the theory of planned behavior shows that subjective norms, perceived behavioral control, and attitude lead to an intention and then a behavior, in this case, cybersecurity behavior (Ajzen, 1991).

H2a – The employee's response efficacy positively influences cybersecurity intention.

H2b – The employee's response cost negatively impacts cybersecurity intention.

H2c – The employee's self-efficacy positively influences cybersecurity intention.

Fear is a driver that motivates individual users to control their fear (Chen et al., 2022). If an employee fears a threat, they take measures to protect themselves. Fear, as an emotional response to the perceived threat of internet security breaches, can significantly impact employees' cybersecurity intentions. The emotional arousal associated with fear can prompt individuals to take preventive actions, such as implementing security measures, updating passwords, and being vigilant against potential threats, thus strengthening their cybersecurity intention. When employees perceive themselves as potential targets for cyber-attacks, they fear the negative consequences of such threats increase. This heightened vulnerability can drive individuals to adopt protective behaviors and increase their cybersecurity intention.

When employees perceive a breach's potential harm or damage, their fear response intensifies. This perception of severity is a motivational force, propelling employees to prioritize cybersecurity and strengthen their intention to engage in protective behaviors. Fear triggers a self-protective response, leading to a heightened sense of personal responsibility for cybersecurity. When employees experience fear, they are likelier to perceive themselves as key actors in preventing security breaches. This increased sense of personal responsibility strengthens their intention to engage in cybersecurity behaviors.

H3 – The employees' fear of an internet security threat positively increases their cybersecurity intention.

Employees' hardiness, characterized by resilience, commitment, and control, can significantly moderate the relationship between fear of internet security threats and cybersecurity intention. Hardiness enhances individuals' resilience in the face of fear. Employees high in hardiness are more likely to perceive internet security threats as challenges rather than overwhelming obstacles. Their ability to bounce back from fear-inducing situations and maintain a sense of control contributes to their cybersecurity intention. Hardiness fosters a commitment to cybersecurity practices. Employees high in hardiness are intrinsically motivated to protect organizational assets and are committed to maintaining high cybersecurity standards. Their strong sense of responsibility and dedication drive their cybersecurity intention, even in the presence of fear (Shappie et al., 2020). A key disposition in hardiness is control, an individual's belief that they can influence the events they experience (Kobasa, 1979). Therefore, if fear drives motivation to control, and hardiness affects the ability to control, hardiness can moderate how an individual user behaves when they fear an internet security threat.

H4 – The employee's hardiness positively moderates the relationship between fear of an internet security threat and cybersecurity intention.

CHAPTER IV: RESEARCH METHODOLOGY

Participants and Procedure

The unit of analysis for this study is military veterans who work in white-collar jobs, and the unit of observation is the individual. The population of US Military Veterans in the US workforce is 8,918,000. Therefore, the minimum sample size has been identified as 385.

Research Design

An online survey study with a quasi-experimental design will be used to observe the units of analysis under natural conditions, without deliberate manipulation, a control group, or random assignment, to explore the strength of the variances for the population. All questions are measured using a 7-point Likert scale ranging from 1 - Strongly Disagree to 7 - Strongly Agree.

Empirical data is captured using an online survey on Qualtrics, and subjects will be recruited via Connect (by CloudResearch) and social media. Each participant is asked if they are a retired US veteran and honorably discharged, and if they respond positively, the subject will proceed with the study. If not, they received a pop-up thanking them for their time and not continuing. There was a captcha and eliminator questions to detract bots and bad data: “Select somewhat agree,” and if they did not answer correctly, their response was deleted. At the end of the survey, a random number is generated to email back to the researcher to receive compensation. The control factors include demographic information (age, gender, education) and industry profile. The total number of items that measure constructs for this study is 69 questions.

Measurements

Questions are derived from literature and used in multiple publications. To measure cybersecurity intention, we use Egelman & Peer's (2015) questions for intention to comply for a total of sixteen questions to measure the dependent variable, cybersecurity intention. Hardiness is measured using Bartone's (1991) study on hardiness and validated in Aigbefo's (2020) study on hardiness in security behavior intention (Bartone, 1991). Aigbefo was able to scale down hardiness questions from 30 to 13 based on low loading and to improve construct reliability or validity. Hardiness contains commitment, control, and challenge as subconstructs; each dimention has 4-5 questions. To measure fear, questions are taken from Chen (2022) study on adaptive coping behaviors and . In Chen's (2022) research, he achieved a Cronbach's Alpha of 0.934 for the fear construct.

To measure the constructs from Protection Motivation Theory (perceived vulnerability, perceived severity, response efficacy, response costs, and self-efficacy), we use the questionnaire from (Anwar et al., 2017), whose items were adapted from previously validated instruments when possible. The questions are referenced from various sources and are a good measurement tool for the constructs (needs citation of the sources).

Once the data is collected, an exploratory factor analysis (EFA) is conducted using IBM's SPSS. A Kaiser-Meyer-Olkin measure will verify the sampling adequacy for the analysis, hoping all KMO values for individual items will be well above the acceptable limit of .50. An initial analysis will be run to obtain eigenvalues for each factor in the data. A scree plot will show ambiguity and inflections that justify the factors. An independent-sample proportion test will be conducted to evaluate whether the proportions of age and gender differ across the sample population.

A Structural Equation Modeling (SEM) will examine the interaction between the fear of an internet security threat and hardiness as predictors of cybersecurity intention while controlling for gender and checking for multicollinearity. The annexes will contain evidence of the data, tables, and figures.

Pilot Studies

An informed pilot was conducted by IT leaders and managers from FIU's DBA cohort 4.5. Before moving on to the main study, the informed pilot made a plausible case for the variables' precision, accuracy, reliability, and validity.

The informed pilot gave positive feedback and overall agreed with the conceptual model. The Qualtrics survey was forwarded to the informed pilot reviewers. Each measurement item was reviewed, and recommendations were acted on. Changes included moving the demographic questions to the end of the survey to avoid survey fatigue. Instructions were changed to “Answer the following questions truthfully regarding your work habits,” from referencing general behavior due to the study’s focus on employed military veterans and their habits and behavior at work. After the informed pilot, the Qualtrics survey was ready for the next phase.

The Qualtrics survey was modified to be anonymous, and participants were initially recruited from Amazon MTurk. Two rounds of pilot studies were conducted using Amazon MTurk using over (257) and (179) recruited participants. Entries were eliminated due to failing attention check questions (22) and (41) for a total of (238) and (138) valid entries. Though there were enough entries to conduct exploratory factor analysis, the factor analysis did not result in a clean EFA for intended latent constructs. After repeated methods of factor loading, the assumed cause was unsatisfactory data by the MTurk participants because the measurement instruments were validated for reliability and validity in other academic research studies.

