Spring 4-2022

A False Sense of Security - Organizations Need a Paradigm Shift on Protecting Themselves against APTs

Srinivasulu R. Vuggumudi

A False Sense of Security—Organizations Need a Paradigm Shift on Protecting Themselves against APTs

A dissertation submitted to Dakota State University in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

in

Information Systems

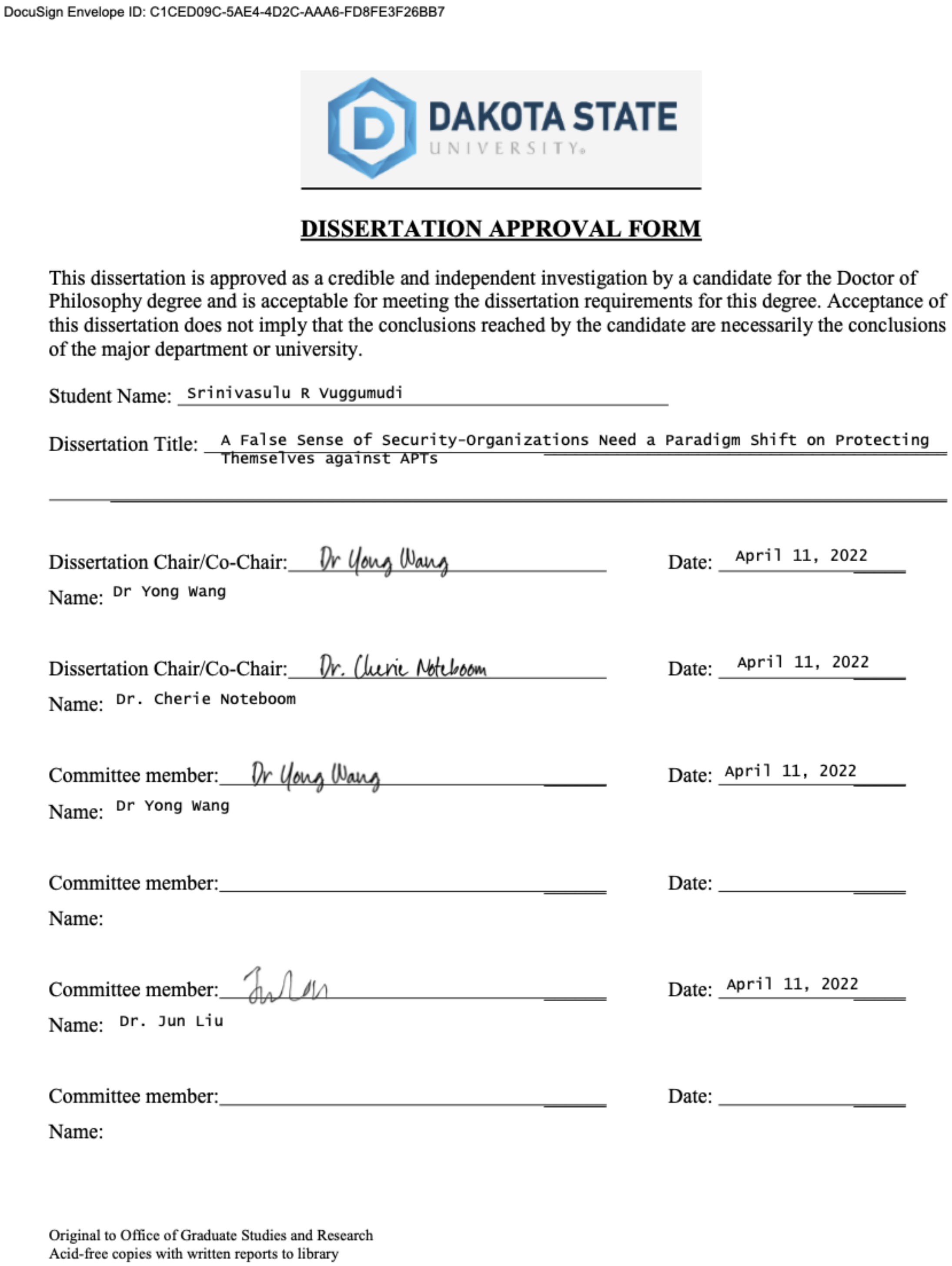
May 2022

By
Srinivasulu R. Vuggumudi

Dissertation Committee:

Dr. Yong Wang
Dr. Jun Liu
Dr. Cherie Noteboom

DISSERTATION APPROVAL FORM



DocuSign Envelope ID: C1CED09C-5AE4-4D2C-AAA6-FD8FE3F26BB7

DAKOTA STATE UNIVERSITY

DISSERTATION APPROVAL FORM

This dissertation is approved as a credible and independent investigation by a candidate for the Doctor of Philosophy degree and is acceptable for meeting the dissertation requirements for this degree. Acceptance of this dissertation does not imply that the conclusions reached by the candidate are necessarily the conclusions of the major department or university.

Student Name: Srinivasulu R Vuggumudi

Dissertation Title: A False Sense of Security-Organizations Need a Paradigm Shift on Protecting Themselves against APTs

Dissertation Chair/Co-Chair: Dr Yong Wang Date: April 11, 2022
Name: Dr Yong Wang

Dissertation Chair/Co-Chair: Dr. Cherie Noteboom Date: April 11, 2022
Name: Dr. Cherie Noteboom

Committee member: Dr Yong Wang Date: April 11, 2022
Name: Dr Yong Wang

Committee member: Date:
Name:

Committee member: Date: April 11, 2022
Name: Dr. Jun Liu

Committee member: Date:
Name:

Original to Office of Graduate Studies and Research
Acid-free copies with written reports to library

ACKNOWLEDGMENT

I would like to express my sincere gratitude to everyone who helped make this thesis possible.

First and foremost, I would like to acknowledge my research advisor Dr. Yong Wang, who has provided me with a constant source of inspiration and encouragement. I am grateful for the opportunity to work with him and for his insightful critiques and continuous guidance, without which this thesis would not have been possible. In addition, I would like to thank my committee members, Dr. Cherie Noteboom and Dr. Jun Liu, for their support and guidance during the initial and final stages of the research. I would also like to thank Kaushik Ragothaman, my fellow research student, who helped me brainstorm and co-authored publications.

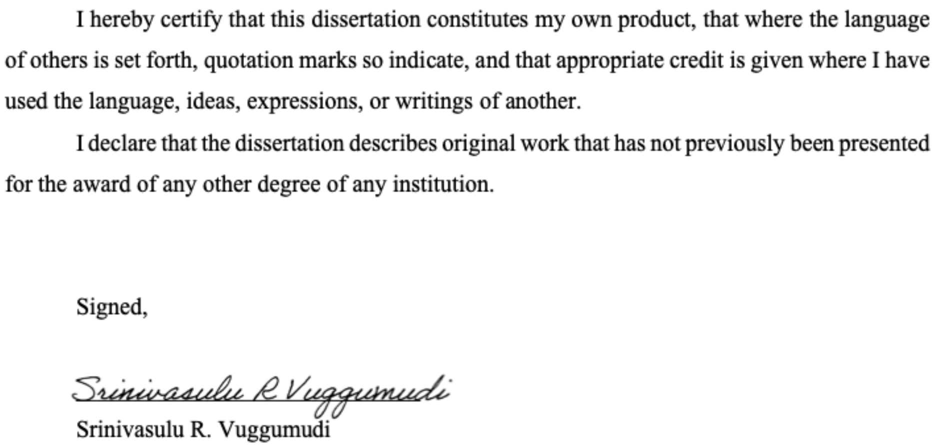
My family and friends have greatly supported this research, culminating in seven years of distance learning. For my daughter and wife, my apologies for missing family time and events. I thank both of you for supporting me, without which I would have stopped these studies a long time ago.

Finally, I thank God Almighty, who made me discover my life’s purpose and for His guidance.

ABSTRACT

Organizations Advanced persistent threats (APTs) are the most complex cyberattacks and are generally executed by cyber attackers linked to nation-states. The motivation behind APT attacks is political intelligence and cyber espionage. Despite all the awareness, technological advancements, and massive investment, the fight against APTs is a losing battle for organizations. An organization may implement a security strategy to prevent APTs. However, the benefits to the security posture might be negligible if the measurement of the strategy's effectiveness is not part of the plan. A false sense of security exists when the focus is on implementing a security strategy but not its effectiveness. This research verifies whether organizations are in a false sense of security while preventing APT attacks, what factors influence the false sense of security, and whether organizational culture influences factors contributing to the false sense of security. The research method utilized was survey-based quantitative research. Confirmatory Factor Analysis (CFA) and Structural Equation Modeling (SEM) were employed in the research model evaluation and hypotheses testing. The data analysis found that the sense of security value among the employees is low, which proves that employees are not confident about their organization's cybersecurity posture and organizations are in a false sense of security. Since Security Awareness and Training, Security Controls, Redundant IDS/IPS, and Cybersecurity Insurance positively influence the sense of security, recommendations were provided to enhance their effectiveness. The research study highlighted that sense of security of the employees is low when the security controls are ineffective. The contribution of this research is to highlight the paradigm shift required for organizations while setting up defenses against APTs. While organizations focus on setting up security controls to satisfy the compliance requirements, the research study outcome emphasizes the importance of the effectiveness of security controls. The dissertation includes limitations of the research and suggestions for further study.

DECLARATION



I hereby certify that this dissertation constitutes my own product, that where the language of others is set forth, quotation marks so indicate, and that appropriate credit is given where I have used the language, ideas, expressions, or writings of another.

I declare that the dissertation describes original work that has not previously been presented for the award of any other degree of any institution.

Signed,

Srinivasulu R Vuggumudi

Srinivasulu R. Vuggumudi

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

Background of the Problem

The United States Air Force coined the phrase advanced persistent threat (APT) in 2006 (Betlich, 2010). An advanced persistent threat (APT) is a prolonged, aimed attack on a specific target in which cyber attackers gain access to a system or network and remains there for an extended period without being detected. The goal of APT attackers is generally stealing data and intellectual property. Advanced Persistent Threats (APTs) occupy news headlines often because of the potential damage they can cause regarding reputation, data (both consumer and corporate), and intellectual property. The infamous cyberattack on credit rating agency Equifax in February of 2017 is still in people's minds. The US Department of Justice confirmed that a team of hackers from the Chinese military was behind the attack on Equifax, in which personally identifiable information (PII) of over 147.9 million people was stolen (Sass, 2020). The computer security firm Eset recently reported that state-sponsored Russian hackers carried out a cyberattack on San Francisco International Airport (SFO) in March 2020. San Francisco International Airport (SFO) revealed that some users of its websites (SFOConnect.com and SFOConstruction.com) might have had their logins stolen by Russian hackers. APTs are a looming threat to large and small enterprises; several vaunted enterprises like Google, RSA, DuPont, Walt Disney, Johnson & Johnson, Morgan Stanley, Sony, General Electric, etc., were victims of APTs (Grimes, 2011).

NIST defines APT as "An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization, or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives" (NIST, 2013). Richard Bejtlich, a well-known cybersecurity expert, explains what APT stands for as follows (Betlich, 2010):

- **Advanced** means the attackers are highly skilled in hacking techniques and sophisticated hacking tools. The attackers start their intrusion efforts by exploiting well-known vulnerabilities. They can up their game to research new vulnerabilities and develop custom exploits if the initial intrusion efforts are unsuccessful.
- **Persistent** means the attackers are focused on the target and set to accomplish a mission. They are not hit and run attackers, but they remain the victim's network evading detection to steal sensitive data over a prolonged period. Persistent does not necessarily mean that the attackers continuously perform malicious activities in the victim's network. The attackers perform the minimum action needed to execute their objectives and avoid detection.
- **Threat** means the adversary is not merely a piece of malicious code. The attackers are organized, funded, and motivated, and their successful intrusion attempts result in potential damage to the organization's finances and reputation.

APTs are distinct from hit and run hacking events because APTs have the following distinguishing characteristics: Customized, Persistent, Organized, Funded, Sophisticated (Advanced tools and techniques), and Timeliness. Nation-state sponsored agents or cybercriminals execute advanced Persistent Threats (APTs). APTs are prolonged and targeted cyberattacks. Cybercriminals use multiple vectors and entry points to navigate defenses to breach into enterprise networks and evade detection for months. APTs present a challenge for organizations because of their complexity, duration, and undetectability.

The dictionary definition of "false sense of security" is simply the belief that some situation is safer than it is (Merriam-Webster, 2022). Technologies and processes often provide organizations with a false sense of security. "Attackers consistently prey on companies that have what cybersecurity experts call a ‘false sense of security’ when it comes to relying too much on technology to defend their networks” (Pilkey, 2017). Enterprises rely on technical solutions to protect themselves from APTs and are in a false sense of security. Though advanced technology solutions are available and currently used in organizations, APTs are still happening. Whether large, medium, or small, no organization is immune to these attacks (Thummala, 2016). An organization may implement a security strategy, but the benefit to the security posture might be negligible. A false Sense of Security exists when the focus is on implementing a security strategy but not on the effectiveness of the security strategy.

Statement of the Problem

The purpose of our research is to determine why technological solutions fail to protect organizations from APTs and decide which security controls need to be implemented, fine-tuned, and enhanced, along with technical solutions to protect organizations from APTs. Our research study identifies the missing pieces of the puzzle to defend organizations from APT attacks. Our research study benefits organizations in protecting their data and intellectual property from APT actors, who are generally cybercriminals based in foreign countries. The research study identifies security policies, procedures, and configurations to focus on in the pursuit of defeating advanced persistent threats (APTs). The research is survey-based quantitative research; based on the survey outcome, we propose remediations regarding implementing and enhancing security policies, procedures, and configurations to set up defenses against APTs.

Objectives of the Research

- Identify the gap between how employees working in the cybersecurity domain feel about cybersecurity and the implemented cybersecurity practices. Verify whether there is a false sense of security among organizations by relying too much on technical solutions and less on best practices or not. Identify what is missing in setting up defenses against APT attacks.
- Identify the gaps left by the standard security testing methodologies like OSSTMM (Open Source Security Testing Methodology Manual), OWASP (Open Web

Application Security Project), NIST (National Institute of Standards and Technology), PTES (Penetration Testing Methodologies and Standards), and ISSAF (Information System Security Assessment Framework).

- Identify the best practices that enhance defenses against APTs when implemented along with the existing technologies.

Research Questions

The escalation in the number of cyber incidents shows no sign of abating. Despite all the awareness, technological advancements, and massive investment, the fight against APTs is a losing battle. It seems logical to look at how APT defenses are set up and consider whether organizations are in a false sense of security. Shall organizations need to think about APT detection strategies? The answer could be lurking in the shadows. In this research, we aim to contribute to the cybersecurity domain by verifying whether there is a false sense of security among organizations. If a false sense of security does exist among organizations, our research highlights what is missing when considering the defenses to prevent APT attacks.

Our research begins with the following questions:

RQ1. Are organizations in a false sense of security while relying on off-the-shelf tools to protect against APT attacks?

Implementing and improving security policies, procedures, and configurations is the first and most crucial step in the pursuit of defeating advanced persistent threats (APTs) (Nadeem, 2016). Our research question provides an answer to whether organizations are in a false sense of security by focusing more on tools and less on security policies, procedures, and configurations or not.

RQ2. What are the most critical factors (practices/controls) contributing to the false sense of security? Is there any relationship among these factors?

Cybersecurity program provides a roadmap for security management practices and controls. The success of the security program depends on the effectiveness of these practices and controls. What factors (practices/controls) contribute most to the false sense of security? Is there a correlation among factors (practices/controls) for the security program's success or absence of the false sense of security?

RQ3. Does organizational culture influence the setup of defenses against APT attacks?

"Information security culture is a subculture of an organization's culture. (Huang & Pearlson, 2019). To enhance an organization's cybersecurity culture, management must implement the latest technology and invest in the organizational culture (Huang & Pearlson, 2019). Since organizational culture is important in cybersecurity, our research question provides an answer to how a false sense of security is present among organizations with different organizational cultures.

Dissertation Outline

The remainder of the dissertation is organized as follows. Chapter 2 surveys the relevant literature for the problem area defined in Chapter 1. The chapter ends with a summary of findings from the literature review. Chapter 3 presents the research design, hypotheses statements, research method, and implementation. The chapter also includes a description of research constructs and an operational definition of constructs. Chapter 4 presents data analysis. Data analysis includes the assessment of measurement model, assessment of structural model, and hypotheses testing. The chapter also presents a discussion of data analysis. Chapter 5 discusses what measures organizations consider in improving employees' sense of security to defend against APT attacks. Chapter 6 starts with the summary of research completed. The chapter presents limitations of the research. The chapter presents the research contributions and ends with discussing the future work.

CHAPTER 2

LITERATURE REVIEW

The literature review explored the cyber kill chain framework developed by Lockheed Martin, challenges with advanced cybersecurity tools, compliance frameworks, and security testing methodologies. The cyber kill chain framework employs tools for the identification and prevention of cyber intrusions activity.