Another platform was utilized to recruit participants: Connect from CloudResearch. Demographic targeting on the platform included US Veterans only and was linked to Qualtrics, where the survey still resided. There were three initial rounds of (10) participants to learn the platform and ensure the questions were delivered and available for the participants to answer. After reviewing answers following completion, a fourth round was conducted with (130) participants with a bounce rate of 21%. Connect provided more reliable data than Amazon MTurk in terms of data collection and a smaller elimination rate. An exploratory factor analysis was conducted to identify the causal relationships between variables in a dataset. The observed variables appeared aligned with the theoretical constructs they were intended to measure, therefore, ready for the next step of final data collection.

Chapter V: DATA ANALYSIS AND RESULTS

Data Analysis

The main study included collecting participant data from the Connect Platform and recruitment from social media. The Connect platform allowed demographic targeting; for this study, the only targeted group was US Veterans. The Connect group yielded (189) data entries and, after eliminating participants due to failing qualifying questions, yielded (158) verified data points. Social Media recruitment was conducted from various Veteran groups on Facebook, LinkedIn, and WhatsApp. Social Media yielded (108) data entries, and after eliminating participants due to failing qualifying questions, it yielded (36) verified data points. The total number of data entries for the main study was (194) participants. Table 2 displays the demographic data for the study.

Table 2 Demographic Data

	Characteristics	Frequency	% of Population
Age	20-24	2	1.0%
	25-34	56	28.7%
	35-44	69	35.5%
	45-54	42	21.5%
	55-64	23	11.8%
	>65	2	2.0%
Years Served	0-4 years	72	37.1%
	5-9 years	75	38.7%
	10-14 years	26	13.4%
	15-19 Years	6	3.1%
	20-25 years	14	7.2%
	>25 years	1	0.5%
Gender	Male	139	71.6%
	Female	55	28.4%
Education	High School/GED	27	13.9%

	Associate's Degree	36	18.6%
	Bachelor's Degree	89	45.9%
	Master's Degree	35	18.0%
	Doctorate/PhD	7	3.6%
Sector	Agriculture; plantations;other rural sectors	1	0.5%
	Basic Metal Production	2	1.0%
	Commerce	6	3.1%
	Construction	7	3.6%
	Education	19	9.8%
	Financial services; professional services	34	17.5%
	Food; drink; tobacco	2	1.0%
	Forestry; wood; pulp and paper	2	1.0%
	Health services	19	9.8%
	Hotels; tourism; catering	2	1.0%
	Mining (coal; other mining)	4	2.1%
	Mechanical and electrical engineering	7	3.6%
	Media; culture; graphical	4	2.1%
	Oil and gas production; oil refining	5	2.6%
	Postal and telecommunications services	7	3.6%
	Public service/Non-profit/Government	19	9.8%
	Shipping; ports; fisheries; inland waterways	2	1.0%
	Textiles; clothing; leather; footwear	1	0.5%
	Transport (including civil aviation; railways; road transport)	5	2.6%
	Transport equipment manufacturing	3	1.5%
	Utilities (water; gas; electricity)	2	1.0%
	Not listed/Other	41	21.1%
Grade	Enlisted	154	79.4%
	Officer	40	20.6%
Organization has an established IS Policy	I don't know	1	0.5%
	No	6	3.1%
	Maybe	23	11.9%
	Yes	164	84.5%
Organization has a policy on cybersecurity awareness	I don't know	3	1.5%
	No	14	7.2%
	Maybe	23	11.9%
	Yes	154	79.4%
Source	CloudResearch	158	81.4%

Social Media	36	18.6%

A principal component analysis was conducted to confirm that survey questions did load on the constructs. Each latent factor is represented by multiple observed indicators (items), and each indicator is assumed to load onto its corresponding latent factor. The factor loading represents the strength and direction of the relationship between the latent factor and the observed indicator, as shown in Table 3.

Table 3 Principal Component Analysis

Component Loadings	**Component**								
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**Uniqueness**
Fear of Internet Security Threat 5	0.94								0.168
Fear of Internet Security Threat 4	0.879								0.185
Fear of Internet Security Threat 7	0.864								0.28
Fear of Internet Security Threat 6	0.816								0.277
Fear of Internet Security Threat 3	0.799								0.201
Fear of Internet Security Threat 2	0.786								0.164
Fear of Internet Security Threat 1	0.715								0.229
Perceived Severity 7		0.944							0.118
Perceived Severity 5		0.918							0.186
Perceived Severity 4		0.888							0.175
Perceived Severity 6		0.877							0.183
Perceived Severity 3		0.809							0.258
Perceived Severity 1		0.763							0.355
Hardiness Commitment 3			0.79						0.361
Hardiness Commitment 2			0.772						0.383
Hardiness Commitment 5			0.75						0.365
Hardiness Commitment 1			0.74						0.416
Hardiness Commitment 4			0.738						0.429
Hardiness Commitment 3			0.692						0.304
Hardiness Control 1			0.548						0.524
Hardiness Control 4			0.467						0.595

Hardiness Challenge 1	0.400						0.654
Perceived Vulnerability 4		0.881					0.217
Perceived Vulnerability 5		0.838					0.191
Perceived Vulnerability 6		0.787					0.215
Perceived Vulnerability 2		0.672					0.45
Perceived Vulnerability 1		0.486					0.625
Response Efficacy 6			0.918				0.138
Response Efficacy 5			0.882				0.181
Response Efficacy 7			0.858				0.249
Self Efficacy 2				0.868			0.25
Self Efficacy 3				0.825			0.277
Self Efficacy 4				0.811			0.302
Self Efficacy 7				0.670			0.393
Response Costs 5					0.808		0.269
Response Costs 6					0.806		0.288
Response Costs 4					0.785		0.324
Cybersecurity Intention_DS 1						0.834	0.287
Cybersecurity Intention_DS 3						0.751	0.373
Cybersecurity Intention_DS 2						0.642	0.466
Cybersecurity Intention_DS 4						0.587	0.552

***Note.* 'oblimin' rotation was used**

A combination of the Jemovi software and R Studio was used to conduct data analysis on the main study. Following the principal component analysis, a confirmatory factor analysis (CFA) was conducted to provide a formal framework for assessing the fit between the proposed model and the observed data, and it was used to confirm the validity of the latent variable measures. Construct reliabilities were reviewed using a factor weighting scheme, including the outer loadings for each latent variable. The CFA is instrumental in validating measurement instruments by examining whether the observed variables accurately reflect the theoretical constructs they are intended to measure. The CFA allows estimation and accountability for measurement errors in the model. By distinguishing between the variance due to true scores and the variance due to measurement error, the CFA helps improve the reliability and validity of their measures and obtain more accurate estimates of the relationships between variables.

Constraints were imposed where the scale factor equals the first indicator, it refers to a specific parameterization of the factor loading(s) within the model, it means that one of the factor loadings for each latent factor is fixed to a specific value, often set to 1. This indicator is referred to as the reference indicator, and it serves as the anchor for scaling the latent factor. Practically, this constraint simplifies the model estimation and interpretation by setting a reference point for the scaling of the latent factor. By fixing one of the factor loadings to 1, the interpretation of the other factor loadings becomes relative to the reference indicator. The reference indicator defines the metric or scale of the latent factor, making it easier to interpret the factor loadings and compare them across different indicators, as shown in Table 4.

Table 4 CFA Factor Loadings

Factor	Indicator	Estimate		SE	Z	p	Stand. Estimate
Perceived Vulnerability	Perceived Vulnerability 5	1	[a]				0.91
	Perceived Vulnerability 6	1.038		0.0575	18.05	< .001	0.889
	Perceived Vulnerability 4	0.928		0.0528	17.57	< .001	0.868
	Perceived Vulnerability 2	0.643		0.0762	8.44	< .001	0.556
	Perceived Vulnerability 1	0.472		0.0706	6.69	< .001	0.457
Hardiness	Hardiness Challenge 3	1	[a]				0.786
	Hardiness Commitment 5	1.009		0.0921	10.94	< .001	0.757
	Hardiness Commitment 2	0.849		0.0893	9.5	< .001	0.688
	Hardiness Commitment 1	0.739		0.0766	9.65	< .001	0.691
	Hardiness Commitment 3	0.929		0.092	10.09	< .001	0.704
	Hardiness Commitment 4	0.811		0.0908	8.93	< .001	0.656

	Hardiness Control 1	0.57		0.0719	7.93	< .001	0.584
	Hardiness Control 4	0.575		0.0854	6.74	< .001	0.498
	Hardiness Challenge 1	0.477		0.0721	6.61	< .001	0.485
Response Efficacy	Response Efficacy 6	1	[a]				0.945
	Response Efficacy 5	0.92		0.0537	17.13	< .001	0.866
	Response Efficacy 7	0.819		0.0532	15.38	< .001	0.811
Response Costs	Response Costs 5	1	[a]				0.921
	Response Costs 6	0.892		0.0811	11.01	< .001	0.799
	Response Costs 4	0.662		0.0759	8.72	< .001	0.613
Self-Efficacy	Self Efficacy 2	1	[a]				0.828
	Self Efficacy 3	0.869		0.0769	11.3	< .001	0.802
	Self Efficacy 4	0.93		0.0894	10.4	< .001	0.727
	Self Efficacy 7	0.552		0.0667	8.27	< .001	0.617
Fear of Internet Security Threat	Fear of Internet Security Threat 5	1	[a]				0.873
	Fear of Internet Security Threat 2	0.932		0.0544	17.15	< .001	0.887
	Fear of Internet Security Threat 4	0.951		0.0547	17.4	< .001	0.883
	Fear of Internet Security Threat 3	0.922		0.0541	17.04	< .001	0.883
	Fear of Internet Security Threat 1	0.889		0.0579	15.36	< .001	0.839
	Fear of Internet Security Threat 6	0.892		0.0621	14.37	< .001	0.797
	Fear of Internet Security Threat 7	0.845		0.06	14.09	< .001	0.786
Cybersecurity Intention	Cybersecurity Intention_DS 1	1	[a]				0.879
	Cybersecurity Intention_DS 2	0.232		0.0472	4.91	< .001	0.384
	Cybersecurity Intention_DS 3	0.99		0.1363	7.26	< .001	0.755
	Cybersecurity Intention_DS 4	0.292		0.0696	4.2	< .001	0.336
Perceived Severity	Perceived Severity 1	1	[a]				0.725
	Perceived Severity 3	0.951		0.0859	11.07	< .001	0.795
	Perceived Severity 4	1.105		0.0866	12.76	< .001	0.911
	Perceived Severity 5	1.111		0.0906	12.26	< .001	0.862
	Perceived Severity 6	1.033		0.0856	12.07	< .001	0.861
	Perceived Severity 7	1.168		0.0875	13.35	< .001	0.952

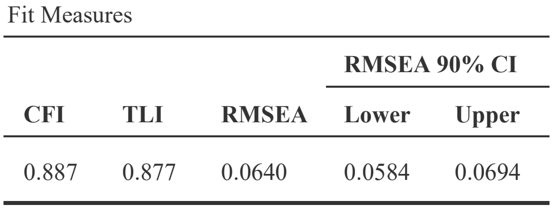
[a] **fixed parameter**

This constraint is common in CFA models to ensure the identifiability of the model, as fixing one loading to a specific value helps to identify the scale of the latent factor. It also aids in improving the convergence and estimation of the model parameters.

Good model fit indicates that the proposed theoretical model adequately represents the relationships among the observed variables. It suggests that the specified model is a plausible explanation of the observed data. Model fit is crucial when testing for measurement invariance across different groups or conditions. Invariance testing involves comparing the fit of nested models with different constraints on the parameters (e.g., factor loadings, intercepts) across groups. Good model fit across groups indicates that the measurement model is invariant, meaning that the measurement properties of the scales are consistent across groups.

Model fit indices provide quantitative assessments of how well the specified model fits the observed data. It helps determine the degree to which the model accurately represents the underlying structure of the data. Good model fit increases confidence in the validity of the results and the conclusions drawn from the analysis. Table 6 are the model fit measures of the main study.

Table 5 Fit Measure



Fit Measures

			RMSEA 90% CI	
CFI	TLI	RMSEA	Lower	Upper
0.887	0.877	0.0640	0.0584	0.0694

The comparative fit index (CFI) and Tucker–Lewis index (TLI) provide a measure of how well the specified model fits the observed data. It compares the fit of the hypothesized model to the fit of a baseline or null model, indicating whether the proposed model adequately represents the relationships among the observed variables.

A high CFI value (close to 1.0) indicates that the specified model fits the data well, suggesting that the observed data support the hypothesized relationships between variables. Conversely, a low CFI value (far from 1.0) suggests that the proposed model does not adequately explain the patterns of covariation among the variables, indicating potential problems with the model specification or data. Values greater than 0.90, conservatively 0.95 indicate good fit. RMSEA is the root mean square error of approximation (values of 0.01, 0.05 and 0.08 indicate excellent, good, and mediocre fit respectively, some go up to 0.10 for mediocre).