Cyber Kill Chain Framework by Lockheed Martin

Kill Chain is a term that originated in the military, which defines a series of steps an adversary follows to attack a target. In 2011, using the Kill Chain concept, Lockheed Martin developed the Cyber Kill Chain framework (Spitzner, 2019). The Cyber Kill Chain identifies what the adversaries must complete achieving their objectives (Lockheed Martin, 2019). By understanding the Cyber Kill Chain framework, defenders are better prepared to identify and stop attackers at each of the respective stages. The closer to the beginning of the cyber kill chain of an attack, the better the attack can be stopped. Moreover, the more stages at which defenders can intercept the attackers, the chances of detecting and terminating the attacks are higher. So, defenders should be equipped with tools to detect and prevent APTs in all cyber kill chain stages. There are seven stages in Lockheed Martin's cyber kill chain as shown in Figure 1: 1) Reconnaissance, 2) Weaponization, 3) Delivery, 4) Exploitation, 5) Installation, 6) Command & Control, and 7) Action on Objectives (Lockheed Martin, 2019).

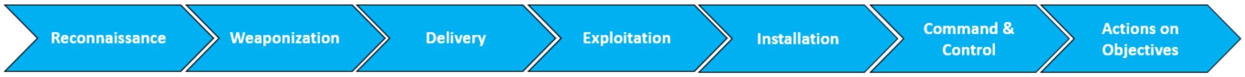


Figure 1. Lockheed Martin's Cyber Kill Chain

Reconnaissance

In the reconnaissance stage, adversaries begin with a target organization, gather information about the target, and look for vulnerabilities. Information gathering activities can be passive or active (Death, 2018; Pols, 2017). In the active information method, adversaries run scanning and fingerprinting tools against an organization’s systems deployed in the demilitarized zone (DMZ) to uncover ports that are vulnerable to exploitation and find out the technology stacks of the systems. Adversaries can also identify security systems in place, such as firewalls, intrusion prevention systems, and authentication mechanisms. In the passive information gathering method, adversaries gather information about the organization and its employees using publicly available databases and social media networks.

Weaponization

During the weaponization stage, adversaries do not interact with the targeted victim but devise methods to get inside the victim’s network. In the weaponization stage, the adversaries develop customized malware to exploit the vulnerabilities discovered during the reconnaissance stage (Death, 2018). Customized malware could be delivered by social engineering methods or exploitation of vulnerabilities discovered in the systems during the reconnaissance stage.

Delivery

In the cyber kill chain's delivery stage, the adversaries transmit the custom-developed malware to the victim’s systems for exploitation (Hutchins et al., 2011). Spear-phishing attack targeting internal employees of the organization is the most common method to transmit malware into the organization’s internal systems (Verizon, 2019). Ninety percent of APT groups use spear-phishing as an effective way to deliver malware into a company's internal network (Positive Technologies, 2019).

Exploitation

In the exploitation phase, the attacker's code triggers exploitation. Attackers target an application or operating system vulnerability for exploitation. Intruders may merely perform exploitation by persuading the victim to open an executable attachment or leverage a feature of the operating system that auto-executes code (Croom, 2010).

Installation

At the installation stage, the already delivered malware downloads additional components to create a persistent backdoor or another ingress accessible to the adversary outside the victim’s network for an extended period (Death, 2018).

Command & Control

In the command and control stage, the adversaries establish a command channel to the victims’ systems or network to remotely manipulate the victim. At this stage, adversaries can move deeper into the network, exfiltrate data, and conduct destructive operations like Denial of Service (DoS) or Distributed Denial of Service (DDoS) (Death, 2018). At this stage, the adversaries are equipped with hands-on keyboard access to the victim’s systems to execute actions to achieve their objectives (Croom, 2010).

Actions on Objectives

The actions and objectives of the attackers are dependent on their specific mission. The most common objective is data exfiltration: collecting, encrypting, and stealing information from the compromised system (Croom, 2010). The adversaries devise methods to avoid detection by the victim’s monitoring/alerting systems while performing their intended actions.

APT Prevention and Detection Tools

The following table (Table 1) provides the most important tools used at various cyber kill chain stages to stop APT attacks. Both Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) tools process data from all stages of the cyber kill chain. Besides, they are relatively new compared to the other tools mentioned in Table 1. Thus, SIEM and SOAR tools are covered more in the discussion.

Table 1. Available Tools to Stop APT Attacks

Cyber Kill Chain Stage	Type of Tools	Description of Tools
Reconnaissance	Firewall, Web Analytics tool (Lockheed Martin Corporation, 2015)	• Firewalls are the first layer of defense against APT attacks because they play the role of controlling network visibility and enforcing security policies (TrendMicro, 2017). Firewalls segment organizations' networks into zones and control inbound and outbound traffic between network zones and the Internet by enforcing the organization's security policies. Configuration of firewalls is critical to prevent APTs. Firewalls must be configured accurately and intelligently to analyze and block any network traffic that signals APTs (Wool, 2016). • Web servers are public-facing assets of organizations. Web Analytics tools provide the ability to correlate logging events based on time and user activity. Abnormal user activities like intelligence gathering on the website, repeatedly

		entering invalid inputs, etc., indicate an intention to breach (Coleman, 2016; Lockheed Martin Corporation, 2015)
Weaponization	Network Intrusion Detection System (NIDS) Network Intrusion Prevention System (NIPS) (Lockheed Martin Corporation, 2015)	• NIDS tools monitor network-based traffic and activity. NIDS tools detect malicious activities by examining network activity logs and network packets moving across the network. NIDS tools use anomaly-based and signature-based detection techniques to analyze log files for malicious activities (Belding, 2019). • NIPS tools are similar to NIDS tools, except for one significant difference; NIPS tools take appropriate action when malicious activity is detected (Belding, 2019).
Delivery	Proxy Filter, Inline Anti-Virus (Lockheed Martin Corporation, 2015)	• Proxy Server/Web Filter helps organizations with web content filtering, blocks users from accessing known malicious sites, spam/phishing sites, proxy avoidance sites, pornography, and all other categories of websites deemed unnecessary for normal business operations (Frenz & Diaz, 2017). • The objective of an inline antivirus solution is to prevent malware delivered via email. During each Simple Mail Transfer Protocol (SMTP) session, the Inline antivirus solution effectively stops malicious software at the email entrance to your network (MDaemon Technologies, n.d.).
Exploitation	Host Intrusion Detection System (HIDS), Vendor Patch, Enhanced Mitigation Experience Toolkit (EMET) (Lockheed Martin Corporation, 2015)	• Host Intrusion Detection System (HIDS) works by taking a snapshot of the existing system files and comparing it to the previous snapshot. If the critical system files were modified or deleted, the alert is sent to the administrator to investigate (Rozenblum, 2001). • “Patch management can be the most effective tool used to protect against vulnerabilities and the least expensive to maintain if implemented effectively” (Ruppert, 2007). Patch Management System (PMS) is a tool that distributes, installs, and manages patches (Seo & Moon, 2006). PMS can automate the patching of operating systems

		and applications running on endpoints and servers. • The Enhanced Mitigation Experience Toolkit (EMET) prevents attackers from gaining access to computer systems. EMET works by anticipating the most common techniques attackers might use to exploit computer systems vulnerabilities and help protect by diverting, terminating, blocking, and invalidating those actions and techniques. Data Execution Prevention (DEP) is a feature of EMET. DEP can help protect your computer by monitoring your programs to use system memory safely. If DEP notices a program misusing computer memory, it closes the program and notifies the user (Microsoft Corporation, 2016).
Installation	HIDS, AntiVirus (Lockheed Martin Corporation, 2015)	• HIDS • Anti Virus
Command & Control (C2)	NIDS, Firewall, NIPS (Lockheed Martin Corporation, 2015)	• NIDS • Firewall • NIPS
Actions on Objectives	Audit Log Analysis, Data Loss/Leak Prevention (DLP) (Lockheed Martin Corporation, 2015; Security Boulevard, 2018)	• Security Information and Event Management (SIEM) tools collect, and aggregate log data generated in the organization's infrastructure (host systems, applications, network, and security devices/applications such as firewalls and antivirus filters). The SIEM software then analyzes the data aggregated to identify security-related incidents and events, such as successful and failed logins, malware activity, and other possibly malicious activities. It sends alerts to the security operations team (Pratt, 2017). • Data leakage prevention (DLP) tool is a solution for identifying, monitoring, and protecting sensitive data as per the organization's data security policies. A DLP tool's main objective is to prevent sensitive data from leaking out of the organization (Razi K, 2017).

Challenges with Prevent APTs

There are various tools to detect and prevent APTs at all stages of the cyber kill chain offered by several vendors. According to Radicati, the market for APT protection solutions is expected to grow from $4.3 billion in 2019 to over $9.4 billion by 2023 (The Radicati Group Inc., 2019). According to FireEye, the global median dwell time (the number of days an attacker is present on the victim's network before they are detected) decreased year after year, 101 days in 2017, 78 days in 2018, and 56 days in 2019 (FireEye, 2019; Kovacs, 2020). The decreasing dwell time trend is good. However, APT attacks are still happening even though organizations are taking measures to detect and prevent APT attacks by installing tools. "Global data from 2018 found that 64 percent of all FireEye managed detection and response customers who were previously Mandiant incident response clients were targeted again in the past 19 months by the same or similarly motivated attack group" (FireEye, 2019).

It is difficult to detect APTs in the early stages of the cyber kill chain. Many APT attackers use customized malware exploiting zero-day vulnerabilities in the target's systems. APT attackers are skilled and focused adversaries who can use multiple vectors and entry points to navigate around defenses to breach into the victim's network and evade detection for months. The more advanced the tools to detect and prevent are, the more advanced and skilled adversaries are. This is an ongoing race between defenders and adversaries where adversaries are gaining the upper hand. There are protocols to follow for a vendor to develop and release a tool into the market, but adversaries can build and use tools without any obstructions. Tools developed by vendors to detect and prevent APTs are general in nature to cater wider market, though they are meant to apply at a specific stage of the cyber kill chain. Adversaries gain the upper hand because tools developed by them are customized for specific targets.

Off-the-shelf solutions for individual servers or endpoints and network protection are hopelessly outclassed by cyber attackers. Cyber attackers always devise a new technique to bypass anti-malware software, sandboxes, and intrusion detection/prevention systems (IDS/IPS) (Positive Technologies, 2019). "Advances in attacker sophistication have not been matched by similar defensive advances. The concept of keeping the internal, trusted network separated from the external, untrusted one (i.e., boundary protection) has become obsolete. The use of blacklists or signatures for attack detection is practically useless against sophisticated attackers. The security industry, having spent decades developing security products such as anti-malware solutions and intrusion detection/prevention systems, refuse to admit the shortcomings of these products" (Virvilis-Kollitiris, 2015). Employees are the first line of defense for any organization. Therefore, they need to have security education and a sober understanding of the protection systems in place to secure their key assets.

Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) tools have been used in Security Operations Centers (SOCs). Both SIEM and SOAR tools are considered advanced tools for cybersecurity operations; however, SOAR tools are not as common as SIEM tools. Security Information and Event Management (SIEM) solutions collect and analyze the event in system logs. The SIEM tools' input is generally logs from firewalls, intrusion detection/prevention systems, network appliances, database servers, application servers, etc. SIEM tools aggregate and correlate event data logs from multiple systems and analyze that data to catch abnormal behavior indicating potential cyberattacks. SIEM tools are equipped with analytics and machine learning tools capabilities. SIEM tools check for event patterns and correlate event information between devices for any anomalous activity and issue an alert when necessary. SIEM tools are not created to unify people, processes, and technologies within a security operations center (SOC). "While the SIEM detects the potential security incidents and triggers the alerts, a SOAR solution then takes these alerts to the next level, responding to them, triaging the data, and taking remediation steps where necessary" (DFLabs, 2019). SOAR tools add value to SOCs as they automate and orchestrate time-consuming, manual tasks, including opening a ticket in a tracking system, such as Jira, without requiring any human intervention. Using SOAR tools SecOps team can automate incident response workflows.

SIEM and SOAR tools are advanced-level cybersecurity tools and appear to have the potential to detect APTs, but there are challenges with these advanced-level tools. "SIEM tools provide a central place to collect events and alerts – but can be expensive, resource-intensive, and customers report that it is often difficult to resolve problems with SIEM data" (Petters, 2020). Most of them will reflect the following as major issues with the adoption and operations of SIEM products: 1) Initial adoption takes time because of the time needed for coordination from various IT organization stakeholders. 2) Time to value realization is very high. 3) Correlation of events is difficult to achieve, leading to a high number of false positives. 4) SIEMs are very high maintenance products. 5) Out-of-the-box reports from SIEM products are mostly useless and require quite a bit of work to get meaningful reports. 6) Operational costs outweigh the benefits (Shukla, 2019). SOAR tools are still not popular yet. According to Gartner, “By year-end 2022, 30% of organizations with a security team larger than five people will leverage SOAR tools in their security operations, up from less than 5% today” (Demisto, 2019). SOAR tools are still evolving, and reliance on SOAR tools for APT detection is not reliable yet. Charles Herring, Chief Technology Officer at Witfoo, says, “If you do not have the critical/basic controls in place, it makes no sense to do advanced controls like SOAR” (Herring, 2020).

Cyber attackers always devise a new technique to bypass anti-malware software, sandboxes, and IDS/IPS systems. Though SIEM and SOAR tools are advanced, there are implementation challenges to make the tools effective. Jurgen Kutscher, Executive Vice President of service delivery at FireEye, says, “FireEye Mandiant has seen organizations largely improving their level of cybersecurity sophistication, but combatting the latest threats is still a huge challenge for them” (Kovacs, 2020). The projection for APT protection solutions is expected to grow from $4.3 billion in 2019 to over $9.4 billion by 2023. However, organizations are not looking at the missing pieces of the puzzle to defend against APTs.

With the heavy focus on tools to prevent APT attacks, non-technical attack vectors like insider threat and social engineering are not given much-needed attention. The Verizon 2019 Data Breach Investigations report states that 34% of all breaches in 2018 were caused by internal actors (Verizon, 2019). In 2018, 60% of breach investigations can attribute successful social engineering as the conduit to the initial point of entry (Help Net Security, 2019).

The committed implementation of a cybersecurity framework is one of the missing pieces in the puzzle to defend against APTs. According to Cris Thomas, strategist, Tenable Network Security, cybersecurity frameworks help organizations create a solid baseline for measuring security effectiveness and meeting compliance requirements. Implementing security frameworks can be challenging without the tools, talent, and support from executive leadership. A study conducted by Tenable Network Security and the Center for Internet Security (CIS) found that 95% of organizations face significant challenges when implementing leading cybersecurity frameworks. The same study reports the top five impediments to cybersecurity framework implementation as follows: 1) Lack of trained staff; 2) Lack of necessary tools to automate controls; 3) Lack of budget; 4) Lack of appropriate tools to audit continuous effectiveness of controls; 5) Lack of integration among tools (Seals, 2013). Because of the implementation challenges of cybersecurity frameworks, most organizations implement cybersecurity frameworks just enough to satisfy auditing requirements.

Penetration testing is driven by a management directive as an activity to address the issue of cybersecurity but is not aligned with the actual intent of the testing. The use of penetration testing is commonly an objective to an adverse audit outcome or cybersecurity incident. Penetration testing used in this fashion provides little or no value to the organizations. Besides, penetration testing is only as good as the tools, the tester, and the methodology applied (Valli et al., 2014). The success of testing security controls depends on the selection of the right security testing framework, like MITRE's ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge), PTES (Penetration Testing Methodologies and Standards), etc. Security teams or organizations gravitate to compliance-type frameworks, ones with checkboxes that can represent a false sense of security and defense (Bromiley, 2020). Compliance-type frameworks are relatively static, and they do not cover the current threats. Red teaming activity is common in mature and security-focused organizations. The challenge with red teaming activity is time and money. Red teaming is not a possible activity for most organizations. Organizations implement multiple security controls to defend their security posture, but all security controls are not tested simultaneously. Testing all security controls simultaneously means all defenses are attacked at the same time. Testing all security controls simultaneously is not a practice covered by any security testing framework. One example of testing all security controls at the same time is simulating data exfiltration activity. When data exfiltration is simulated, DLP solution, firewalls, NIDS, HIDS, and SIEM are tested. Testing DLP, firewalls, NIDS, HIDS, and SIEM independently does not give much value compared to simultaneous testing all controls in the exfiltration path. In an organization, different stakeholders are responsible for different security defenses (controls). Thus, testing all defenses at a single point in time requires challenging coordination but is necessary.

Security Controls to Remediate APTs

Immensely few academic publications contributed to the remediation strategies exclusively for APT attacks. Bukac et al. proposed a response strategy based on the kill chain concept (Bukac et al., 2014). This strategy aims to collect as much information as possible when an incident occurs and then perform remediation efforts. Messaoud et al. proposed an APT lifecycle model based on attackers' objectives (Messaoud et al., 2017). They suggested four protection technologies. However, they all focus on only technical controls. Brewer et al. suggested an analytics-driven approach to defending against APTs (Brewer, 2014). Mohsin and Anwar discussed an ontology-based approach that uses cyber threat intelligence to evaluate IoT networks against APT attacks (Mohsin & Anwar, 2016). In addition to the remediation strategies, risk management approaches are proposed for the APTs. In (L. X. Yang et al., 2018), Yang et al. developed a risk management approach based on game theory to efficiently allocate resources to fix insecure hosts in an organization. In (X. Yang et al., 2017), the risk assessment is based on state evolution and is modeled as a constrained optimization problem. The risk is measured by the maximum expected loss. In this work, an organization's network is assumed to be fixed; however, in real terms, the network configuration may vary over time. Granadillo et al. proposed a dual approach by evaluating a given security countermeasure's technical and financial impacts by performing a case study on APTs (Daniel Gonzalez Granadillo et al., 2015). Adelaive et al. conducted a systematic review on the mitigation effects of APT attacks (Adelaiye et al., 2018). They identified twelve mitigation techniques, almost all of them being technical controls. Only a limited number of articles in their review discussed security awareness. Their study identifies the low utilization of human intelligence and behavioral patterns in preventing and detecting APT attacks. Further, the level of effectiveness of the mitigation strategies is not obtainable from their study. No research study was found on the topic of the effectiveness of security controls in the context of preventing APT attacks.