For the main study, we must allow some variables to covary and impose constraints. Allowing variables to covary means specifying correlations between certain pairs of observed variables in the model. These correlations are represented by covariances, indicating the degree to which two variables vary. By reviewing the residual covariances, exceptionally high covariances were selected to covary. Allowing variables to covary acknowledges the possibility of shared variance between certain pairs of variables not accounted for by the latent factors in the model. Allowing these covariances can improve the model's fit to the data by capturing these additional sources of covariance. Four pairs are identified by using R Studio to find pairs with a high modification index and a minimum value of 30, as shown in Table 7.

Table 6 Largest MI values for Model

lhs	op	rhs	mi	epc
Fear of Int Sec 1	~~	Fear of Int Sec 2	57.372	0.436
Perc Sev 3	~~	Perc Sev 6	47.364	0..582
Perc Sev 1	~~	Perc Sev 5	34.998	0.774
Fear of Int Sec 2	~~	Fear of Int Sec 6	30.760	-0.411

By adding the residual covariances to the model, we recalculate the fit measure with matching result on R Studio and Jemovi as shown in Table 8.

Table 7 Fit Measures with Modification Indices

Fit Measures

			RMSEA 90% CI	
CFI	TLI	RMSEA	Lower	Upper
0.918	0.911	0.055	0.049	0.061

Next, we look at the correlations table for the individual items. Here we are looking for variables that are not correlated to anything (most correlations less than .3) or that are too strongly correlated (e.g., correlations above .9). The highest correlation in our model, seen in Table 9, is fear correlated with perceived severity, which came out to .464, this is still acceptable.

Table 8 Model Correlations

	Prcv_V	Prcv_S	Hrdnss	Rspn_E	Rspn_C	Slf_Ef	Cybr_I	Fear
Perceived_Vulnerability	1.000							
Perceived_Severity	0.341	1.000						
Hardiness	-0.080	-0.009	1.000					
Response_Efficacy	0.007	0.112	0.345	1.000				
Response_Costs	0.335	-0.056	-0.163	-0.048	1.000			
Self_Efficacy	-0.143	0.050	0.382	0.199	-0.136	1.000		

Cybersecurity_Intention	-0.019	0.102	0.152	0.128	-0.286	0.093	1.000	
Fear	0.512	0.464	-0.035	0.040	0.116	-0.041	0.133	1.000

Next, we conducted a reliability analysis to find each construct’s Cronbach's alpha. Cronbach’s alpha is a statistic used in reliability analysis to assess the internal consistency of items or variables intended to measure the same underlying construct or concept. It measures the degree to which items that are supposed to measure the same construct produce similar scores. Cronbach's alpha ranges from 0 to 1. A value of 1 indicates perfect internal consistency, meaning that all items are perfectly correlated. On the other hand, a value of 0 indicates no internal consistency, suggesting that the items are unrelated. The reliability analysis, seen in Table 8, returned high reliabilities (>.814), except the Cybersecurity Intention factor, which resulted in a Cronbach alpha of .686. Typically, Cronbach's alpha values above 0.7 are considered acceptable for research purposes, although the acceptable threshold may vary depending on the context and the specific field of study.

Table 9 Reliability Analysis

	Cronbach's α	**McDonald's ω**
Perceived Vulnerability	0.856	0.867
Perceived Severity	0.941	0.944
Hardiness	0.870	0.871
Response Efficacy	0.905	0.907
Response Costs	0.814	0.827
Self-Efficacy	0.827	0.833
Cybersecurity Intention	0.686	0.740

Fear of Internet Security Threat	0.949	0.950

Findings

This study aimed to investigate the factors that cause veterans' cybersecurity intentions. A summary of the findings can be found below in Table 11. The first set of hypotheses (H1a & H1b) proposed that a veteran employee’s threat appraisal, perceived vulnerability, and perceived severity increase their fear of an internet security threat. The relationships are supported and indicate that veterans’ fears of internet security are based on their abilities to perceive their own vulnerabilities and how damaging a security threat could be to them.

The second set of hypotheses (H2a, H2b, and H2c) proposed that veteran employees' coping appraisals directly influenced their cybersecurity intention to protect the information and technology resources of the organization from potential security breaches. The data does not significantly indicate that a veteran employee’s response efficacy (H2a) positively influences their cybersecurity intentions. The data does support that their response costs (H2b) will negatively impact their cybersecurity intention, which may indicate that the availability of information may cause veterans to sidestep some information security protocols. The following hypothesis (H2c) does not support a veteran’s self-efficacy to influence their cybersecurity intention positively. It may indicate an over-confidence in a veteran’s abilities or belief in a robust and secure network.

The next hypothesis (H3) proposed that a veteran employee's fear of an internet security threat would positively increase their cybersecurity intention. The data positively supports this relationship, but it was near the 5% threshold in hypothesis testing with a p-value of 0.035. Therefore, it is notable that there is moderate support for the relationship.

The final hypothesis (H4) was that a veteran's hardiness moderates the relationship between their fear and cybersecurity intention. The proposed relationship lacks support, with a p-value of 0.274. A veteran's hardiness, which is their ability to commit, control, and overcome challenges, does not significantly impact the relationship between fear and cybersecurity intentions.

Table 10 Hypothesis Summary

	Hypothesis	Results	β	p-value
H1a	The employee's perceived vulnerability increases the employee's fear of an internet security threat.	Supported	0.802	<.001
H1b	The employee's perceived severity increases the employee's fear of an internet security threat.	Supported	0.316	<.001
H2a	The employee's response efficacy positively influences cybersecurity intention.	Not Supported	0.097	0.411
H2b	The employee's response cost negatively impacts cybersecurity intention.	Supported	-0.371	0.002
H2c	The employee's self-efficacy positively influences cybersecurity intention.	Not Supported	.007	0.939
H3	The employees' fear of an internet security threat positively increases their cybersecurity intention.	Supported	0.167	0.035
H4	The employee's hardiness positively moderates the relationship between fear of an internet security threat and cybersecurity intention.	Not Supported	0.238	0.274

Chapter VI DISCUSSION

Summary of Findings

The study was conducted to answer the following Research Question: What are the contributing factors toward cybersecurity protection behaviors among US military veterans in white-collar jobs? A model was created based on prior literature and research studies, and a questionnaire was distributed to test that model. The data showed that the model was a proper fit; thus, its findings could be relied upon. Of the (7) proposed hypotheses, (4) were supported.

Primarily, a military veteran has a significant ability to conduct a threat appraisal. They know how vulnerable they are and can understand how severe a cyber attack can be. Dealing with adversarial threats daily and training in general cyber security awareness while serving has helped them better understand their environment. Veterans are trained to operate in high-stress environments and take quick, decisive actions. Veterans are skilled in assessing and managing risks. They often have experience identifying potential threats and vulnerabilities, which is crucial in cybersecurity for predicting and mitigating cyber attacks. Military training emphasizes the importance of attention to detail, which is essential in cybersecurity for detecting subtle anomalies and signs of security breaches that might otherwise be overlooked.

A veteran employee’s response efficacy (compliance with IS security policies) and self-efficacy (belief that they can successfully comply with IS security policies) do not contribute to their cybersecurity intentions to protect the organization's information and technology resources from potential security breaches. The data supported veterans' response costs negatively impacted their cybersecurity intentions, which may include picking easy-to-guess passwords or ensuring their systems were updated. The subject's hardiness lacks moderation in how fear influences those same security intentions. If a veteran has not received specific training in cybersecurity, they might feel less confident in their ability to handle cyber threats effectively. Cybersecurity often involves specialized knowledge of software, hardware, and complex digital systems that might not be covered by general military training or annual cybersecurity awareness training.

Veterans are typically trained for physical security and combat scenarios, vastly different from virtual or digital threats. The intangible nature of cyber threats might make it challenging for them to assess and respond to these risks effectively without additional training. Cybersecurity jobs can sometimes be isolating, with many hours spent in front of computer screens analyzing data. Veterans, who are often accustomed to the camaraderie and direct, physical teamwork of military environments, may find this shift challenging, impacting their stress levels and overall mental health.

The field of cybersecurity is fast-evolving, requiring continuous learning and adaptation. Veterans might find it stressful to keep up with the latest technologies, security protocols, and threat landscapes, potentially impacting their confidence in coping with cyber threats. The culture in civilian tech environments can significantly differ from military settings, which are structured and hierarchical. Adapting to more flexible, often less structured civilian workplaces might affect veterans' perceived self-efficacy in managing cyber-related tasks. Some veterans may struggle with mental health issues like

PTSD, which can affect concentration, decision-making, and stress management—critical components in effective coping appraisal in high-stress environments like cybersecurity.

Implications

Protection Motivation Theory was the bedrock for the model, and the threat appraisals were strongly supported, unlike the coping appraisal of PMT. PMT is a psychological model designed to explain how people are motivated to react protectively towards perceived threats. It factors in elements such as the perceived severity of and vulnerability to a threat, the perceived efficacy of the protective behavior (response efficacy), and the belief in one's ability to perform such behaviors (self-efficacy). Based on the subjects and their backgrounds in the military, other considerations may have arisen when studying veterans. While PMT provides a valuable framework for understanding protective motivation in general, the unique experiences, perceptions, and challenges veterans face may require adaptations or entirely different models to effectively address their specific needs and motivations. Tailoring interventions and support to consider these factors is crucial for effectively promoting health and well-being in veteran populations.

Veterans, particularly those who have served in combat roles, have faced real and immediate threats. This exposure might alter their perception of coping in civilian contexts, making theoretical or less immediate threats seem less significant or urgent. Veterans may experience mental health issues such as PTSD, anxiety, or depression, which can affect their motivation and perception. For instance, someone dealing with PTSD might have a heightened sense of taking protective actions due to anxiety or a sense of powerlessness. Depending on their experiences and the nature of their service, some veterans might be skeptical of information from specific sources, including the government or media.

Military and government networks must follow the Follow Information Processing Standard (FIPS), developed within the Information Technology Laboratory and published by NIST. FIPS is a standard for adoption and use by federal departments and agencies. Military members, as end-users, are typically the least privileged on their networks with robust cybersecurity awareness training compliance and heightened information security policies. Therefore, network users know that the network is constantly monitored and end-users can lower their vigilance. As an implication of the theory, no factor captures an end-user's awareness of network monitoring and confidence towards organizational information security policies.

The effectiveness of PMT can also depend on the level of social support and the community context. Veterans might have different social support structures, which can influence how they process information about threats and the recommended protective behaviors.The military training and mindset around preparedness and response to threats can also influence how veterans perceive and respond to threats in civilian life. Their training might make them more likely to assess threats and responses differently than PMT models predict for the general population. For many veterans, their identity as a soldier and their military experiences are core to their sense of self. This can influence how they interpret their own capabilities and motivations for protective behavior, possibly diverging from the assumptions underlying PMT.

Cybersecurity professionals must stay abreast of the latest developments in cyber threats, encompassing various forms such as malware, ransomware, phishing attacks, and other sophisticated tactics. This requires continuous monitoring of global cybersecurity incidents, threat intelligence feeds, and data breaches to identify patterns and trends.

Understanding the evolving threat landscape involves a multifaceted approach. It includes the examination of new vulnerabilities in software, hardware, and network infrastructures that cybercriminals exploit. Additionally, the analysis delves into the techniques employed by threat actors, such as social engineering, zero-day exploits, and advanced persistent threats (APTs).

The identification and analysis process often leverages threat intelligence platforms, machine learning algorithms, and data analytics to sift through vast information efficiently. Cybersecurity professionals collaborate with industry peers, government agencies, and information-sharing communities to gain insights into emerging threats and collaborative defense strategies.

As the threat landscape evolves, the motivations behind cyber-attacks also shift. Beyond financial gain, motives may include geopolitical influence, ideological reasons, or even state-sponsored cyber espionage. Understanding these motivations is crucial for anticipating and preparing for future threats.

Limitations and Future Research

The research had the limitations of a general quantitative study with an online questionnaire. An online questionnaire was appropriate because the target audience, veterans in white-collar jobs, generally work full-time in front of a computer and thus more easily targetable. A more selective audience would identify veterans with combat experience, white-collar experience in the military, and various levels of mental health. Data was collected on social media and CloudResearch, not partnering with companies that have active veteran communities.

Other subpopulations are military entrepreneurs and veterans in executive leadership positions. These veterans set the cybersecurity policies of their companies, therefore comparing veteran-led companies may unravel findings on cybersecurity policy and perceptions towards assessing risks against cyber attacks. Veteran-led companies often exhibit a proactive approach to cybersecurity. This proactive stance is rooted in the military principle of staying ahead of potential threats through continuous monitoring and preparation. Veterans in executive roles will likely implement stringent cybersecurity measures, emphasizing the importance of threat detection, incident response, and recovery plans. Their experience in handling complex, high-pressure situations enables them to devise resilient and adaptable strategies to evolving cyber threats.

Comparing veteran-led companies' cybersecurity policies with civilian-led companies can reveal significant insights. Veteran-led companies may prioritize cybersecurity differently, emphasizing specific aspects such as threat intelligence, employee training, and robust incident response mechanisms. This comparative analysis could uncover variations in policy focus, investment in cybersecurity technologies, and overall risk management strategies.