Chapter Summary

In our literature review, we found the following:

- Cyber attackers outclass off-the-shelf solutions.
- Employees need security education and a sober understanding of the protection systems in place to secure their key assets.
- If critical/basic security controls not in place, it makes no sense to do advanced controls like SOAR.

- Heavy focus is usually on tools to prevent APT attacks. Non-technical attack vectors like insider threat and social engineering are not given much-needed attention.
- The effectiveness of security controls in preventing APT attacks has not been studied.

CHAPTER 3

RESEARCH DESIGN, METHODOLOGY, AND IMPLEMENTATION

During the literature review, we found the likely causes contributing to the losing battle of corporations with APTs. Based on the literature review, in this chapter, we formally define the research constructs, research model, operational definition of constructs, hypothesis statements, and research method. The chapter also details research implementation and ends with the chapter summary.

Research Design

The field of information systems research has contributed several theories pertaining to the adoption and usage of technology. Theoretical models such as the Technology Acceptance Model (TAM) (Davis, 1985), the Theory of Planned Behavior (Ajzen, 1985), and the Health Belief Model (Becker, 1974) exist and have been utilized in empirical research in information security. However, the models (Ajzen, 1985; Becker, 1974; Davis, 1985) are based on behavioral constructs and utilized to target individual behavior. There is a lack of empirical research to evaluate organizational security strategies based on employees' subjective feelings on security. Therefore, we investigate this problem and propose a theoretical model for evaluating organizational security strategies in terms of the sense of security.

To formulate a research model that theorizes various factors that influence the sense of security, we selected independent, dependent, and moderator variables from our literature review. Employees’ confidence level about the strategic organizational activities of security represents the sense of security. The key factors considered in the model include security awareness and training, converged testing, security controls, segmentation, redundant IDS/IPS, insider threat prevention, and cybersecurity insurance. The proposed research model is illustrated in Figure 2.

The common methods used to mitigate APTs include: 1) anomaly detection, 2) whitelists, 3) blacklists, 4) intrusion detection system (IDS), 5) awareness, 6) deception, 7) cryptography, 8) traffic/ data analysis, 9) Security Information and Event Management (SIEM), 10) pattern recognition, 11) risk assessment, 12) multi-layer security (Adelaiye et al., 2018). Our selection of independent variables was primarily based on these methods. The NIST Special Publication 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations" also influenced our selection of constructs. NIST provides a comprehensive framework of controls that organizations can follow to mitigate APTs. All the independent variables are based on the current threat landscape and the industry best practices. If the threat landscape changes, new independent variables could be needed for new security controls to emerge.

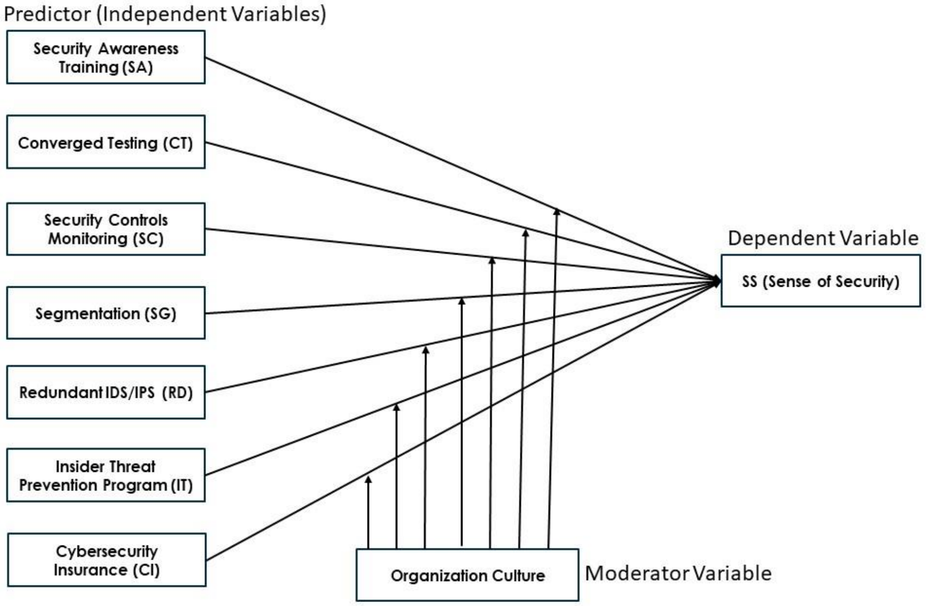

Predictor (Independent Variables)
Security Awareness Training (SA)
Converged Testing (CT)
Security Controls Monitoring (SC)
Segmentation (SG)
Redundant IDS/IPS (RD)
Insider Threat Prevention Program (IT)
Cybersecurity Insurance (CI)
Dependent Variable
SS (Sense of Security)
Organization Culture
Moderator Variable

Figure 2. Theoretical Model

Independent Variables (Latent Variables)

We started our selection of independent variables based on the standard methods used to mitigate APTs: 1) Anomaly Detection 2) Whitelists 3) Blacklists 4) Intrusion Detection System (IDS) 5) Awareness 6) Deception 7) Cryptography 8) Traffic/ Data analysis 9) SIEM 10) Pattern Recognition 11) Risk assessment 12) Multi-layer security (Adelaiye et al., 2018).

We continued our exploration of selecting independent variables by doing an extensive literature review of APT attacks. We selected our independent variables based on the information available on the notorious cyberattacks, industry best practices, and standard methods to mitigate APTs found in our literature review.

Some of the standard methods used to mitigate APTs can be grouped into one control. For example, Anomaly Detection, Intrusion Detection System (IDS), and Traffic/ Data analysis are one control because IDS systems work based on traffic/data analysis and anomaly detection. One control or one independent variable IDS includes three APT mitigation methods: Anomaly Detection, IDS, and Traffic/ Data analysis. Similarly, Whitelists and Blacklists can be treated as one control or independent variable Firewall because Whitelists and Blacklists are associated with Firewall implementation.

As the cyberattacks continue to grow, the security controls or defense mechanisms to prevent those are also expanding. New controls are adopted to changing threats and vulnerabilities. Every new control can be a candidate to be an independent variable in future research. Our selection of independent variables is based on the current threat landscape and industry best practices. If the threat landscape changes need for new security controls emerges, and so do new independent variables.

Security Awareness and Training (SA)

“Security awareness training is a usually overlooked factor in most of implemented information security programs” (Al-Daeef et al., 2017). In the context of Information Technology (IT), security awareness and training programs are the typical means used to communicate security requirements and appropriate behavior (Bada et al., 2014). Industry compliance standards/requirements make organizations run security awareness programs. Security awareness programs fail; failure means they do not have an impact. IT security awareness and training program can quickly become obsolete if not updated with the technology advancements, IT infrastructure and organizational changes, and shifts in organizational mission and priorities (Wilson & Hash, 2003). If organizations do not keep their security awareness and training programs current, employees find no value and lose motivation.

If compliance is the goal of an organization, it is much simpler to achieve. Achieving an effect through user behavior change is a far more significant challenge. The “2020 IBM X-Force Threat Intelligence Index” noted that “Over 8.5 billion records were compromised in

2019, a number that's more than 200 percent greater than the number of records lost in 2018. The inadvertent insider can largely be held responsible for this significant rise. Records exposed due to misconfigured servers (including publicly accessible cloud storage, unsecured cloud databases, improperly secured rsync backups, or open internet-connected network area storage devices) accounted for 86 percent of the records compromised in 2019" (IBM, 2020).

Phishing is the number one attack vector for credential theft, and the root cause of nearly half of malware and ransomware infections. Security awareness programs educate employees to recognize phishing and other latest attack vectors essential to protecting data. Organizations need to keep their security awareness and training programs current and test users periodically on what is taught in the training programs. It is important for an organization to test employees and use punishment to reinforce the importance of being aware when clicking on links. Testing employees will result in employees proactively using caution when opening emails, attachments, and clicking on links (Carella et al., 2017).

Since the effectiveness of security awareness and training programs is significant to defend against APT attacks, we selected "Security Awareness and Training" as one of the independent variables in our study.

Converged Testing (CT)

"Technical or logical controls involve the hardware or software mechanisms used to manage access and to provide protection for resources and systems. As the name implies, it uses technology" (Chapple et al., 2018). Examples of logical or technical controls include authentication methods (such as usernames, passwords, smartcards, and biometrics), encryption, firewalls, and routers. "Administrative controls are the policies and procedures defined by an organization's security policy and other regulations or requirements. They are sometimes referred to as management controls. These controls focus on personnel and business practices" (Chapple et al., 2018). Examples of administrative controls include policies, procedures, hiring practices, background checks, data classifications, and labeling. During security testing (penetration testing, blue team testing, purple team testing, or red team testing), the focus is on technical controls. Our literature review did not find any testing methodology that includes technical and administrative controls in the security testing scope. We selected converged (administrative + technical controls) testing as an independent variable.

Cybersecurity Insurance (CI)

CISA defines cybersecurity insurance as "Cybersecurity insurance is designed to mitigate losses from a variety of cyber incidents, including data breaches, business interruption, and network damage" CISA (*Cybersecurity Insurance | CISA*, n.d.). Since APT attacks involve data exfiltration and an organization can go bankrupt after a successful cyberattack, we considered selected Cybersecurity Insurance as an independent variable to verify organizations' preparedness for APT attacks.

Security Controls (SC)

Michael de Crespigny, CEO of the Information Security Forum (ISF), says, "real cybersecurity is not about technical controls. You need those, but they won't provide the complete answer because of the very dynamic nature of the internet" (InfoSecurity Magazine, 2012). The countermeasures that organizations implement to detect, prevent, reduce, counteract, or minimize security risks are called security controls (IBM Cloud Education, 2019). A study done by the Darwin Deason Institute for Cyber Security found that the biggest drivers of cybersecurity investment are "perceived risk reduction" and "compliance" (Moore et al., 2015). "Perceived risk reduction" is subjective; CISOs invest in security controls that, in their eyes at least, reduce the risk facing the firm. In the same study, subjects reported that compliance obligations drive a significant fraction of the overall budget. Security controls based on compliance requirements and subjective decisions cannot protect organizations from the ever-changing threat landscape. Contemporary cybersecurity risk management practices are primarily driven by compliance requirements, forcing organizations to focus on security controls and vulnerabilities. Security controls should be built from threat intelligence to complement controls focusing on compliance requirements and known vulnerabilities (Muckin & Fitch, 2019).

According to Josh Lefkowitz, the CEO of Flashpoint, maintaining compliance should never be the security program's end goal. He states that compliance does not guarantee security. It is important to note that most data breaches in recent years have happened at compliant businesses (Lefkowitz, 2018). Setting up the right security controls is one challenge and effectively monitoring and auditing them is another challenge. Continuous monitoring enables management to continually review business processes for adherence to and deviations from the organization's intended security posture. However, security controls' monitoring is not a common practice. According to a whitepaper published by Deloitte, continuous controls monitoring (CM) and continuous auditing (CA), and their benefits are known to most financial and auditing executives. However, relatively few enterprises have realized the full potential of CM and CA, particularly at the enterprise-wide level (Deloitte, 2010). Automatic auditing of controls reduces the effort necessary for audits or certifications. If the control checks are done manually, and the interval between audits is months or even years, it is impossible to detect insufficient or changed controls (Koschorreck, 2011). Treating security monitoring as a quarterly auditing process means most compromises will go undetected for weeks or months. The attacks are continuous, and the monitoring must match (Conrad, 2014).

It is common to find auditors who audit security controls use a checklist approach. The outcome of the checklist approach may not address the specific threats the company faces. The auditors may completely miss controls supposed to be in place or recommend out of scope controls. Instead of working from a checklist, if the auditors should work through threats and risk analysis, they end up with a set of recommendations that are just tailored to that system (Grossman, 2013).

Patch management is a critical security control that needs attention regarding how to manage the patch management process. The infamous Equifax data breach is the result of missing a patch. The patch management process involves identifying, acquiring, installing, and verifying patches for products and systems. Several challenges complicate patch management. If organizations do not overcome these challenges, patch management becomes ineffective and leads to easily preventable compromises (Souppaya & Scarfone, 2013).

Since the current practices of deploying controls, monitoring, and auditing are not enough to prevent advanced persistent threats, we selected “Security Controls” as one of the variables to study.

Redundant IDS/IPS (RD)

Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS) appliances are the first line of defense for organizations against cyberattacks. IPS and IDS systems are traditionally divided into two categories: signature-based and anomaly-based. IDS/IPSs in both types face an arsenal of challenges from attackers. The war between attackers and IPS/IDS developers never ends (Cheng et al., 2012). Even though an IPS/IDS system is mostly reliable, there is a possibility that an attacker can evade it, which creates a large gap in cybersecurity. IPS/IDS systems are improved continuously against evasion techniques, but new evasion techniques that can bypass IPS/IDS systems are still evolving (Kilic, Hakan Katal, Neset Sertaç , Selcuk, 2019). The most crucial feature of IPS/IDS is detecting data exfiltration. If data exfiltration is not detected, cyber attackers win the battle. Implementing redundant IPS/IDS systems is a crucial component in setting up defenses against APT attacks. If one IPS/IDS cannot detect data exfiltration, another IPS/IDS from a different vendor may detect data exfiltration. Having multiple products to monitor the same activity makes it easier for analysts to confirm the validity of alerts and identify false positives and also provides redundancy should one product fail for any reason (K. A. Scarfone & Mell, 2007). So, we selected "Redundant IPS/IPS" as one of the variables to study. Redundant IDS/IPS can be included in the Security Controls variable, but we deliberately excluded it because IDS/IPS is the first defense cyber attackers need to exploit to evade detection of data exfiltration. So, Redundant IDS/IPS plays an important role in the defense in depth strategy and so needs more focus in the research study.

Segmentation (SG)

Data and network segmentation are essential in protecting organizations from cyberattacks. Network segmentation is an architectural approach that involves dividing a larger network into smaller network segments, which can be accomplished through firewalls, virtual local area networks, and other separation techniques. Network segmentation allows network administrators to control traffic flow between zones (segments) with granular policies. According to Palo Alto Networks, the coarser network zones (and the corresponding security policy rules that allow traffic between zones) reduce the network's attack surface (Palo Alto Networks, 2019).

Modern cyberattacks take advantage of weak security postures of data centers where an attacker can move laterally within the data center between different systems to steal information. Datacenter design includes segmentation as a fundamental information security principle, but at its most basic level. Micro-segmentation is required to effectively protect data centers from modern attacks; micro-segmentation down to the individual workload is needed (Vincentis, 2017).

Segmentation of information sets is a vital component of cybersecurity. Data segmentation is achieved by taking advantage of network segmentation; data gets stored in separate network zones based on classification levels. The value of the information sets that need to be protected may differ. The higher the value of the information set, the stricter the isolation required in implementing segmentation. The Gordon-Loeb Model suggests segmenting databases (i.e., data segmentation) to protect data from cybersecurity breaches and minimize the impact of any cybersecurity breaches that occur (Gordon et al., 2016). The same segmentation principle can be applied to intellectual property like patents and designs and source code repositories.

When a network is compromised, an attacker's lateral movement is limited with network segmentation preventing an attack from spreading. Besides, network segmentation is an obstacle for insiders because sensitive data and systems can be isolated from "curious" insiders. In April 2018, a poor network segmentation resulted in a cyberattack at NASA's Jet Propulsion Laboratory (Bradbury, 2019). So, we selected "Segmentation" as one of the variables to study. Segmentation can be included in the Security Controls variable, but we deliberately excluded it from Security Controls because segmentation plays an important role in the defense in depth strategy. Segmentation technologies like Zero Trust are being adopted, and new technologies are evolving. Segmentation needs more focus in the research study.

Insider Threat Prevention (IT)

"An insider threat is the risk posed by employees or contractors regarding the theft of sensitive data, misuse of their access privileges, or fraudulent activity that puts the organization's reputation and brand at risk. The insider's behavior can be malicious, complacent, or ignorant, which in turn can amplify the impact to the organization resulting in monetary and reputational loss" (Ben & Bhat, 2020). An insider threat program (ITP) is a set of policies, tools, and security/threat assessment personnel focused on detecting insider threat risks. The objective of an ITP is mitigating or preventing insider threat incidents (Greitzer et al., 2019). An effective ITP incorporates several tools to help prevent, detect, and respond to concerning behaviors and activity. These tools or technical controls fall into one of five categories (Spooner et al., 2018):

1. User Activity Monitoring: Organizations need visibility into host-based activities on their assets. This kind of visibility helps organizations prevent and detect malicious insiders, but it will also play a key role in responding to and investigating an incident.