Empirical studies and case analyses of veteran-led companies can provide concrete evidence of the impact of military leadership on cybersecurity policies. For instance, examining companies that have successfully thwarted significant cyber attacks or have demonstrated exceptional resilience in the face of cyber threats can shed light on the effectiveness of veteran-led cybersecurity strategies. These case studies can highlight best practices and innovative approaches that other organizations can adopt.

While military veterans bring significant strengths to cybersecurity leadership, they may also face challenges adapting to cyber threats' dynamic and fast-paced nature, as shown in this study's findings related to their cognitive appraisal of cybersecurity behavior. Continuous education and collaboration with cybersecurity experts are essential to keep pace with technological advancements and emerging threats. However, the structured and disciplined approach of military veterans provides a solid foundation upon which they can build and enhance their cybersecurity capabilities.

Veterans exhibited that their assessment of threats and awareness of their vulnerabilities were significant causes of behavior. A veteran's threat appraisal may be applied to other theories or situations where veterans must maintain self-awareness of their actions. A future empirical study could compare employees with military backgrounds to those civilians without military backgrounds. The civilian group must also not have a background comparable to a military background, such as a military academy graduate or history in prison, to create distance between the two groups. It would be essential to annotate the various levels of each independent variable between the groups and if the relationships with the dependent variable are still supported as in previous studies.

A qualitative study could focus on observed cybersecurity behavior and seek to identify veterans' cognitive appraisal and whether veterans are tacitly wired to keep high cybersecurity behaviors. A ground theory study could follow college graduates into the corporate world versus those who choose to join the military and use their education benefits to join the corporate workforce later. The groups would be kept distant by adding qualifications that include honorable discharge for the veterans and no criminal history for the non-veterans to eliminate subjects that may skew the data and exclude subjects that have experienced a military-like experience while incarcerated.

Other countries should also be considered. Militaries between nations differ, and militaries between the West and Asia vary even more. Some advocates believe that the military is representative of their respective society. In contrast, other advocates claim they are not representative of society and thus represent society's very best. Different countries focus on the volunteer force of military professionals (US and UK), while other countries require conscription (Korea and Israel). A company may consider applicants with military backgrounds due to their ability to appraise threats.

Military veterans in white-collar jobs and executive leadership positions play a crucial role in shaping their companies' cybersecurity policies. Their unique skills and perspectives contribute to a proactive and comprehensive approach to cybersecurity, emphasizing preparedness, vigilance, and resilience. As the digital landscape continues to evolve, integrating military principles and practices into cybersecurity will remain a significant asset in safeguarding organizations against the ever-growing threat of cyber attacks.

LIST OF REFERENCES

Aigbefo, Q. A., Blount, Y., & Marrone, M. (2020). The influence of hardiness and habit on security behaviour intention. *Behaviour & Information Technology*, 1-20.

Ajzen, I. (1991). The theory of planned behavior. *Organizational behavior and human decision processes*, *50*(2), 179-211.

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS quarterly*, 613-643.

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, *69*, 437-443. https://doi.org/https://doi.org/10.1016/j.chb.2016.12.040

Atkins, S., & Lawson, C. (2021). An improvised patchwork: success and failure in cybersecurity policy for critical infrastructure. *Public Administration Review*, *81*(5), 847-861.

Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv preprint arXiv:1901.02672*.

Banham, R. (2017). Cybersecurity threats proliferating for midsize and smaller businesses. *Journal of Accountancy*, *224*(1), 75.

Bartone, P. T., Eid, J., Helge Johnsen, B., Christian Laberg, J., & Snook, S. A. (2009). Big five personality factors, hardiness, and social judgment as predictors of leader performance. *Leadership & Organization Development Journal*, *30*(6), 498-521.

Chen, H., & Qi, R. (2022). Restaurant frontline employees' turnover intentions: three-way interactions between job stress, fear of COVID-19, and resilience. *International Journal of Contemporary Hospitality Management*(ahead-of-print).

Chen, Y., Luo, X. R., & Li, H. (2022). Beyond adaptive security coping behaviors: Theory and empirical evidence. *Information & management*, *59*(2), 103575.

Chou, W.-y. S., Liu, B., Post, S., & Hesse, B. (2011). Health-related Internet use among cancer survivors: data from the Health Information National Trends Survey, 2003–2008. *Journal of Cancer Survivorship*, *5*, 263-270.

Connor-Smith, J. K., Compas, B. E., Wadsworth, M. E., Thomsen, A. H., & Saltzman, H. (2000). Responses to stress in adolescence: measurement of coping and involuntary stress responses. *Journal of consulting and clinical psychology*, *68*(6), 976.

Corman, A. (2023). The Human Element in Cybersecurity–Bridging the Gap Between Technology and Human Behaviour.

Dempsey, J., Moore, E., & Phillips, D. J. (2019). Veteran Tech Entrepreneurial Ecosystems.

Doherty, N. F., & Tajuddin, S. T. (2018). Towards a user-centric theory of value-driven information security compliance. *Information Technology & People*, *31*(2), 348-367.

Downs, E., Willemsen, P., Leff, D., Adigun, C., Kothapalli, S. S., Miller, L., Boynton, K., & Berndt, M. M. (2022). Grave errors: Exploring the influence of motion mechanics on learning outcomes in a virtual cemetery.

Florian, V., Mikulincer, M., & Taubman, O. (1995). Does hardiness contribute to mental health during a stressful real-life situation? The roles of appraisal and coping. *Journal of personality and social psychology*, *68*(4), 687.

Floyd, D. L., Prentice ‐ Dunn, S., & Rogers, R. W. (2000). A meta ‐ analysis of research on protection motivation theory. *Journal of applied social psychology*, *30*(2), 407-429.

He, M., Devine, L., & Zhuang, J. (2018). Perspectives on cybersecurity information sharing among multiple stakeholders using a decision ‐ theoretic approach. *Risk Analysis*, *38*(2), 215-225.

Hentea, M. (2008). Improving security for SCADA control systems. *Interdisciplinary Journal of Information, Knowledge, and Management*, *3*, 73.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, *43*(4), 615-660.

Johnson, J., Berg, T., Anderson, B., & Wright, B. (2022). Review of electric vehicle charger cybersecurity vulnerabilities, potential impacts, and defenses. *Energies*, *15*(11), 3931.

Kobasa, S. C. (1979). Stressful life events, personality, and health: an inquiry into hardiness. *Journal of personality and social psychology*, *37*(1), 1.

Li, L., Xu, L., & He, W. (2022). The effects of antecedents and mediating factors on cybersecurity protection behavior. *Computers in Human Behavior Reports*, *5*, 100165.

Maddi, S. R. (2006). Hardiness: The courage to grow from stresses. *The journal of positive psychology*, *1*(3), 160-168.

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of experimental social psychology*, *19*(5), 469-479.

Mathieson, K. (1991). Predicting user intentions: comparing the technology acceptance model with the theory of planned behavior. *Information Systems Research*, *2*(3), 173-191.

McCombie, S., Uhlmann, A. J., & Morrison, S. (2020). The US 2016 presidential election & Russia's troll farms. *Intelligence and National Security*, *35*(1), 95-114.

Merritt, M. (2020). Improving Veteran Transitions to Civilian Cybersecurity Roles. *NIST Special Publication*, *1500*, 16.

Milne, S., Sheeran, P., & Orbell, S. (2000). Prediction and intervention in health‐related behavior: A meta‐analytic review of protection motivation theory. *Journal of applied social psychology*, *30*(1), 106-143.

Mouloua, S. A., Ferraro, J., Mouloua, M., Matthews, G., & Copeland, R. R. (2019). Trend Analysis of Cyber Security Research Published in HFES Proceedings From 1980 to 2018. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*. https://doi.org/10.1177/1071181319631467

Nobles, C. (2018). Botching human factors in cybersecurity in business organizations. *HOLISTICA–Journal of Business and Public Administration*, *9*(3), 71-88.

Petersen, R., Santos, D., Wetzel, K., Smith, M., & Witte, G. (2020). Workforce framework for cybersecurity (NICE framework).

Ray, P. D., Kumar, R., Reed, C., & Agarwal, A. P. (2011). Interoperating Smart Grid Cyber Security Systems: Adaptive Risk Management across Unified OT and IT Domains.

Reeves, A., Delfabbro, P., & Calic, D. (2021). Encouraging employee engagement with cybersecurity: How to tackle cyber fatigue. *SAGE open*, *11*(1), 21582440211000049.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *The journal of psychology*, *91*(1), 93-114.

Safa, N. S., & Von Solms, R. (2016). An information security knowledge sharing model in organizations. *Computers in Human Behavior*, *57*, 442-451.

Savin, V. D., & Anysz, R. N. (2021). Cybersecurity threats and vulnerabilities of critical infrastructures. *American Research Journal of Humanities Social Science (ARJHSS)*, *4*(7), 90-96.

Shappie, A. T., Dawson, C. A., & Debb, S. M. (2020). Personality as a predictor of cybersecurity behavior. *Psychology of Popular Media*, *9*(4), 475.

Smith, A. D., & Rupp, W. T. (2002). Issues in cybersecurity; understanding the potential risks associated with hackers/crackers. *Information Management & Computer Security*, *10*(4), 178-183.

Stamp, J., Dillinger, J., Young, W., & DePoy, J. (2003). Common vulnerabilities in critical infrastructure control systems. *SAND2003-1772C. Sandia National Laboratories*.

Triplett, W. (2021). Establishing a cybersecurity culture organization. *Acta Scientific COMPUTER SCIENCES Volume*, *3*(8).

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & management*, *49*(3-4), 190-198.

Veale, M., & Brown, I. (2020). Cybersecurity. *Internet Policy Review*, *9*(4), 1-22.

Wong, J. Y.-H., Fong, D. Y.-T., Choi, A. W.-M., Chan, C. K.-Y., Tiwari, A., Chan, K. L., Lai, V., Logan, T., & Bartone, P. (2014). Transcultural and psychometric validation of the Dispositional Resilience Scale (DRS-15) in Chinese adult women. *Quality of life Research*, *23*(9), 2489-2494.

APPENDICES

APPENDIX 1 Survey Instrument

Qualifier Question:

- Are you an honorably discharged US Veteran?
- Are you employed full-time in an organization that requires internet access on computers and/or other mobile devices to complete job tasks and communicate?

Demographic Questions

- Age
- Gender
- Education
- Industry
- Years in military
- Discharged as Enlisted or Officer

Other Control Factor Questions

- The organization I work for has an established information security policy (Y/N)
- The organization I work for provides employees with information security training (Y/N)

The questions below are a 5-point Likert Scale, options are:

1 - Strongly Disagree

2 - Disagree

3 - Neutral

4 - Agree

5 - Strongly Agree

***Message:**

Instructions: Answer the following questions truthfully regarding your work habits.

Table 11 Survey Questions

Code	Construct	Questions	Source
Cyber_Intent_1	Cyber Intent - Device Securement	I set my computer screen to automatically lock if I don't use it for a prolonged period of time.	Eglemen, 2015

Cyber_Intent_2		I use a password/passcode to unlock my laptop or tablet.	Eglemen, 2015
Cyber_Intent_3		I manually lock my computer screen when I step away from it.	Eglemen, 2015
Cyber_Intent_4		I use a PIN or passcode to unlock my mobile phone.	Eglemen, 2015
Cyber_Intent_5	Cyber Intent - Password Generation	I regularly change my passwords even if I'm not forced to.	Eglemen, 2015
Cyber_Intent_6		I use different passwords for different accounts that I have.	Eglemen, 2015
Cyber_Intent_7		When I create a new online account, I try to use a password that goes beyond the site's minimum requirements.	Eglemen, 2015
Cyber_Intent_8		I do not include special characters in my password if it's not required.*	Eglemen, 2015
Cyber_Intent_9	Cyber Intent - Proactive Awareness	When someone sends me a link, I open it without first verifying where it goes.*	Eglemen, 2015
Cyber_Intent_10		I know what website I'm visiting based on its look and feel, rather than by looking at the URL bar.*	Eglemen, 2015
Cyber_Intent_11		I submit information to websites without first verifying that it will be sent securely (e.g., SSL, "https://", a lock icon). *	Eglemen, 2015
Cyber_Intent_12		When browsing websites, I mouseover links to see where they go, before clicking them.	Eglemen, 2015
Cyber_Intent_13		If I discover a security problem, I continue what I was doing because I assume someone else will fix it.*	Eglemen, 2015
Cyber_Intent_14	Cyber Intent - Updating	When I'm prompted about a software update, I install it right away.	Eglemen, 2015
Cyber_Intent_15		I try to make sure that the programs I use are up-to-date.	Eglemen, 2015
Cyber_Intent_16		I verify that my anti-virus software has been regularly updating itself.	Eglemen, 2015
PV1	Perceived Vulnerability	I feel that my chance of receiving an email attachment with a virus is high.	Anwar (2017)
PV2		It is likely that my organization's information and data is vulnerable to security breaches.	Anwar (2017)
PV3		I feel that my organization could become vulnerable to security breaches if I don't adhere to its information security policy.	Anwar (2017)
PV4		It is very likely that I will be a victim of a cyberattack in the future.	S. Vrhovec and A. Mihelič (2021)
PV5		My chances of becoming a victim of a cyberattack are very high.	S. Vrhovec and A. Mihelič (2021)
PV6		I strongly feel that I will become a victim of a cyberattack in the future.	S. Vrhovec and A. Mihelič (2021)
PS1	Perceived Severity	Having my computer infected by a virus because of opening a suspicious email attachment is a serious problem for me.	Anwar (2017)