2. Data Loss Prevention: DLP tools allow organizations to monitor and control how users interact with data. Using the DLP tools, organizations implement policies that prohibit users from copying content to removable media or emailing it out of the organization.
3. Security Information and Event Management: SIEM tools aggregate systems' event logs into a centralized repository and perform automated analysis on those logs. SIEM systems can help detect anomalies, which may lead to discovering potentially malicious insiders.
4. Analytics: Analytics tools extend the functionality of the SIEM by providing additional advanced visualization capabilities such as charts and graphs that can make anomalies more visually apparent
5. Digital Forensics and Investigations: These tools can be used to assist in the investigation of malicious insider actions and provide the necessary evidence for potential legal actions

A SANS Institute study ranked malicious insider threat as more damaging than accidental or negligent staff. The report also confirmed that Bring Your Own Device (BYOD) was acting as a driving force to increase insider threats. The policies of an ITP should be adaptive. One of the signs of a matured ITP program is to have adaptive policies and procedures that change with the evolving threats to minimize vulnerabilities (Greitzer et al., 2019). The use of BYOD provides more opportunities for insiders to introduce risk, whether they are negligent or malicious. Since insider threats are an essential attack vector in APT attacks, we selected "Insider Threat Prevention" as one of the variables to study.

Dependent Variable

Sense of Security (SS)

Sense of Security (SS) can be better explained with the Japanese word, Anshin. Anshin is formed by; "An" means to ease, and "Shin" is to mind. Someone feels Anshin when they are free from worry and fear (Murayama et al., 2006). Confidence keeps someone away from worry and fear, which means having confidence equals to Anshin. SS in our research represents the confidence level of employees about the strategic organizational activities of security.

Moderator Variables

Organization Culture (OC)

"Organizational culture is generally seen as a set of key values, assumptions, understandings, and norms shared by members of an organization and taught to new members. Organizational culture is an important moderator in business research" (Farooq & Vij, 2017).

According to Robert E. Quinn and Kim S. Cameron at the University of Michigan at Ann Arbor, there are four organizational culture types: Clan, Adhocracy, Market, and Hierarchy (Maloney et al., 2010).

- Clan oriented cultures are family-like, focusing on mentoring, nurturing, and "doing things together."
- Adhocracy oriented cultures are dynamic and entrepreneurial, focusing on risk-taking, innovation, and "doing things first."
- Market oriented cultures are results-oriented, focusing on competition, achievement, and "getting the job done."
- Hierarchy oriented cultures are structured and controlled, focusing on efficiency, stability, and "doing things right."

In the corporate world, start-up organizations generally have adhocracy oriented cultures. The goal of any start-up organization is to do things first, fast, and capture the market. It is ubiquitous to ignore or give low priority to cybersecurity with a false sense of security, assuming they are low profile targets. Our research study could answer how organizational culture impacts the false sense of security.

Table 2. Constructs and Operational Definitions

Factor	Operational Definition
Security awareness and training	Effectiveness of security awareness and training
Converged testing	Implementation of converged testing
Security controls	Effectiveness of security controls
Segmentation	Effectiveness of segmentation
Redundant IDS/IPS	Implementation of redundant IDS/IPS
Insider threat prevention	Effectiveness of insider threat prevention
Cybersecurity insurance	Purchase of cybersecurity insurance
Sense of security	User confidence with strategic security activities
Organization culture	Type of organization culture (clan, adhocracy, market, or hierarchy) (Maloney et al., 2010)

There are seven constructs, as shown in Figure 2. Five of the constructs (Security Controls, Insider Threat Prevention, Cybersecurity Insurance, Segmentation, and Security Awareness and Training) need to be measured with a group of observable variables. The questions corresponding to each construct with multiple observable variables are provided in Appendix A.

Hypotheses

This research aims to find answers to 14 hypotheses:

H1: Successful implementation of security awareness and training positively impacts the sense of security.

H2: Successful execution of converged testing positively impacts the sense of security.

H3: Successful implementation of security controls positively impacts the sense of security.

H4: Successful implementation of segmentation positively impacts the sense of security.

H5: Successful implementation of redundant IDS/IPS positively impacts the sense of security.

H6: Successful implementation of insider threat prevention positively impacts the sense of security.

H7: Successful execution of cybersecurity insurance purchase positively impacts the sense of security.

H8: Organizational culture moderates the relationship between security awareness and training and the sense of security.

H9: Organizational culture moderates the relationship between converged testing and the sense of security.

H10: Organizational culture moderates the relationship between security controls and the sense of security.

H11: Organizational culture moderates the relationship between segmentation and the sense of security.

H12: Organizational culture moderates the relationship between redundant IDS/IPS and the sense of security.

H13: Organizational culture moderates the relationship between insider threat prevention and the sense of security.

H14: Organizational culture moderates the relationship between cybersecurity insurance and the sense of security.

Research Method

Quantitative Research

Our research approach is quantitative using the survey method. "A quantitative approach is one in which the investigator primarily uses postpositivist claims for developing knowledge (i.e., cause and effect thinking, reduction to specific variables and hypotheses and questions, use of measurement and observation, and the test of theories), employs strategies of inquiry such as experiments and surveys, and collects data on predetermined instruments that yield statistical data" (Creswell, 2003). The quantitative approach is the best choice when the objective of the study is identifying factors that influence an outcome, the utility of an intervention, or understanding the best predictors of outcomes (Creswell, 2003). Our research goal is to identify the factors (security policies, best practices, procedures, and configurations) to improve the defenses against advanced persistent threats (APTs).

Quantitative research uses deductive reasoning, where the researcher forms a hypothesis, collects data to investigate the problem, and then uses the data from the investigation for analysis. After the analysis is completed, conclusions are shared to prove the hypotheses are not false or false (Shirish, 2014). Our quantitative study takes the path of survey research as we need to collect the data for analysis. In survey research, the researcher must affirm a model that identifies the expected relationships among these variables before considering executing a survey. The survey is constructed to test the researcher's stated model against observations of the phenomena (Glasow, 2005).

Survey instrument

The survey instrument consists of 45 questions where respondents are requested to submit responses in the form of a Likert five-point scale with one representing "strongly disagree" and five representing "strongly agree." A five-point Likert-type scale is selected to increase response rate and response quality along with reducing respondents' "frustration level" (Babakus & Mangold, 1992). There are seven constructs, as shown in Figure 2. Five of the constructs (Security Controls, Insider Threat Prevention, Cybersecurity Insurance, Segmentation, and Security Awareness and Training) need to be measured with a group of observable variables. The survey questionnaire is designed to measure the latent variables (constructs) that need to be measured with observable variables. The survey questions are regarding cybersecurity controls and practices followed in the industry. The data collected is participants' opinions about cybersecurity controls and practices followed in the industry. Along with the subject's opinion on cybersecurity controls, the survey gathers the subject's Organization's Size (Small, Medium, or Large), Organization's Industry Sector, and Organization's Culture(Clan, Adhocracy, Market, or Hierarchy).

Data collection

The survey population is cybersecurity professionals with five or more years of work experience and work for a private (for-profit) organization. The Survey Monkey platform is used to deliver the survey questionnaire and collect responses from the survey participants. The survey is anonymous. We deliver the survey with the Anonymous Responses collector option turned on. When the SurveyMonkey's Anonymous Responses collector option is turned on, SurveyMonkey does not track and store identifiable respondent information in survey results. The data collected from the SurveyMonkey platform does not contain any information that can be used for de-identification. The survey will be provided by multiple collectors (social media and email). Our LinkedIn contacts will receive a (URL) link to the survey form on Survey Monkey in my LinkedIn feed (message). The survey will be delivered to members of professional organizations such as ISSA (Information Systems Security Association), Silicon Valley Chapter, ISSA San Francisco Chapter, and ISLF (Information Security Leadership Foundation). The communication directors of both the ISSA chapters and ISLF will email the link to the survey on Survey Monkey form in an email message to the chapter members. We reach out to our former supervisors, colleagues, and professional contacts by email, requesting them to participate in the survey. The email contains the (URL) link to the survey form on

Survey Monkey. Our former supervisors, colleagues, and professional connections may forward the survey to their team members. At DSU, the IRB to have the Office of Graduate Studies distribute the link to the survey for eligible Ph.D. students at the DSU's Beacom College of Computer and Cyber Sciences**.** The survey will be distributed to 1000 or more qualified participants. We expect to get at least 300 responses.

Analysis

Confirmatory factor analysis (CFA) allows for more precise testing of an instrument's factor structure. CFA addresses construct validity by assigning the items in an instrument to their respective factors according to theoretical expectations (Ahmad, 2005). R Studio will be used to conduct CFA. CFA assumes that researchers enter the factor analysis with a firm idea about the number of factors they will encounter and which variables will most likely load onto each factor. CFA provides factor loadings and factor correlations. Factor loading explains the strength of the relationship between each item and the factors. A factor loading value of >= 0.7 indicates a strong relationship between the item (observable variable) and the factor. Questions (observable variables) from the questionnaire with factor loading values of < 0.7 will be ignored to condense the number of observable variables.

If two factors have a strong correlation, one of the factors will be eliminated. CFA helps to determine the model fit. The result of the CFA analysis provides several model fit indices like root mean square error of approximation (RMSEA), comparative fit index (CFI), and Tucker–Lewis index (TLI) to determine model fit for further analysis (Kim et al., 2016).

Once unnecessary observable variables and factors are discarded, the theoretical model will be ready to uncover the cause and effect relationships using the partial least square structural equation model (PLS-SEM). The primary reasons for using PLS in this study are: (1) The study is primarily intended for causal-predictive analysis (2) PLS requires fewer statistical specifications and constraints on the data than the covariance-based strategy of LISREL (e.g., assumptions of normality), and (3) PLS is effective for those early-theory testing situations that characterize the study (Park et al., 2012). Two more reasons for considering PLS-SEM are: (1) The constructs in the study are formatively measured (Hair et al., 2014). (2) PLS-SEM is more appropriate because the theory is less developed (Hamdollah & Baghaei, 2016). R Studio will be used to conduct PLS-SEM.

Research Implementation

As we planned, the Survey Monkey platform was used to administer the survey questionnaire and collect responses from the survey participants. The survey was distributed to 600 qualified participants using email and LinkedIn in spring 2021. There were 253 returned questionnaires out of the 600 distributed. 207 out of the 253 returned questionnaires were useable, i.e., 82% completion rate.

We performed CFA first before testing the proposed hypotheses to ensure that the instrument appropriately measures the latent constructs. We used R and R Studio to conduct CFA. CFA assumes that researchers enter the factor analysis with a firm idea about the number of factors they will encounter and which variables will most likely load onto each factor. CFA provides factor loadings and factor correlations. Factor loading explains the strength of the relationship between each item and the factors. A factor loading value of ≥ 0.7 indicates a strong relationship between the item (observable variable) and the factor (Park et al., 2012). The constructs with factor loading values of < 0.7 are ignored to condense the number of observable variables.

The result of the CFA analysis provides several model fit indices like goodness-of-fit index (GFI), adjusted goodness of fit index (AGFI), normed fit index (NFI), Tucker-Lewis Index (TLI), comparative fit index (CFI), and root mean square error of approximation (RMSEA) to determine model fit for further analysis (Kim et al., 2016). The model fit indices from the CFA analysis were as follows: GFI = 0.890, AGFI = 0.840, NFI = 0.817, TLI =0.000, CFI = 0.962, and RMSEA = 0.070. All are in the acceptable range (Hooper et al., 2008; Steiger, 2007).

We used Warp PLS 7.0 to perform structural equation modeling. Warp PLS provides an integrated environment for combining measurement and structural models' calculations. Using Warp PLS, we examined the validity and reliability of our research instrument, model accuracy, the effect of independent variables on the dependent variable, and how the moderator variable influences the relation between independent and dependent variables. After CFA, we fed our research model to Warp PLS to conduct SEM analysis. Table 3 shows the correlations among the constructs.

Table 3. Correlation Matrix

	SA	SG	SC	CI	RD	CT	SS	OC	IT	OC*CT	OC*RD	OC*CI	OC*SC	OC*SG	OC*SA	OC*IT
SA																
SG	0.807															
SC	-0.647	-0.642														
CI	0.670	0.715	-0.565													
RD	0.723	0.768	-0.550	0.696												
CT	0.763	**0.848**	-0.615	0.767	0.689											
SS	0.675	0.647	-0.511	0.561	0.597	0.634										
OC	-0.015	-0.006	0.027	-0.132	-0.011	-0.071	-0.154									
IT	**0.856**	**0.865**	-0.632	0.674	0.728	0.805	0.612	-0.049								
OC*CT	-0.019	0.029	-0.016	-0.184	-0.027	-0.038	-0.016	0.214	-0.065							
OC*RD	0.027	0.018	-0.105	-0.197	-0.086	-0.027	-0.022	0.128	-0.005	0.711						
OC*CI	-0.157	-0.070	0.052	-0.276	-0.180	-0.167	-0.150	0.281	-0.173	0.787	0.747					
OC*SC	-0.058	-0.133	0.038	0.057	-0.106	-0.016	0.016	-0.198	-0.103	-0.627	-0.478	-0.556				
OC*SG	0.031	0.064	-0.142	-0.083	0.020	0.031	0.004	0.195	-0.024	0.878	0.748	0.700	-0.598			
OC*SA	0.014	0.029	-0.060	-0.183	0.030	-0.020	0.025	0.224	-0.008	0.800	0.676	0.748	-0.676	0.776		
OC*IT	-0.007	-0.022	-0.106	-0.195	-0.004	-0.065	-0.017	0.196	-0.017	0.857	0.736	0.720	-0.619	0.896	0.858	

As shown in Table 3, Warp PLS warned about the highly correlated constructs, CT and SG (0.848), IT and SA (0.856), IT and SG (0.865), presented in the model. This led to the next step in eliminating two constructs, CT and IT, which have correlations (> 0.85) with the SG. The refined research model for evaluating the sense of security is shown in Figure 3.

After revising the model, we performed SEM analysis with Warp PLS again. The analysis did not reveal any other correlations among the constructs. It implies that the correlations among the constructs are within the acceptable range.

Chapter Summary

Based on the literature review, this chapter introduced research constructs, research model, operational definition of constructs, hypothesis statements, and research method. In addition, the chapter presented details on research implementation. In the research implementation phase, a survey was distributed to 600 qualified participants using email and LinkedIn. There were 253 returned questionnaires out of the 600 distributed. 207 out of 253 returned questionnaires were useable, i.e., 82% completion rate. After the survey was completed, using R Studio, CFA was performed to ensure that the instrument appropriately measures the latent constructs. We used R and R Studio to conduct CFA. The factors with factor loading values of < 0.7 are ignored to condense the number of observable variables. After CFA, the research model was fed to Warp PLS to conduct SEM analysis. Before performing SEM analysis, Warp PLS checks for highly correlated constructs. Convergent Testing and Insider Threat Prevention constructs had correlations greater than 0.85 with other constructs in the research model. So, we removed Convergent Testing and Insider Threat Prevention constructs from the research model. We fed the updated research model to Warp PLS again to perform SEM. No high correlations were found among the constructs in the updated research model.

CHAPTER 4

DATA ANALYSIS

In the previous chapter, we presented research constructs, research model, operational definition of constructs, hypothesis statements, and research method. In addition, we provided the details on research implementation. As part of the research implementation, we conducted a survey and performed CFA to ensure that the instrument appropriately measures the latent constructs. The factors with factor loading values of < 0.7 were ignored to condense the number of observable variables. Next, we fed the research model to Warp PLS to conduct SEM analysis. Warp PLS reported Convergent Testing and Insider Threat Prevention as constructs that had correlations greater than 0.85 with other constructs in the research model. So, we removed Convergent Testing and Insider Threat Prevention constructs from the research model. We fed the updated research model to Warp PLS again to perform SEM. No high correlations were found among the constructs in the updated research model. In this chapter, we discuss the assessment of the measurement and structural models and testing of hypotheses statements before moving discussion of the findings.

Assessment of Measurement Model

The indicators used in the model are reflective. We further assessed the observing internal consistency, each indicator’s reliability, convergent reliability, and discriminant validity for the refined model.

The first step in reflective measurement model assessment is examining the indicator loadings. Factor loading values above 0.708 are recommended, as they indicate that the construct explains more than 50 percent of the indicator’s variance, thus providing acceptable item reliability (Hair et al., 2019). Factor loadings of all constructs are above the recommended value of 0.708, as shown in Table 4.