PS2		If I violate my organization's security policy, the sanctions will put me in serious trouble.	Anwar (2017)
PS3		At work, having my confidential information accessed by someone without my consent or knowledge is a serious problem for me.	Anwar (2017)
PS4		Loss of data resulting from hacking is a serious problem for me.	Anwar (2017)
PS5		Having my computer infected by a virus because of opening a suspicious email attachment is a severe problem for me.	Li et al (2022)
PS6		At work, having my confidential information accessed by someone without my consent or knowledge is a severe problem for me.	Li et al (2022)
PS7		Loss of data resulting from hacking is a severe problem for me.	Li et al (2022)
RC1	Response Costs	I believe that checking the filename of the email attachment can help me avoid viruses that may infect my computer.	Anwar (2017)
RC2		I believe that compliance with my organization's information security policy will reduce the risk of losing valuable work.	Anwar (2017)
RC3		Cyber security training makes me feel more equipped to deal with security problems on the computer.	Anwar (2017)
RC4		It is inconvenient to check the security of an email with attachments.	Li et al (2022)
RC5		Changing the privacy setting on social media sites is inconvenient.	Li et al (2022)
RC6		Backing up a computer regularly is inconvenient.	Li et al (2022)
RE1	Response Efficacy	Complying with the information security policies in my organization will keep security breaches down.	Anwar (2017)
RE2		If I comply with information security policies, the chance of information security breaches occurring will be reduced.	Anwar (2017)
RE3		Careful compliance with information security policies helps to avoid security problems.	Anwar (2017)
RE4		Using information security technologies is an effective way to protect confidential information.	Anwar (2017)
RE5		Anti-spyware software works for protection	Johnston, 2010
RE6		Anti-spyware software is effective for protection	Johnston, 2010
RE7		When using anti-spyware software, a computer is more likely to be protected.	Johnston, 2010
SE1	Self-efficacy	My organization constantly reminds me to practice its computer and Internet security policies.	Anwar (2017)
SE2		I know how to apply security patches to operating systems.	Anwar (2017)

SE3		I feel confident in setting the Web browser to different security levels.	Anwar (2017)
SE4		I feel confident in handling virus-infected files.	Anwar (2017)
SE5		Anti-spyware software is easy to use	Johnston, 2010
SE6		Anti-spyware software is convenient to use	Johnston, 2010
SE7		I can use anti-spyware software without much effort.	Johnston, 2010
HCM1	Hardiness – Commitment	Most of my life gets spend doing things that are worthwhile.	(Aigbefo et al., 2020)
HCM2		By working hard, you can always achieve your goals.	(Aigbefo et al., 2020)
HCM3		I am really look forward to my work.	(Aigbefo et al., 2020)
HCM4		Trying your best at work really pays off in the end.	(Aigbefo et al., 2020)
HCM5		Most days, life is really interesting and exciting for me.	(Aigbefo et al., 2020)
HCR1	Hardiness – Control	When I make plans, I'm certain I can make them work.	(Aigbefo et al., 2020)
HCR2		If I am working on a difficult task, I know when to seek help.	(Aigbefo et al., 2020)
HCR3		Most of the time, people listen carefully to what I say.	(Aigbefo et al., 2020)
HCR4		What happens to me tomorrow depends on what I do today.	(Aigbefo et al., 2020)
HCH1	Hardiness - Challenge	It's exciting to learn something about myself.	(Aigbefo et al., 2020)
HCH2		I like a lot of variety in my work.	(Aigbefo et al., 2020)
HCH3		I often wake up eager to take up my life wherever it left off.	(Aigbefo et al., 2020)
HCH4		Changes in routines are interesting to me.	(Aigbefo et al., 2020)
FR1	Fear of Internet Security Attack	When it comes to my feelings and concerns about Internet security attacks, I fear exposure to Internet security attacks.	(Chen et al., 2022)
FR2		When it comes to my feelings and concerns about Internet security attacks, I worry about Internet security attacks.	(Chen et al., 2022)
FR3		When it comes to my feelings and concerns about Internet security attacks, I am anxious about potential loss due to Internet security attacks.	(Chen et al., 2022)
FR4		I am very afraid of cyberattacks.	S. Vrhovec and A. Mihelič (2021)
FR5		The prevalence of cyberattacks is terrifying.	S. Vrhovec and A. Mihelič (2021)
FR6		Potential losses due to cyberattacks are causing me strong discomfort.	S. Vrhovec and A. Mihelič (2021)

FR7	The danger of cyberattacks is alarming.	S. Vrhovec and A. Mihelič (2021)
***Denotes Reverse Coding**		

APPENDIX 2: Information Letter

INFORMATIONAL LETTER
CYBERSECURITY PROTECTION BEHAVIOR AMONG US MILITARY VETERANS IN WHITE-COLLAR JOBS

Hello, my name is Alex Djahankhah. You have been chosen at random to be in a research study about identifying the factors that determine cybersecurity behavior among US Veterans. The purpose of this study is to explore whether significant cybersecurity beliefs and behaviors exist in military veterans that enter the knowledge-based job market. If you decide to be in this study, you will be one of 385 people in this research study. Participation in this study will take 30 minutes of your time. If you agree to be in the study, I will ask you to do the following things:

1. Review and provide consent to take this study.

2. Answer multiple-choice survey questions via Qualtrics.

There are no foreseeable risks or benefits to you for participating in this study. This study is expected to benefit society through the possibility of monetary compensation for completing the survey.

You will receive a payment of $3 for your participation three days after survey completion. There are no costs to you for participating in this study. If you have questions while taking part, please stop me and ask.

You *will* remain anonymous.

If you have questions for one of the researchers conducting this study, you may contact Alex Djahankhah at +81 090-1734-1871.

If you would like to talk with someone about your rights of being a subject in this research study or about ethical issues with this research study, you may contact the FIU Office of Research Integrity by phone at 305-348-2494 or by email at ori@fiu.edu.

Your participation in this research is voluntary, and you will not be penalized or lose benefits if you refuse to participate or decide to stop. You may keep a copy of this form for your records.

VITA

ALEX DJAHANKHAH

Born, New York, New York

2009-2011	B.A., Mathematics Florida Gulf Coast University Fort Myers, Florida
2017-2019	M.S., Information Management MBA Arizona State University Tempe, Arizona
2021 -2024	Doctoral Candidate Florida International University Miami, Florida
	US Marine Corps III MEF Information Group Okinawa, Japan