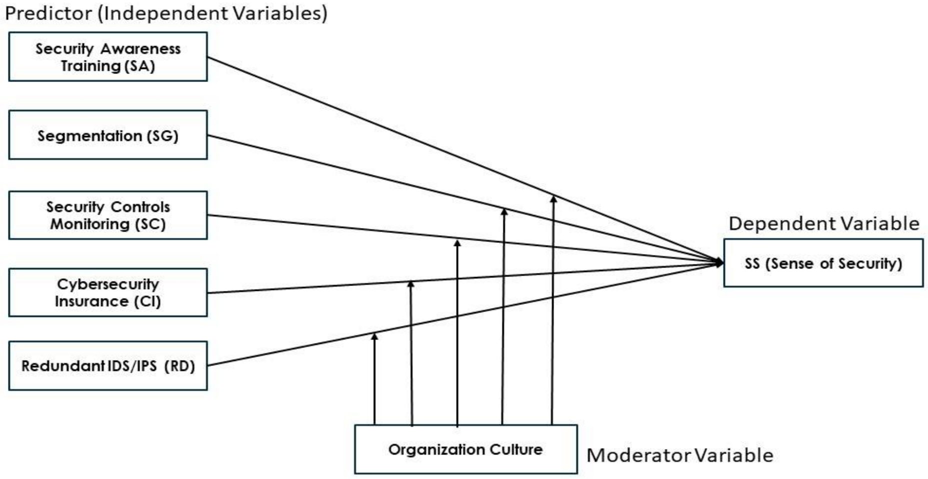

Predictor (Independent Variables)
Security Awareness Training (SA)
Segmentation (SG)
Security Controls Monitoring (SC)
Cybersecurity Insurance (CI)
Redundant IDS/IPS (RD)
Dependent Variable
SS (Sense of Security)
Organization Culture
Moderator Variable

Figure 3. Refined Research Model for Evaluating Sense of Security

The second step is assessing internal consistency reliability by examining composite reliability (CR). CR values between 0.70 and 0.90 range from satisfactory to good. CR values of 0.95 and above indicate the presence of redundant factors, thereby reducing construct validity (Hair et al., 2019). The CR values of SA, SC, and SG are in the acceptable range. The CR values of CI and RD are equal to one because both the constructs have only one factor. A higher CR value indicates higher reliability if the CR value is not above 0.95. Therefore, CR values of all constructs are in the good range. Cronbach’s alpha value is another measure of internal consistency reliability that assumes similar thresholds (Hair et al., 2019). Cronbach’s alpha value is described as excellent (0.93–0.94), strong (0.91–0.93), reliable (0.84–0.90), robust (0.81), fairly high (0.76–0.95), high (0.73–0.95), good (0.71–0.91), relatively high (0.70–0.77), slightly low (0.68), reasonable (0.67–0.87), adequate (0.64–0.85), moderate (0.61–0.65), not satisfactory (0.4–0.55), and low (0.11) (Taber, 2018). The Cronbach’s alpha values of all the constructs are shown in Table 4. The Cronbach’s alpha values of the constructs under study are in the excellent to the reliable range.

Table 4. Factor Loadings, CR, Cronbach's Alpha, Dijakstra's PLSc, AVE.

Construct	Indicators	Loading	Composite Reliability	Cronbach's Alpha	Dijakstra's PLSc	AVE
SA	SA1	0.873	0.932	0.890	0.894	0.905
	SA3	0.912				
	SA4	0.931				
SG	SG3	0.866	0.938	0.918	0.923	0.868
	SG4	0.867				
	SG6	0.854				
	SG7	0.877				
	SG8	0.874				
SC	SC6	0.847	0.835	0.605	0.659	0.847
	SC9	0.847				
CI	CI1	1.000	1.000	1.000	1.000	1.000
RD	RD1	1.000	1.000	1.000	1.000	1.000

"While Cronbach's alpha may be too conservative, the composite reliability may be too liberal, and the construct's true reliability is typically viewed as within these two extreme values" (Hair et al., 2019). As an alternative, Dijkstra and Henseler proposed consistent PLS (PLSc) as an approximately exact measure of construct reliability, whose value usually lies between Cronbach's alpha and the composite reliability (Dijkstra & Henseler, 2015). The Dijkastra's PLSc values of all constructs lie between Cronbach's alpha value and CR value, as shown in Table 4. Internal consistency reliability of constructors was verified with factor loadings, composite reliability, Cronbach's alpha, and Dijkastra's PLSc.

The third step of the reflective measurement model assessment is to examine the convergent validity of each construct measure. "Convergent validity is the extent to which the construct converges to explain the variance of its items" (Hair et al., 2019). The average variance extracted (AVE) for all items on each construct is the metric used for evaluating a construct's convergent validity. An acceptable AVE is 0.50 or higher to establish convergent validity (Hair et al., 2019; Kante et al., 2018).

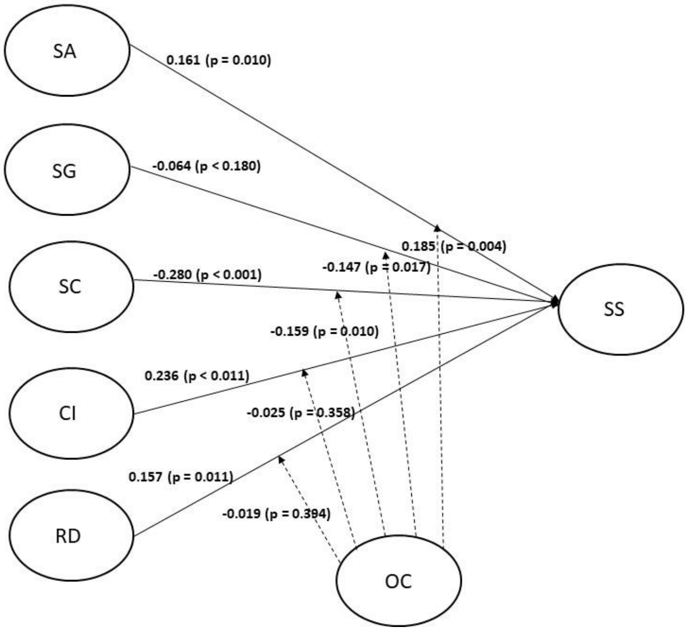


Figure 4. Coefficient of Determination

The fourth step is to assess discriminant validity, which tests whether the concepts or the measurements that are not supposed to be related are unrelated. Discriminant validity represents the extent to which a construct is empirically distinct from other constructs in the structural model (Hair et al., 2019). Discriminant validity is assessed with the heterotrait-monotrait (HTMT) ratio of the correlations. The HTMT is defined as the mean value of the item correlations across constructs relative to the (geometric) mean of the average correlations for the items measuring the same construct (Hair et al., 2019). The threshold value for HTMT is 0.90, and the HTMT value above 0.90 suggests a lack of discriminant validity (Henseler et al., 2015). The HTMT ratio values for the constructs in our model are below the threshold value of 0.90, as shown in Table 5, confirming that discriminant validity is present.

Table 5. HTMT Ratios

	SA	SG	SC	CI	RD
SA					
SG	0.893				
SC	0.882	0.861			
CI					
RD					

Assessment of Structural Model

The structural model is used to estimate the relationships between the latent dependent and independent variables. Before assessing the structural relationships, collinearity must be examined to make sure that multicollinearity is not present. The variance inflation factor (VIF) is the most common way to detect multicollinearity. VIF values above 5 are indicative of probable collinearity issues among the predictor constructs (Hair et al., 2011, 2019). The VIF values of predictor variables in our model are below, as shown in Table 6. Therefore, there is no collinearity issue.

Table 6. VIF Values

	SA	SG	SC	CI	RD
VIF	3.902	4.447	2.014	2.855	3.156

The next step is examining the standard assessment criteria, including the coefficient of determination (R^2), the blindfolding-based cross-validated redundancy measure Q^2, and the statistical significance and relevance of the path coefficients (Hair et al., 2019).

The coefficient of determination (R^2) is considered in the case of endogenous constructs (Hair et al., 2019), but there are no endogenous constructs in our model. Since the R^2 value is a measure of a model predictive power and WarpPLS computes R^2 value, we considered examining R^2 value. R^2 value of 0.75, 0.50 and 0.25 can be considered substantial, moderate, and weak (Hair et al., 2011; Henseler et al., 2009). The R^2 value of our research model is 0.52, as shown in Figure 4. Our model's predictive power is moderate. "As a rule of thumb, Q^2 values higher than 0, 0.25 and 0.50 depict small, medium and large predictive relevance of the PLS-path model" (Hair et al., 2019). The Q^2 value of our research model is 0.622. Thus, our research model's predictive relevance is high.

Hypotheses Testing

H1 states that successful implementation of security awareness and training positively impacts the sense of security. Table 7 shows that the p-value of security awareness and training on influencing the sense of security is 0.010 with the value of path coefficient of 0.161. This p-value is less than 0.05 (significance < 0.05). Therefore, it can be concluded that the successful implementation of security awareness and training positively impacts the sense of security.

H2 states that successful execution of converged testing positively impacts the sense of security. This hypothesis was dropped from the study as convergent testing is highly correlated with the other predictor variable segmentation.

H3 states that successful implementation of security controls positively impacts the sense of security. Table 7 shows that the p-value of security controls on influencing the sense of security is less than 0.001 with the value of path coefficient of 0.280. This p-value is less than 0.05 (significance < 0.05). Therefore, it can be concluded that the successful implementation of security controls positively impacts the sense of security.

H4 states that successful implementation of segmentation does not impact the sense of security. Table 7 shows that the p-value of segmentation influencing the sense of security is less than 0.180 with the value of path coefficient of 0.064. This p-value is great than 0.05 (significance < 0.05). Therefore, it can be concluded that the successful implementation of segmentation does not impact the sense of security.

H5 states that successful implementation of redundant IDS/IPS positively impacts the sense of security. Table 7 shows that the p-value of redundant IDS/IPS on influencing the sense of security is 0.011 with the value of path coefficient of 0.157. This p-value is less than 0.05 (significance < 0.05). Therefore, it can be concluded that the successful implementation of redundant IDS/IPS positively impacts the sense of security.

H6 states that successful implementation of insider threat prevention positively impacts the sense of security. This hypothesis was dropped from the study as insider threat prevention is highly correlated with two predictor variables, segmentation and security awareness and training.

H7 states that successful execution of cybersecurity insurance purchase positively impacts the sense of security. Table 7 shows that the p-value of cybersecurity insurance influencing the sense of security is less than 0.001 with the value of path coefficient of 0.236. This p-value is less than 0.05 (significance < 0.05). Therefore, it can be concluded that the successful execution of cybersecurity insurance purchase positively impacts the sense of security.

H8 states that organizational culture moderates the relationship between security awareness and training and the sense of security. Table 7 shows that the p-value of organizational culture on influencing the relationship between security awareness and training and the sense of security is 0.004 with the value of path coefficient of 0.185. This p-value is less than 0.05 (significance < 0.05). Therefore, it can be concluded that organizational culture moderates the relationship between security awareness and training and the sense of security.

H9 states that organizational culture moderates the relationship between converged testing and the sense of security. This hypothesis was dropped from the study as the predictor variable convergent testing was dropped from the study.

H10 states that organizational culture moderates the relationship between security controls and the sense of security. Table 7 shows that the p-value of organizational culture on influencing the relationship between security controls and sense of security is 0.010 with the value of path coefficient of 0.159. This p-value is less than 0.05 (significance < 0.05). Therefore, it can be concluded that organizational culture moderates the relationship between security controls and the sense of security.

H11 states that organizational culture moderates the relationship between segmentation and the sense of security. Table 7 shows that the p-value of organizational culture on influencing the relationship between segmentation and sense of security is 0.017 with the value of path coefficient of 0.147. This p-value is less than 0.05 (significance < 0.05). Therefore, it can be concluded that organizational culture moderates the relationship between segmentation and the sense of security.

H12 states that organizational culture moderates the relationship between redundant IDS/IPS and the sense of security. Table 7 shows that the p-value of organizational culture on influencing the relationship between redundant IDS/IPS and the sense of security is 0.394 with the value of path coefficient of 0.019. This p-value is great than 0.05 (significance < 0.05). Therefore, it can be concluded that organizational culture does not moderate the relationship between redundant IDS/IPS and the sense of security.

H13 states that organizational culture moderates the relationship between insider threat prevention and the sense of security. This hypothesis was dropped from the study as the predictor variable insider threat prevention was dropped from the study.

H14 states that organizational culture moderates the relationship between cybersecurity insurance and the sense of security. Table 7 shows that the p-value of organizational culture on influencing the relationship between cybersecurity insurance and the sense of security is 0.358 with the value of path coefficient of 0.025. This p-value is great than 0.05 (significance < 0.05). Therefore, it can be concluded that organizational culture does not moderate the relationship between cybersecurity insurance and the sense of security.

Table 7. PATH Coefficients

Relation	Path Coefficient	p-Value	Description
H1 SA -> SS	0.161	0.010	Supported
H3 SC -> SS	-0.280	<0.001	Supported
H4 SG -> SS	-0.064	0.180	Not Supported
H5 RD -> SS	0.157	0.011	Supported
H7 CI -> SS	0.236	<0.001	Supported
H8 OC -> SA	0.185	0.004	Supported
H10 OC -> SC	-0.159	0.010	Supported
H11 OC -> SG	-0.147	0.017	Supported
H12 OC -> RD	-0.019	0.394	Not Supported
H14 OC -> CI	-0.025	0.358	Not Supported

Discussion

There is news on data breaches due to APTs almost every day. The amount of money spent on improving the security posture, whether it is on cybersecurity products, services, or training, increases year by year. Despite all the awareness training, technological advancements, and massive investment, the fight against APTs could be challenging for any organization if their cybersecurity products, services, or training are not adequately or effectively implemented. While managing cybersecurity posture, corporations focus on security products and services but not on employees' perception of cybersecurity posture. This research is aimed at how employees feel about the security posture of corporations and the effectiveness of security measures implemented by the corporations. We referred to employees' perception of cybersecurity posture as the sense of security and investigated what factors influence the sense of security. Our survey found that employees are not confident about their organizations' cybersecurity posture. The responses we received showed that the average value of employees' confidence about cybersecurity posture was 1.8 (Strongly Disagree 1, Disagree 2, Neither Agree nor Disagree 3, Agree 4, Strongly Agree 5).

Our study confirms that security awareness and training, security controls, implementation of redundant IDS/IPS, and purchase of cybersecurity insurance positively influence employees' sensor of security. This study also confirms that organizational culture influences the relationship of security awareness and training and security controls with the sense of security.

This research found that effective segmentation did not influence the employees' sense of security. The reason that our hypothesis regarding the segmentation was not supported might be due to a lack of understanding/knowledge/awareness of segmentation. Our study confirms that the organizational culture influences the relationship of segmentation with the sense of security.

Cybersecurity is a vast domain. Since it is impossible to include many independent variables in the research, we limited our independent variables to seven. During the SEM analysis, we found that there were strong correlations (> 0.85) among converged testing, insider threat prevention, and segmentation. We had to drop two independent variables, e.g., convergent testing and insider threat prevention, from the initial model.

Chapter Summary

In this chapter, we evaluated measurement and structural models before proceeding to evaluate the hypotheses. As part of the measurement model assessment, first, we verified that factor loading values are above 0.708. Next, we observed that internal consistency reliability, convergent validity, and discriminant validity measures are in the desired range. As part of the structural model assessment, we verified that no multicollinearity exists, and predictive power and relevance are in the desired range. After successfully validating both measurement and structural models, we tested hypotheses statements using path coefficient and p values. Our survey found that employees are not confident about their organizations' cybersecurity posture. The responses we received showed that the average value of employees' confidence about cybersecurity posture was 1.8, which is low, confirming that the organizations are in a false sense of security. In the hypotheses testing, we found that a) successful implementation of security awareness and training positively impacts the sense of security (H1 supported) b) successful implementation of security controls positively impacts the sense of security (H3 supported) c) successful implementation of segmentation does not impact the sense of security (H4 not supported) d) successful implementation of redundant IDS/IPS positively impacts the sense of security (H5 supported) e) successful execution of cybersecurity insurance purchase positively impacts the sense of security (H7 supported) f) organizational culture moderates the relationship between security awareness and training and the sense of security (H8 supported) g) organizational culture moderates the relationship between security controls and the sense of security (H10 supported) h) organizational culture moderates the relationship between segmentation and the sense of security (H11 supported) i) organizational culture does not moderate the relationship between redundant IDS/IPS and the sense of security (H12 not supported) j) organizational culture does not moderate the relationship between cybersecurity insurance and the sense of security (H14 not supported).

CHAPTER 5

IMPROVING EMPLOYEES' SENSE OF SECURITY TO PREVENT APTS

In the last chapter, the research identified what constructs positively influences the sense of security of employees. In the context of APTs, the research proved that inefficient implementation of security controls results in a low sense of security of employees. In this chapter, we recommend what controls to enhance based on the constructs to increase the sense of security of employees.

Remediation Strategy to Prevent APTS

Since the effectiveness of the controls plays a significant role in combating the APTs, we suggest the following recommendations for the constructs contributing to the false sense of security.

Security Awareness and Training

Information security programs frequently overlook the importance of security awarene ss. While organizations invest in security technology and continuously train security personnel, very little is done to increase security awareness among the other employees (Aloul, 2012). Unfortunately, the non-security personnel group is the weakest link to get trapped in social engineering and phishing scams (Aloul, 2012). As it was known a few years ago, Scam email had features such as a fake sender address and grammatical errors. Currently, targeted attacks look more professional, with almost genuine-looking content. It is frightening to know that Human Negligence drives 90% of cyberattacks, that 68% of employees fell for the phishing mail, and that 92.4% of malware is delivered via a phishing email (Khan et al., 2020).

Security awareness and training campaigns typically track who took the training or attended awareness sessions, the number of users who passed the exams, etc. However, these campaigns fail to measure the impact of the awareness sessions (Aloul, 2012). Because the effectiveness of security awareness and training campaigns are not measured, employees indicated a low sense of security regarding security awareness and training in our survey. We recommend a cyber security awareness measurement model: Analyze, Predict, Awareness, and Test (APAT) (Khan et al., 2020). APAT model involves a four-step cycle: analyzing the current threats, predicting the impact of threats, providing security awareness and training, and measuring the effectiveness of security awareness and training provided. The APAT model solves the challenge of delivering an effective security awareness and training program as the program outcome measurement is a part of the model. The APAT model also addresses the challenge of providing relevant and updated training. Table 8 shows our recommendation regarding security awareness and training and what controls to enhance in the NIST 800-53 Security and Privacy Controls (NIST, 2020).

Redundant IDS/IPS

Intrusion Detection Systems (IDS)/Intrusion Prevention Systems (IPS) are the first lines of defense against APT attacks. “APTs are specifically designed to defeat controls such as firewalls, anti-virus and intrusion-detection systems, and especially those that rely on signatures and can therefore guard only against known threats” (Tankard, 2011). If an organization's IPS/IDS system can be bypassed, an attacker can quickly get inside the organization’s internal network to perform the next steps in the cyberattack. Although IPS/IDS systems are constantly improved, evolving evasion techniques can still bypass an IPS/IDS system.

We recommend redundancy in setting up IDS/IPS since Intrusion Detection Systems (IDS)/Intrusion Prevention Systems (IPS) are the first lines of defense for organizations. Intrusion Detection and Prevention Systems (IDPS) technologies are classified into four primary types: 1) network-based, 2) wireless, 3) network behavior analysis (NBA), and 4) host-based (K. A. Scarfone & Mell, 2007). Each technology type offers benefits over the other, such as detecting some events that the others cannot, detecting some events with significantly greater accuracy than the other technologies, and performing in-depth analysis without substantially impacting the performance of the protected hosts (K. A. Scarfone & Mell, 2007). The use of multiple IDSs and other security systems gives a better picture of the monitored network; they cooperate to complement each other's coverage (Elshoush, 2014). Even if each IDS uses a different detection technique, they analyze each other's alerts and reduce false positives. A reliable intrusion detection solution cannot be achieved without using multiple types of IDS/IPS technologies (K. A. Scarfone & Mell, 2007). To improve intrusion detection capabilities, some organizations also use multiple products of the same IDPS technology type (K. A. Scarfone & Mell, 2007). Since each product developer uses somewhat different detection methodologies and detects some events that another product cannot, when multiple products are used to monitor the same activity, it is easier for analysts to validate alerts and identify false positives, and it also provides redundancy/reliability should one product fail (K. A. Scarfone & Mell, 2007).

Security Controls

Security controls are the countermeasures that organizations implement to detect, prevent, reduce, counteract, or minimize security risks are called security controls (IBM Cloud Education, 2019). Today's cyber security risk management practices are primarily driven by compliance requirements, forcing organizations to focus on security controls and vulnerabilities (Muckin & Fitch, 2019). Our literature review found that one of the biggest drivers of cybersecurity investment is compliance, and compliance obligations drive a significant fraction of the overall budget. Security controls based on compliance requirements cannot protect organizations from the ever-changing threat landscape. To address the ever-changing threat landscape, security controls should be built from threat intelligence to complement controls focusing on compliance requirements and known vulnerabilities (Muckin & Fitch, 2019).

Threat Intelligence (TI) is the knowledge about adversaries and their motivations, intentions, and methods (Gschwandtner et al., 2018). We recommend adding security controls based on threat intelligence, which complements and supplements compliance-driven security controls. “Threat intelligence (TI) promises to provide actionable information about current threats for information security management systems (ISMS)” (Gschwandtner et al., 2018). Cyber Threat Intelligence (CTI) platforms are being developed by many major cybersecurity companies such as FireEye, ThreatConnect, McAfee, and many others to streamline and create efficient and effective CTI capabilities, enabling an unprecedented ability to prioritize threats, pinpoint key threat actors, understand their tools, techniques, and procedures (TTP), deploy appropriate security controls, and ultimately, improve overall cybersecurity hygiene (Samtani et al., 2019). We recommend considering a CTI platform because of its agility without much human intervention. “As technological changes occur more quickly, auditors must keep pace with emerging technological changes and their impacts on their client's data processing system as well as their own audit procedures” (Rezaee & Reinstein, 1998). When selecting a control assessor or team of assessors, we recommend selecting the assessor or assessors with deep technical knowledge regarding the systems and their security. Table 8 shows our recommendation regarding security awareness and training and what controls to enhance in the NIST 800-53 Security and Privacy Controls (NIST, 2020).

Cybersecurity Insurance

Cybersecurity insurance pays for a company to hire a cybersecurity corporation that conducts a forensic investigation to reveal precisely what happened in an attack (Morris, 2021). It pays for the legal services required after the attack. Suppose the cyber attack leads to people filing litigation against a company. In that case, the insurance will step in to pay for defense attorneys and a settlement or court-awarded damages to the plaintiffs (Morris, 2021). “But despite the importance of cyber insurance as one of the tools for organizations to manage their cyber risks, there are still problems relating to this market which have persisted over the years, mainly in aspects of the lack of information and knowledge that affect market maturity and the willingness to use it” (Pavel, 2020). It is no wonder why organizations are lagging in adopting cybersecurity insurance in their security programs.

Since APT attacks involve data exfiltration and an organization can go bankrupt after a successful cyberattack, we recommend adding cybersecurity insurance to the organization’s security program. “When appropriately managed, cyber insurance can become another tool in the risk management toolbox” (Christopher, 2017). “Security is more than technical controls, and insurance can help provide true financial controls to cyber security” (Christopher, 2017). There is published research with a strong argument for making cybersecurity insurance mandatory for SMEs (Lemnitzer, 2021).

Table 8 shows our recommendation regarding security awareness and training and what controls to enhance in the NIST 800-53 Security and Privacy Controls (NIST, 2020).

Table 8. Independent Variables and Corresponding Security control(s) to Be Enhanced

Independent Variable	NIST Control	Action Item
Security Controls	CA-2 CONTROL ASSESSMENTS	Enhance the security control by making sure that the assessor or assessment team selected for assessment has deep technical knowledge of the systems and their security.

	ACCESS Control Group: AC-1 to AC-25	Enhance the applicable controls based on threat intelligence feeds.
	PL-2 SYSTEM SECURITY AND PRIVACY PLANS	Enhance the control based on the threat intelligence feeds.
Redundant IDS/IPS	SI-4 SYSTEM MONITORING	Enhance the control with redundant IDS/IPS systems to monitor the network and systems.
Security Awareness and Training	AT-2 LITERACY TRAINING AND AWARENESS	Enhance the control by applying the APAT (Analyze, Predict, Awareness, and Test) model.
Cybersecurity Insurance	PM-1 INFORMATION SECURITY PROGRAM PLAN	Enhance the control by adding a plan to procure cybersecurity insurance.
	PM-4 PLAN OF ACTION AND MILESTONES PROCESS	Enhance the control by purchasing cybersecurity insurance.
	PM-9 RISK MANAGEMENT STRATEGY	Enhance the control by adding cybersecurity insurance as a risk transfer method.

Chapter Summary

Since Security Awareness and Training, Security Controls, Redundant IDS/IPS, and Cybersecurity Insurance positively influence the sense of security, we suggested our recommendations to enhance their effectiveness. We recommended a cyber security awareness measurement model called Analyze, Predict, Awareness, and Test (APAT) to implement security awareness and training. In the case of Security Controls, we recommended adding security controls based on threat intelligence, which complements and supplements compliance-driven security controls. We recommended taking advantage of Cyber Threat Intelligence (CTI) platforms to manage security controls. As part of our recommendations, we stressed the importance of implementing Redundant IDS/IPS and purchasing cybersecurity insurance.

CHAPTER 6

SUMMARY AND CONCLUSION

Since we completed all phases of the planned research, in this chapter, we present the summary of the research, limitations, contributions, and future work of this research.

Research Summary

The purpose of our research is to determine why technological solutions fail to protect organizations from APTs and decide which security controls need to be implemented, fine-tuned, and enhanced, along with technical solutions to protect organizations from APTs. The research study identifies security policies, procedures, and configurations to focus on in the pursuit of defeating advanced persistent threats (APTs).

Despite all the awareness, technological advancements, and massive investment, the fight against APTs is a losing battle. It seems logical to look at how APT defenses are set up and consider whether organizations are in a false sense of security. Shall organizations need to think about new strategies to detect APTs? Shall organizations need a paradigm shift in setting defenses against APTs? In this research, our objective is to contribute to the cybersecurity domain by verifying whether there is a false sense of security among organizations. If a false sense of security does exist among organizations, our research highlights what is missing when considering the defenses to prevent APT attacks.

Our research study began with the following research questions:

- RQ1. Are organizations in a false sense of security while relying on off-the-shelf tools to protect against APT attacks?
- RQ2. What are the most critical factors (practices/controls) contributing to the false sense of security? Is there any relationship among the factors contributing to the false sense of security?
- RQ3. Does organizational culture influence the setup of defenses against APT attacks?

In our literature review, we found the following:

- Cyber attackers outclass off-the-shelf solutions.
- Employees need security education and a sober understanding of the protection systems in place to secure their key assets.
- If critical/basic security controls are not in place, it makes no sense to do advanced controls like SOAR.
- Heavy focus on tools to prevent APT attacks, non-technical attack vectors like insider threat and social engineering are not given much-needed attention.

Based on the literature review, we defined research constructs, research model, operational definition of constructs, hypothesis statements, and research method. The research is survey-based quantitative research; based on the survey outcome, we planned to propose remediations regarding implementing and enhancing security policies, procedures, and configurations to set up defenses against APTs.

In the research implementation phase, a survey was distributed to 600 qualified participants using email and LinkedIn. There were 253 returned questionnaires out of the 600 distributed. 207 out of 253 returned questionnaires were useable, i.e., 82% completion rate. After the survey was completed, using R Studio, CFA was performed to ensure that the instrument appropriately measures the latent constructs. We used R and R Studio to conduct CFA. The factors with factor loading values of < 0.7 are ignored to condense the number of observable variables. After CFA, the research model was fed to Warp PLS to conduct SEM analysis. Before performing SEM analysis, Warp PLS checks for highly correlated constructs. Convergent Testing and Insider Threat Prevention constructs had correlations greater than 0.85 with other constructs in the research model. So, we removed Convergent Testing and Insider Threat Prevention constructs from the research model. We fed the updated research model to Warp PLS again to perform SEM. No high correlations were found among the constructs in the updated research model.

We evaluated measurement and structural models before proceeding to evaluate the hypotheses. As part of the measurement model assessment, first, we verified that factor loading values are above 0.708. Next, we observed that internal consistency reliability, convergent validity, and discriminant validity measures are in the desired range. As part of the structural model assessment, we verified that no multicollinearity exists, and predictive power and relevance are in the desired range. After successfully validating both measurement and structural models, we tested hypotheses statements using path coefficient and p values. In the hypotheses testing, we found that a) successful implementation of security awareness and training positively impacts the sense of security (H1 supported) b) successful implementation of security controls positively impacts the sense of security (H3 supported) c) successful implementation of segmentation does not impact the sense of security (H4 not supported) d) successful implementation of redundant IDS/IPS positively impacts the sense of security (H5 supported) e) successful execution of cybersecurity insurance purchase positively impacts the sense of security (H7 supported) f) organizational culture moderates the relationship between security awareness and training and the sense of security (H8 supported) g) organizational culture moderates the relationship between security controls and the sense of security (H10 supported) h) organizational culture moderates the relationship between segmentation and the sense of security (H11 supported) i) organizational culture does not moderate the relationship between redundant IDS/IPS and the sense of security (H12 not supported) j) organizational culture does not moderate the relationship between cybersecurity insurance and the sense of security (H14 states that).

Since Security Awareness and Training, Security Controls, Redundant IDS/IPS, and Cybersecurity Insurance positively influence the sense of security, we suggested our recommendations to enhance their effectiveness. We recommended a cyber security awareness measurement model called Analyze, Predict, Awareness, and Test (APAT) to implement security awareness and training. In the case of Security Controls, we recommended adding security controls based on threat intelligence, which complements and supplements compliance-driven security controls. We recommended taking advantage of Cyber Threat Intelligence (CTI) platforms to manage security controls. As part of our recommendations, we stressed the importance of implementing Redundant IDS/IPS and purchasing cybersecurity insurance.

Limitations

The limitations of this research include: 1) We reached out to 600 qualified participants and received 253 returned questionnaires. Our survey response rate was close to 42%. We had sufficient data to conduct data analysis. However, it will be great to receive more survey responses. 2) Because the survey is about employee perception of corporate security posture and the survey population is security professionals, it is possible that more than half of the survey population did not feel comfortable responding to the survey even though it was anonymous. 3) Our research is the first of its kind, studying the employees' perception of security posture vs. corporate security measures. We could not find a model to adopt from the existing information systems literature. 4) Since we dropped Convergent Testing from our research model, we could not study the construct further to identify the gaps left by the standard security testing methodologies like OSSTMM, OWASP, NIST, PTES, and ISSAF. 5) Cybersecurity is a vast domain. It is hard to select and limit the number of independent variables in the research.

Contributions

Despite all the awareness, technological advancements, and massive investment, the fight against APTs is a losing battle for organizations. The objective of our research is to discover why technological solutions fail to protect organizations from APTs and is there something organizations are missing when setting up defenses against APTs. We started our research with three research questions formally: 1) Are organizations in a false sense of security while relying on off-the-shelf tools to protect against APT attacks? 2) What are the most critical factors (practices/controls) contributing to the false sense of security? Is there any relationship among the factors contributing to the false sense of security? 3) Does organizational culture influence the setup of defenses against APT attacks?

Our research found that organizations in a false sense of security while relying on off-the-shelf tools to protect against APT attacks. We studied the relationship between the effectiveness of security controls and the sense of security of employees. Our research study highlighted that sense of security of the employees is low when the security controls are ineffective. Our research suggests that organizations do need a paradigm shift while setting up defenses against APT attacks; focusing on the effectiveness of the security controls is the key. Our research identified the effectiveness of Security Awareness and Training, Security Controls, Redundant IDS/IPS, and Cybersecurity Insurance are the key factors influencing the sense of security of the employees. Not only did we identify Security Awareness and Training, Security Controls, Redundant IDS/IPS, and Cybersecurity Insurance as the important factors influencing the sense of security of the employees, but we also suggested how to implement them effectively. Our research identified organizational culture does play a role in influencing the relationship between Security Awareness and Training, and Security Controls. Our contribution to the industry is to highlight the paradigm shift required for organizations while setting up defenses against APTs. While organizations focus on setting up security controls to satisfy the compliance requirements, we emphasize the importance of the effectiveness of security controls.

Future Work

Despite all the awareness training, technological advancements, and massive investment, this research confirms that employees are not confident about the cybersecurity posture of organizations. Our research identified what influences the employee perception of cybersecurity posture or sense of security. Organizations need to consider not only implementing the security measures but also their effectiveness. Organizations rely on analytical reports generated by tools to validate the effectiveness of security measures implemented. However, they rarely consider the employee perception or confidence about the implemented cybersecurity measures. Employee feedback on security measures is a great additional method to validate the effectiveness of the implemented security measures. Employee feedback helps to check the real effectiveness of security measures and may help to invest the security budget in the right place. The research confirms that organizations need a paradigm shift in protecting themselves against APTs. We dropped two independent variables, convergent testing and insider threat prevention, because of the correlations with the segmentation. In further research, the two constructs we dropped may need to be reevaluated to find out what caused correlations because of their presence. Further, additional independent variables could be considered in the research model.

REFERENCES

Adelaiye, O., Ajibola, A., & Faki, S. (2018). Evaluating Advanced Persistent Threats Mitigation Effects : A Review. *International Journal of Information Security Science*, *7*(4), 159–171. https://www.researchgate.net/publication/331210253_Evaluating_Advanced_Persistent_Threats_Mitigation_Effects_A_Review%0Ahttps://www.researchgate.net/publication/331210253_Evaluating_Advanced_Persistent_Threats_Mitigation_Effects_A_Review

Ahmad, M. M. (2005). Psychometric evaluation of the Cognitive Appraisal of Health Scale with patients with prostate cancer. *Journal of Advanced Nursing*, *49*(1), 78–86. https://doi.org/10.1111/j.1365-2648.2004.03266.x

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. In *Action control* (pp. 11–39). Springer.

Al-Daeef, M. M., Basir, N., & Saudi, M. M. (2017). Security awareness training: A review. *Lecture Notes in Engineering and Computer Science*, *2229*, 446–451.

Aloul, F. A. (2012). The Need for Effective Information Security Awareness. *Journal of Advances in Information Technology*, *3*(3). https://doi.org/10.4304/jait.3.3.176-183

Babakus, E., & Mangold, W. G. (1992). Adapting the SERVQUAL scale to hospital services: an empirical investigation. *Health Services Research*, *26*(6), 767–786. http://www.ncbi.nlm.nih.gov/pubmed/1737708%0Ahttp://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=PMC1069855

Bada, M., Sasse, A., & Bada, M., Sasse, A., Nurse, J. (2014). Cyber Security Awareness Campaigns: Why They Fail to Change Behavior. *International Conference on Cyber Security for Sustainable Society*, 11. http://www.cs.ox.ac.uk/publications/publication9343-abstract.html%0Ahttp://discovery.ucl.ac.uk/1468954/1/Awareness CampaignsDraftWorkingPaper.pdf

Becker, M. H. (1974). The health belief model and personal health behavior. *Health Education Monographs*, *2*, 324–473.

Belding, G. (2019). *Security+: Technologies And Tools - NIPS / NIDS - Infosec Resources*. Infosec Institute. https://resources.infosecinstitute.com/certification/security-technologies-and-tools-nips-nids/

Ben, S., & Bhat, A. (2020). *Insider Threat Report by Securonix*. https://brage.bibsys.no/xmlui/bitstream/handle/11250/143847/Syvertsen - Insider Threat.pdf?sequence=1&isAllowed=y

Betlich, R. (2010). What APT is (And What it Ins't). *Information Security*.

Bradbury, D. (2019). *NASA Data Breach Demonstrates Need for Proper Network Governance*. InfoSecurity Magazine. https://www.infosecurity-magazine.com/infosec/nasa-data-breach-network/

Brewer, R. (2014). Advanced persistent threats: Minimising the damage. *Network Security*, *2014*(4), 5–9. https://doi.org/10.1016/S1353-4858(14)70040-6

Bromiley, M. (2020). *What Security Practitioners Really Do When It Comes to Security Testing*. https://www.sans.org/media/analyst-program/security-practitioners-security-testing-39210.pdf

Bukac, V., Lorenc, V., & Matyas, V. (2014). *Red Queen's Race: APT win-win game*.

Carella, A., Kotsoev, M., & Truta, T. M. (2017). Impact of security awareness training on phishing click-through rates. *Proceedings - 2017 IEEE International Conference on Big Data, Big Data 2017*, *2018-Janua*, 4458–4466. https://doi.org/10.1109/BigData.2017.8258485

Chapple, M., Stewart, J. M., & Gibson, D. (2018). *(ISC)2 CISSP Certified Information Systems Security Professional Official Study Guide, 8th Edition* (8th Editio). Sybex. https://learning.oreilly.com/library/view/isc2-cissp-certified/9781119475934/c02.xhtml

Cheng, T. H., Lin, Y. D., Lai, Y. C., & Lin, P. C. (2012). Evasion techniques: Sneaking through your intrusion detection/prevention systems. *IEEE Communications Surveys and Tutorials*, *14*(4), 1011–1020. https://doi.org/10.1109/SURV.2011.092311.00082

Christopher, J. D. (2017). *Incentivizing Cyber Security: A Case for Cyber Insurance*.

Coleman, C. (2016). *Welcome Operationalizing Threat Intelligence for Dynamic Defense Addressing the Cyber Kill Chain: Full Gartner Research Report And LookingGlass Perspectives*. https://www.gartner.com/imagesrv/media-products/pdf/lookingglass/lookingglass-1-34D62N3.pdf

Conrad, E. (2014). *Continuous Ownage: Why you Need Continuous Monitoring*. SANS. https://www.sans.org/webcasts/continuous-ownage-continuous-monitoring-99042/success

Creswell, J. W. (2003). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (2nd Editio). SAGE.

Croom, C. (2010). The Cyber Kill Chain: a Foundation for a New Cyber Security Strategy. *High Frontier - The Journal for Space & Missile Professionals*, *6*(4), 52–56. https://apps.dtic.mil/dtic/tr/fulltext/u2/a549792.pdf

Cybersecurity Insurance | CISA. (n.d.). Cybersecurity & Infrastructure Security Agency. Retrieved February 13, 2021, from https://www.cisa.gov/cybersecurity-insurance

Daniel Gonzalez Granadillo, G., Garcia-Alfaro, J., Debar, H., Ponchel, C., Rodriguez-Martin, L., Gonzalez Granadillo Joaquin Garcia-Alfaro Hervé Debar, G., & Ponchel Laura Rodriguez Martin, C. (2015). *Considering technical and financial impact in the selection of security countermeasures against Advanced Persistent Threats*. 1–6. https://doi.org/10.1109/NTMS.2015.7266480ï

Davis, F. D. (1985). *A technology acceptance model for empirically testing new end-user information systems: Theory and results*.

Death, D. (2018). *The Cyber Kill Chain Explained*. Forbes Technology Council. https://www.forbes.com/sites/forbestechcouncil/2018/10/05/the-cyber-kill-chain-explained/?sh=4af284ac6bdf

Deloitte. (2010). *Continuous monitoring and continuous auditing From idea to implementation*. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/audit/us-aers-continuous-monitoring-and-continuous-auditing-whitepaper-102910.pdf

Demisto. (2019). *Gartner Releases 2019 Market Guide for Security Orchestration, Automation, and Response (SOAR)*. Demisto. https://blog.demisto.com/gartner-releases-2019-market-guide-for-soar

DFLabs. (2019). *The Difference Between SIEM and SOAR (Why Do I Need SOAR, If I Have SIEM?)*. DFLabs. https://www.dflabs.com/resources/blog/the-difference-between-siem-and-soar-why-do-i-need-soar-if-i-have-siem/

Dijkstra, T. K., & Henseler, J. (2015). Consistent partial least squares path modeling. In *MIS Quarterly: Management Information Systems* (Vol. 39, Issue 2, pp. 297–316). University of Minnesota. https://doi.org/10.25300/MISQ/2015/39.2.02

Elshoush, H. T. I. (2014). An innovative framework for collaborative intrusion alert correlation. *Proceedings of 2014 Science and Information Conference, SAI 2014*, 607–614. https://doi.org/10.1109/SAI.2014.6918249

Farooq, R., & Vij, S. (2017). Moderating Variables in Business Research. *The IUP Journal of Business Strategy*, *14*(4), 34–54.

FireEye. (2019). *FireEye 2019 Mandiant M-Trends Report Finds Organizations Across the Globe Are Faster to Identify Attacker Activity Compared to Previous Year*.

Frenz, C. M., & Diaz, C. (2017). *Anti-Ransomware Guide*. https://owasp.org/www-pdf-archive/Anti-RansomwareGuidev1-3.pdf

Glasow, P. A. G. (2005). *Fundamentals of Survey Research Methodology*. www.mitre.org/sites/default/files/pdf/05_0638.pdf

Gordon, L. A., Loeb, M. P., & Zhou, L. (2016). Investing in Cybersecurity: Insights from the Gordon-Loeb Model. *Journal of Information Security*, *07*(02), 49–59. https://doi.org/10.4236/jis.2016.72004

Greitzer, F. L., Purl, J., Leong, Y. M., & Sticha, P. J. (2019). Positioning Your Organization to Respond to Insider Threats. *IEEE Engineering Management Review*, *47*(2), 75–83. https://doi.org/10.1109/EMR.2019.2914612

Grimes, R. A. (2011). *Prepare for advanced persistent threats, or risk being the next RSA*. CSO Online. https://www.csoonline.com/article/2623889/prepare-for-advanced-persistent-threats--or-risk-being-the-next-rsa.html

Grossman, W. M. (2013). Auditors: Friend or Foe? *InfoSecurity Magazine*. https://www.infosecurity-magazine.com/magazine-features/auditors-friend-or-foe/

Gschwandtner, M., Demetz, L., Gander, M., & Maier, R. (2018, August 27). Integrating threat intelligence to enhance an organization's information security management. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3230833.3232797

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *Journal of Marketing Theory and Practice*, *19*(2), 139–152. https://doi.org/10.2753/MTP1069-6679190202

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. In *European Business Review* (Vol. 31, Issue 1, pp. 2–24). Emerald Group Publishing Ltd. https://doi.org/10.1108/EBR-11-2018-0203

Hair, J. F., Sarstedt, M., Hopkins, L., & Kuppelwieser, V. G. (2014). Partial least squares structural equation modeling (PLS-SEM): An emerging tool in business research. *European Business Review*, *26*(2), 106–121. https://doi.org/10.1108/EBR-10-2013-0128

Hamdollah, R., & Baghaei, P. (2016). Partial least squares structural equation modeling with R. *Practical Assessment, Research and Evaluation*, *21*(1), 1–16.

Help Net Security. (2019). *Cybercriminals are becoming more methodical and adaptive*. https://www.helpnetsecurity.com/2019/04/26/cybercriminals-becoming-methodical/

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, *43*(1), 115–135. https://doi.org/10.1007/s11747-014-0403-8

Henseler, J., Ringle, C. M., & Sinkovics, R. R. (2009). The use of partial least squares path modeling in international marketing. *Advances in International Marketing*, *20*, 277–319. https://doi.org/10.1108/S1474-7979(2009)0000020014

Herring, C. (2020). *An Ounce of Prevention is Worth a Pound of SOAR*. Charles Herring's Blog. https://charlesherring.com/blog/ounce-prevention-worth-pound-soar#.XqabA2hKiUl

Hooper, D., Coughlan, J., & Mullen, M. R. (2008). Structural Equation Modelling: Guidelines for Determining Model Fit. *Electronic Journal of Business Research Methods*, *6*, 53–60. www.ejbrm.com

Huang, K., & Pearlson, K. (2019). *Building a Model of Organizational Cybersecurity Culture*.

Hutchins, E., Cloppert, M., & Amin, R. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *6th International Conference on Information Warfare and Security, ICIW 2011*, *July 2005*, 113–125.

IBM. (2020). *X-Force Threat Intelligence Index*. https://www.ibm.com/downloads/cas/DEDOLR3W

IBM Cloud Education. (2019). *What are Security Controls?* https://www.ibm.com/cloud/learn/security-controls

InfoSecurity Magazine. (2012). Technical controls not enough to ensure real cyber security. *InfoSecurity Magazine*. https://www.infosecurity-magazine.com/news/technical-controls-not-enough-to-ensure-real/

Kante, M., Kipchumba Chepken, C., Oboko, R., & Chepken, C. (2018). Partial Least Square Structural Equation Modelling ' use in Information Systems : an updated guideline of practices in exploratory settings. *Kabarak Journal of Research & Innovation*, *6*(1), 49–67. http://eserver.kabarak.ac.ke/ojs/

Khan, A. H., Sawhney, P. B., Das, S., & Pandey, D. (2020). Cyber Security Awareness Measurement Model (APAT). *2020 International Conference on Power Electronics and IoT Applications in Renewable Energy and Its Control, PARC 2020*, 298–302. https://doi.org/10.1109/PARC49193.2020.236614

Kilic, Hakan Katal, Neset Sertaç , Selcuk, A. A. (2019). Evasion Techniques Efficiency Over The IPS / IDS Technology. *UBMK 2019 - Proceedings, 4th International Conference on Computer Science and Engineering*, 542–547.

Kim, H., Ku, B., Kim, J. Y., Park, Y. J., & Park, Y. B. (2016). Confirmatory and exploratory factor analysis for validating the phlegm pattern questionnaire for healthy subjects. *Evidence-Based Complementary and Alternative Medicine*, *2016*. https://doi.org/10.1155/2016/2696019

Koschorreck, G. (2011). Automated audit of compliance and security controls. *Proceedings - 6th International Conference on IT Security Incident Management and IT Forensics, IMF 2011*, 137–148. https://doi.org/10.1109/IMF.2011.12

Kovacs, E. (2020). *FireEye Spotted Over 500 New Malware Families in 2019*. SecurityWeek. https://www.securityweek.com/fireeye-spotted-over-500-new-malware-families-2019

Lefkowitz, J. (2018). Compliance is Not Synonymous With Security. *SecurityWeek*. https://www.securityweek.com/compliance-not-synonymous-security

Lemnitzer, J. M. (2021). Why cybersecurity insurance should be regulated and compulsory. *Journal of Cyber Policy*, *6*(2), 118–136. https://doi.org/10.1080/23738871.2021.1880609

Lockheed Martin. (2019). *Gaining the advantage. Applying Cyber Kill Chain Methodology to Network Defense*. https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf

Lockheed Martin Corporation. (2015). Seven Ways to Apply the Cyber Kill Chain with a Threat Intelligence Platform. In *Seven Ways to Apply the Cyber Kill Chain® with a Threat Intelligence Platform*. https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Seven_Ways_to_Apply_the_Cyber_Kill_Chain_with_a_Threat_Intelligence_Platform.pdf

Maloney, K., Antelman, K., Arlitsch, K., & Butler, J. (2010). Future leaders' views on organizational culture. *College and Research Libraries*, *71*(4), 322–347. https://doi.org/10.5860/crl-47

MDaemon Technologies. (n.d.). *Alt-N Technologies: SecurityPlus for MDaemon - Antivirus & Security Software*. Retrieved February 14, 2021, from https://www.altn.com/Products/SecurityPlus-Antivirus-MDaemon/#InlineScanning

Merriam-Webster. (2022, February 27). *"False sense of security."* Merriam-Webster.Com Dictionary. https://www.merriam-webster.com/dictionary/false%20sense%20of%20security

Messaoud, B. I. D., Guennoun, K., Wahbi, M., & Sadik, M. (2017). Advanced Persistent Threat: New analysis driven by life cycle phases and their challenges. *2016 International Conference on Advanced Communication Systems and Information Security, ACOSIS 2016 - Proceedings*, 1–6. https://doi.org/10.1109/ACOSIS.2016.7843932

Microsoft Corporation. (2016). *Enhanced Mitigation Experience Toolkit 5.5*. https://download.microsoft.com/download/7/7/1/771312BF-53F1-4FE1-B894-8EE93ABE567E/EMET 5 5 User%27s Guide.pdf

Mohsin, M., & Anwar, Z. (2016). *Where to Kill the Cyber Kill-Chain: An Ontology-Driven Framework for IoT Security Analytics*. https://doi.org/10.1109/FIT.2016.12

Moore, T., Dynes, S., & Chang, F. R. (2015). Identifying How Firms Manage Cybersecurity Investment. *Workshop on the Economics of Information Security (WEIS), Berkeley, CA*, 1–27.

Morris, A. (2021). First the attack, then the lawsuits: Why every business should have cybersecurity insurance. *BenefitsPRO; New York*.

Muckin, M., & Fitch, S. C. (2019). *A Threat-Driven Approach to Cyber Security*.

Murayama, Y., Hikage, N., Hauser, C., Chakraborty, B., & Segawa, N. (2006). An Anshin model for the evaluation of the sense of security. *Proceedings of the Annual Hawaii*

International Conference on System Sciences, *8*(C), 1–10. https://doi.org/10.1109/HICSS.2006.46

Nadeem, S. M. (2016). *How to combat Advanced Persistent Threats*. Mailfence. https://blog.mailfence.com/tips-on-how-to-protect-your-data/

NIST. (2013). NIST Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations. *NIST SP-800-53 Ar4*, 400+. https://doi.org/10.6028/NIST.SP.800-53Ar4

NIST. (2020). *Security and Privacy Controls for Information Systems and Organizations*. https://doi.org/10.6028/NIST.SP.800-53r5

Palo Alto Networks. (2019). *PAN-OS® Administrator's Guide*. https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/pan-os/9-0/pan-os-admin/pan-os-admin.pdf

Park, I., Cho, J., & Rao, H. R. (2012). The effect of pre- and post-service performance on consumer evaluation of online retailers. *Decision Support Systems*, *52*(2), 415–426. https://doi.org/10.1016/j.dss.2011.10.001

Pavel, T. (2020). *Cyber Insurance Market in Israel-What is the Official Policy?*

Petters, J. (2020). *What is SIEM? A Beginner's Guide*. Veronis. https://www.varonis.com/blog/what-is-siem/

Pilkey, A. (2017). *Technology giving companies a false sense of security, says F-Secure Red Team*. https://www.f-secure.com/gb-en/press/p/technology-giving-companies-a-false-sense-of-security-says-f-secure-red-team

Pols, P. (2017). *The Unified Kill Chain Designing a Unified Kill Chain for analyzing, comparing and defending against cyber attacks*. https://www.csacademy.nl/images/scripties/2018/Paul-Pols---The-Unified-Kill-Chain.pdf

Positive Technologies. (2019). *Hack at all costs Putting a price on APT attacks*. https://www.ptsecurity.com/ww-en/analytics/advanced-persistent-threat-apt-attack-cost-report/

Pratt, M. K. (2017). *What is SIEM software? How it works and how to choose the right tool*. CSO Online. https://www.csoonline.com/article/2124604/what-is-siem-software-how-it-works-and-how-to-choose-the-right-tool.html

Razi K, A. (2017). Data Loss Prevention A Holistic Approach. In *SecureReading*. https://doi.org/10.1109/MITP.2010.52

Rezaee, Z., & Reinstein, A. (1998). The impact of emerging information technology on auditing. *Managerial Auditing Journal ; Bradford*, *13*(8), 465–471.

Rozenblum, D. (2001). Understanding Intrusion Detection Systems. In *Sans Institute (Information Sceurity Reading Room)*. https://www.sans.org/reading-room/whitepapers/detection/understanding-intrusion-detection-systems-337

Ruppert, B. (2007). Patch Management. In *Sans Institute (Information Sceurity Reading Room)*. https://www.sans.org/reading-room/whitepapers/iso17799/patch-management-2064

Samtani, S., Abate, M., Benjamin, V., & Li, W. (2019). Cybersecurity as an Industry: A Cyber Threat Intelligence Perspective. In *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 1–20). Springer International Publishing. https://doi.org/10.1007/978-3-319-90307-1_8-1

Sass, R. (2020). *The Equifax Saga: It Could Happen Again. Don't Let It*. InfoSecurity Magazine. https://www.infosecurity-magazine.com/opinions/equifax-could-happen-again/

Scarfone, K. A., & Mell, P. M. (2007). *Guide to Intrusion Detection and Prevention Systems (IDPS)*. https://doi.org/10.6028/NIST.SP.800-94

Scarfone, K., & Mell, P. (2007). Guide to Intrusion Detection and Prevention Systems (IDPS). In *Recommendations of the National Institute of Standards and Technology*. https://doi.org/10.4018/978-1-59904-379-1.ch012

Seals, T. (2013). *Organizations Struggle with Implementing Security Frameworks*. InfoSecurity Magazine. https://www.infosecurity-magazine.com/news/organizations-struggle-security/

Security Boulevard. (2018). *The Cyber Kill Chain: What You Need to Know*. https://securityboulevard.com/2018/08/the-cyber-kill-chain-what-you-need-to-know/

Seo, J. T., & Moon, J. (2006). Design and Implementation of a Patch Management System to Remove Security Vulnerability in Multi- platforms. *Fuzzy Systems and Knowledge Discovery, September 2006*. https://doi.org/10.1007/11881599

Shirish, T. S. (2014). *Research Methodology in Education*. Lulu.

Shukla, R. (2019). *Most SIEM Products Fail . And, So Does Threat Monitoring !* Peerlyst. https://www.peerlyst.com/posts/most-siem-products-fail-and-so-does-threat-monitoring-rajeev-shukla

Souppaya, M., & Scarfone, K. (2013). NIST Guide to Enterprise Patch Management Technologies. *NIST Special Publication 800-40*, 18.

Spitzner, L. (2019). *Applying Security Awareness to the Cyber Kill Chain*. SANS Institute. https://www.sans.org/security-awareness-training/blog/applying-security-awareness-cyber-kill-chain

Spooner, D., Silowash, G., Costa, D., & Albrethsen, M. (2018). Navigating the insider threat tool landscape: Low cost technical solutions to jump start an insider threat program. *Proceedings - 2018 IEEE Symposium on Security and Privacy Workshops, SPW 2018*, 247–257. https://doi.org/10.1109/SPW.2018.00040

Steiger, J. H. (2007). Understanding the limitations of global fit assessment in structural equation modeling. *Personality and Individual Differences*, *42*(5), 893–898. https://doi.org/10.1016/j.paid.2006.09.017

Tankard, C. (2011). Advanced Persistent threats and how to monitor and deter them. *Network Security*, *2011*(8), 16–19. https://doi.org/10.1016/S1353-4858(11)70086-1

The Radicati Group Inc. (2019). *Advanced Persistent Threat (APT) Protection Market, 2019-2023* (Issue 0). https://www.radicati.com/wp/wp-content/uploads/2019/01/APT_Protection_Market,_2019-2023_Executive_Summary.pdf

Thummala, J. B. (2016). Defending Advanced Persistent Threats - Be Better Prepared to Face the Worst. *InfoSecurity Magazine*. https://www.infosecurity-magazine.com/opinions/defending-advanced-persistent/

TrendMicro. (2017). *Best Practices: Deploying an Effective Firewall - Noticias de seguridad - Trend Micro MX*. Security Technology. https://www.trendmicro.com/vinfo/mx/security/news/security-technology/best-practices-deploying-an-effective-firewall

Valli, C., Woodward, A., Hannay, P., & Johnstone, M. (2014). Why Penetration Testing Is a Limited Use Choice for Sound Cyber Security Practice. *ADFSL Conference on Digital Forensics, Security and Law*, *c*, 35–40.

Verizon. (2019). *2019 Data Breach Investigations*.

Vincentis, M. de. (2017). *Micro-segmentation for Dummies, 2nd Vmware Special Edition* (2nd ed.). John Wiley & Sons. http://library1.nida.ac.th/termpaper6/sd/2554/19755.pdf

Virvilis-Kollitiris, N. (2015). *Detecting Advanced Persistent Threats through Deception Techniques* (Issue October).

Wilson, M., & Hash, J. (2003). Building an Information Technology Security Awareness and Training Program. In *NIST SP-800-50* (Issue October).

Wool, A. (2016). *Thwarting APT Attacks | Network Computing*. Network Computing. https://www.networkcomputing.com/network-security/thwarting-apt-attacks

Yang, L. X., Li, P., Yang, X., & Tang, Y. Y. (2018). A risk management approach to defending against the advanced persistent threat. *IEEE Transactions on Dependable and Secure Computing*. https://doi.org/10.1109/TDSC.2018.2858786

Yang, X., Zhang, T., Yang, L.-X., Wen, L., & Tang, Y. Y. (2017). *Assessing the risk of advanced persistent threats*. http://arxiv.org/abs/1707.02437

APPENDIX A: QUESTIONS (FACTORS)

The following is the questionnaire distributed to cybersecurity professionals with five or more years of work experience and work for a private (for-profit) organization.

Table 1. Questions (Factors) - Security Awareness and Training

Construct (Latent Variable)	Questions	References
Security Awareness and Training	Q2. Do you agree that organizations have actively managed security awareness and training programs?	(Al-Daeef et al., 2017) (Bada et al., 2014) (Wilson & Hash, 2003) (IBM, 2020) (Carella et al., 2017)
	Q3. Do you agree that the security awareness and training programs prepare an organization's employees to thwart cyber threats?	
	Q4. Do you agree that organizations test all employees periodically regarding security awareness by sending spoof phishing emails?	
	Q5. Do you agree that organizations mandate all new employees to take security awareness training before working on their job-related activities without exceptions?	
	Q6. Do you agree that organizations' security awareness training programs provide no significant value to prevent cyberattacks?	

Table 2. Questions (Factors) - Segmentation

Construct (Latent Variable)	Questions	References
Segmentation	Q7. Do you agree that network segmentation is a typical security practice in organizations? Example: development, research, quality, and production teams reside on different segments of the network and cannot talk to each other directly.	(Palo Alto Networks, 2019) (Vincentis, 2017) (Gordon et al., 2016) (Bradbury, 2019)

	Q8. Do you agree that organizations keep databases on a segmented and isolated network?	
	Q9. Do you agree that organizations keep their confidential data segmented into multiple tables residing in databases on segmented networks? (Microsegmentation of data: If one database and one network are compromised, cybercriminals cannot get the complete data leading to personal and confidential data exposure.)	
	Q10. Do you agree that organizations keep their source code repository segmented? (All source code cannot reside in a single repository. If the source code repository is segmented, it becomes harder for cybercriminals to steal source code and product designs)	
	Q11. Do you agree that organizations permit their employees to access source code repositories outside the corporate network without a VPN connection?	
	Q12. Do you agree that organizations enforce a policy preventing employees from sending source code as text (by email) outside the corporate domain?	
	Q13. Do you agree that an organization’s network access policy covers interdepartmental network access to enforce the security principle “need to know”?	
	Q14. Do you agree that organizations continuously monitor logs of source code repositories along with network and database access logs for security events?	

Table 3. Questions (Factors) - Cybersecurity Insurance

Construct (Latent Variable)	Questions	Reference
Cybersecurity Insurance	Q16. Do you agree that organizations carry a cybersecurity insurance policy to survive financially after a significant security incident?	(*Cybersecurity Insurance | CISA*, n.d.)
	Q17. Do you agree that organizations actively maintain an asset inventory list with raking from high value to low value?	

Table 4. Questions (Factors) - Insider Threat Prevention

Construct (Latent Variable)	Question	References
Insider Threat Prevention	Q18. Do you agree that organizations have an actively managed insider threat prevention program?	(Ben & Bhat, 2020) (Greitzer et al., 2019) (Spooner et al., 2018) (Greitzer et al., 2019)
	Q19. Do you agree that organizations enforce a policy preventing employees from sending documents/images/any attachments outside the corporate domain?	
	Q20. Do you agree that organizations have an actively managed BYOD policy for employees to connect to the corporate network to access email, MS Office, etc.?	
	Q21. Do you agree that organizations install mobile device management (MDM) software on employees' mobile devices without any exception if the employees can access corporate email, office software, etc.?	
	Q22. It is common for organizations to let employees access the corporate network from public WiFi or home network using their personal or corporate mobile devices. Do you agree that organizations can remotely wipe out an employee's mobile device if the mobile device is stolen or lost?	
	Q23. Do you agree that organizations install DLP (Data Loss/Leak Prevention) software at	

	the network level in organizations' environments?	
	Q24. Do you agree that organizations install a DLP (Data Loss/Leak Prevention) software on all employee laptops who potentially carry confidential business and customer data	
	Q25. Do you agree that organizations enforce a policy regarding the use of external hard drives or USB drives with corporate devices?	
	Q26. Do you agree that organizations perform threat hunting activities, either manually or automated?	
	Q27. Do you agree that organizations use behavior analytics tools to monitor privileged accounts and suspected user accounts?	
	Q28. Do you agree that organizations have an actively managed policy for source code repository access?	

Table 5. Questions (Factors) - Security Controls

Construct (Latent Variable)	**Questions**	**References**
Security Controls	Q29. Suppose organizations use a tool to deploy software updates/patches automatically. Do you think organizations have an actively managed process to conduct periodic checks to verify the installation of updates/patches?	(InfoSecurity Magazine, 2012) (IBM Cloud Education, 2019) (Moore et al., 2015) (Muckin & Fitch, 2019) (Lefkowitz, 2018) (Deloitte, 2010) (Koschorreck, 2011) (Conrad, 2014) (Grossman, 2013) (Souppaya & Scarfone, 2013)
	Q30. Do you agree that organizations have an actively managed policy to assess and consume third party (software and infrastructure) service providers (SaaS/PaaS/IaaS)?	
	Q31. Do you agree that organizations undertake appropriate due diligence before engaging third-party service providers to protect themselves from supply chain attacks	
	Q32. Do you agree that organizations have appropriate contractual mechanisms to be notified quickly of potential security issues	

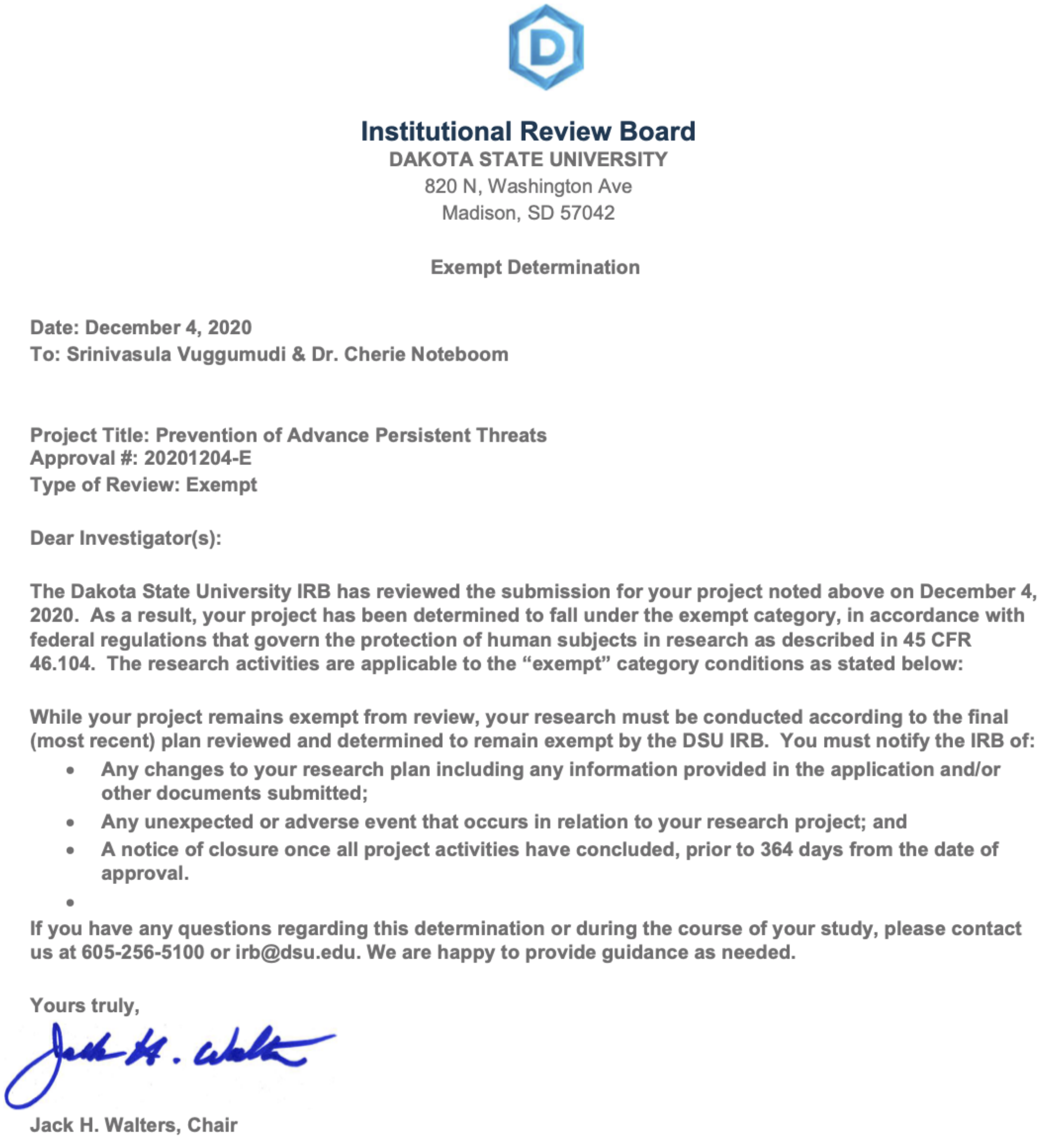
	with SaaS/IaaS/PaaS/other cloud service providers?	
	Q34. Do you agree that organizations implement processes and tools to monitor security controls continuously?	
	Q35. Do you agree that audit requirements drive the implementation of security controls in an organization but not an ever-changing security posture?	
	Q36. Do you agree that satisfying audit requirements drive the security budget instead of holistic security requirements?	
	Q37. Do you agree that in between audit cycles, maintaining/managing security controls get less attention?	
	Q38. Do you agree that compliance standards like NIST, PCI, etc. are static and do not update with the changing threat landscape?	
	Q39. Do you agree that security controls implemented to meet audit requirements are insufficient to protect an organization from cyberattacks?	
	Q40. Do you agree that auditors verifying the security controls generally lack in-depth security knowledge but go by a checklist?	
	Q41. Do you agree that auditors randomly verify the security controls, but not necessarily the essential security controls because of their missing in-depth security knowledge?	
	Q42. Do you agree that successfully meeting audit requirements regarding the security controls guarantees protection for an organization from the known security threats?	

Table 6. Questions (Single Factors) All Remaining Variables

Construct	**Question (Measure)**	**Reference**

Converged Testing (Latent Variable)	Q15. Do you agree that organizations design security tests (penetration tests, blue teaming, red teaming, etc.) to test all security controls (defenses-in-depth) at the same time? (Security controls in this context include both administrative and technical.)	(Chapple et al., 2018)
Redundant IDS/IPS (Latent Variable)	Q33. Having multiple products monitoring network traffic makes it easier for analysts to confirm the validity of alerts, identify false positives, and provide redundancy. Do you agree that organizations implement multiple IDS/IPS products monitoring their network?	(Cheng et al., 2012) (Kilic, Hakan Katal, Neset Sertaç , Selcuk, 2019) (K. Scarfone & Mell, 2007)
Sense of Security (Dependent Variable)	Q43. Are you confident about the cybersecurity posture (state) of organizations?	(Murayama et al., 2006)
Organization's Size (Moderator) ** Not included in the study	Q44. What is the size of your organization?	
Organization's Culture (Moderator)	Q45. What is the culture of your organization?	
Organization's Industry Sector (Moderator) ** Not included in the study	Q46. Which of the following best describes the industry sector of your organization?	

APPENDIX B: IRB APPROVAL



Institutional Review Board
DAKOTA STATE UNIVERSITY
820 N, Washington Ave
Madison, SD 57042

Exempt Determination

Date: December 4, 2020
To: Srinivasula Vuggumudi & Dr. Cherie Noteboom

Project Title: Prevention of Advance Persistent Threats
Approval #: 20201204-E
Type of Review: Exempt

Dear Investigator(s):

The Dakota State University IRB has reviewed the submission for your project noted above on December 4, 2020. As a result, your project has been determined to fall under the exempt category, in accordance with federal regulations that govern the protection of human subjects in research as described in 45 CFR 46.104. The research activities are applicable to the "exempt" category conditions as stated below:

While your project remains exempt from review, your research must be conducted according to the final (most recent) plan reviewed and determined to remain exempt by the DSU IRB. You must notify the IRB of:

- **Any changes to your research plan including any information provided in the application and/or other documents submitted;**
- **Any unexpected or adverse event that occurs in relation to your research project; and**
- **A notice of closure once all project activities have concluded, prior to 364 days from the date of approval.**
-

If you have any questions regarding this determination or during the course of your study, please contact us at 605-256-5100 or irb@dsu.edu. We are happy to provide guidance as needed.

Yours truly,

Jack H. Walters, Chair