Dakota State University

Beadle Scholar

Faculty Research & Publications

College of Business and Information Systems

Summer 7-12-2022

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

Srinivasulu R. Vuggumudi
Dakota State University

Yong Wang
Dakota State University

Jun Liu
Dakota State University

Cherie Noteboom
Dakota State University

Kaushik Ragothaman
Updated - AIS

Follow this and additional works at: https://scholar.dsu.edu/bispapers

Part of the Other Social and Behavioral Sciences Commons

Recommended Citation

Vuggumudi, S., Wang, Y., Liu, J., Noteboom, C., & Muthusamy Ragothaman, K. N. (2022). A False Sense of Security—Organizations Need a Paradigm Shift on Protecting Themselves against APTs . International Journal of Contemporary Research and Review, 13(07), 21851?21867. Retrieved from https://ijcrr.info/index.php/ijcrr/article/view/964

This Article is brought to you for free and open access by the College of Business and Information Systems at Beadle Scholar. It has been accepted for inclusion in Faculty Research & Publications by an authorized administrator of Beadle Scholar. For more information, please contact repository@dsu.edu.

International Journal of Contemporary Research and Review

Received 18-06-2022 | Revised 30-06-2022 | Accepted 10-07-2022 | Published Online 12-07-2022

https://ijcrr.info/index.php/ijcrr/article/view/964/992

ISSN (O) 0976-4852

IJCRR 13 (07), 21851–21867(2022)

Social Sciences and Humanities

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

Srinivasulu Vuggumudi[1] | Yong Wang[1] | Jun Liu[1] | Cherie Noteboom[1] | Kaushik Nagarajan Muthusamy Ragothaman[1]

[1]Dakota State University

Copyright : © 2021 The Authors. Published by Publisher. This is an open access article under the CC BY-NC-ND license (https://creativecommons.org/licenses/by-nc-nd/4.0/).

Abstract:

Advanced Persistent Threats (APTs) are among the most complex cyberattacks and are generally executed by cyber-attackers linked to nation-states. An organization may have security strategies to prevent APTs. However, a false sense of security may exist when the focus is on implementing security strategies but not on the effectiveness of implemented security strategies. This research aims to find out 1) if organizations are in a false sense of security while preventing APT attacks, 2) what factors influence the false sense of security, and 3) whether organizational culture influence factors contributing to the false sense of security. A theoretical model is developed to evaluate the sense of security to answer the three research questions. The initial model includes seven independent variables, one moderator variable, and one dependent variable. We designed and conducted a survey among cybersecurity professionals to test 14 hypotheses on the sense of security. We further refined and finalized the model based on the data analysis from the survey data. This research confirms that employees are not confident about organizations' cybersecurity posture despite all the awareness training, technological advancements, and massive investment. We also identified key factors which influence the employee perception of cybersecurity posture. Based on the research findings, we provided recommendations that can be followed to improve the effectiveness of implemented security strategies.

Keywords: Advanced Persistent Threats, APTs, Cybersecurity, Sense of Security, False Sense of Security

I. Introduction

The United States Air Force coined the phrase Advanced Persistent Threat (APT) in 2006 [1]. An advanced persistent threat is defined as "an entity that engages in a malicious, organized, and highly sophisticated long-term or reiterated network intrusion and exploitation operation to obtain information from a target organization, sabotage its operations, or both" [2]. An APT attack is a prolonged, aimed attack on a specific target, in which cyber attackers gain access to a system or network and remain there for an extended period without being detected. 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 Stuxnet and the recent Solar Winds attacks indicate the severity of the impact of successful APT attacks on organizations.

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 [2], [3]. Cybercriminals use multiple vectors and entry points to breach enterprise networks and evade detection for months. APTs present a challenge for organizations because of their complexity, duration, and undetectability.

“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” [4]. A false sense of security is simply the belief that some situation is safer than it is [5]. Technologies and processes often provide organizations with a false sense of security. Enterprises rely on technical solutions to protect themselves from APTs. APTs are looming threats to enterprises, both large and small enterprises. Despite the awareness training, technological advancements, and massive investment adopted in many organizations, APT attacks still happen often [6]. It implies that sophisticated tools alone cannot prevent organizations from APT attacks [7]. Several vaunted enterprises like Google, RSA, DuPont, Walt Disney, Johnson & Johnson, Morgan Stanley, Sony, General Electric, etc., were also victims of APT attacks [8]. An organization may have security strategies to prevent APTs. However, the benefits of the implemented security strategies to the organization’s security posture might be negligible. A false sense of security may exist when an organization focuses on implementing security strategies but not on the effectiveness of implemented security strategies.

On the other hand, organizational security strategies are driven by compliance requirements. There is a 125% increase in cybersecurity incidents, impacting every industry and geography year by year. APTs are considered a significant factor in this increase. Most data breaches in recent years have happened at compliant businesses. Being compliant alone does not help them evade APT attacks. The effectiveness of security strategies directly influences on an organization’s sense of security. Hence, it is critical to understand the factors that influence the false sense of security to help organizations ensure the effectiveness of implemented security strategies. Research on the sense of security is emerging. There is no empirical information systems research that focuses on this area. This research aims to understand if organizations are in a false sense of security while preventing APT attacks and if their culture influences their preventive measures. Motivated by the discussed theoretical and practical concerns, our research targets to provide answers to two research questions (RQs): RQ1) What are the most critical factors (practices/controls) contributing to the false sense of security? RQ2) Does organizational culture influence defenses against APT attacks?

In this paper, we proposed a research model that theorizes various factors that influences the sense of security. Specifically, we explored the relationship between the security measures and employees' perceived sense of security in organizations. This kind of relationship is never examined before in the academic literature. Our findings indicate the sense of security of employees is low when the security controls are ineffective. We identified what factors contribute to enhancing the sense of security. We also highlight what is missing in organizations while they consider their defenses to prevent APT attacks.

The remainder of this paper is organized as follows. Section II discusses background on APTs, and theoretical models utilized in information security research. Section III presents our proposed theoretical model for this research and the proposed hypotheses. Section IV introduces the methodology adopted for this research, followed by data analysis and results, discussion, and research limitations in Sections V, VI, and VII. Section VIII summarizes and concludes the paper.

II. Background

APTs present a challenge due to their unique and complex nature. Therefore, security professionals face an uphill battle in defending their networks as attacks become increasingly sophisticated, particularly when it comes to APTs. The lack of typical attack patterns and the constantly new combination of different modes of attacks and vectors make APT attacks unpredictable and extremely difficult for organizations to detect [9].

Our literature review indicates that: 1) Cyber attackers hopelessly outclass off-the-shelf solutions [10][11]. 2) Employees need security education and a sober understanding of the protection of systems to secure their critical assets [12],[13]. 3) If critical/basic security controls are not in place, it makes no sense to place advanced controls like Security Orchestration, Automation, and Response (SOAR) [14]. 4) Organizations focus heavily on tools to prevent APT attacks; non-technical attack vectors such as insider threat and social engineering are not given much-needed attention [6],[14],[16] . 5) Penetration testing practice and compliance frameworks [16],[17] adopted by organizations were not effective. The evaluation of security strategies has been focused on meeting compliance requirements and tools. Vulnerabilities are often found in the daily execution of organizational activities[19]. Security risk needs to be considered from an organizational perspective [19].

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) [20], the Theory of Planned Behavior[21], the Health Belief model [22] exist and have been utilized in empirical research in information security. However, the models in [20],[21],[22] 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 look into this problem and propose a theoretical model for evaluating organizational security strategies in terms of the sense of security.

III. Theoretical Model for Evaluating 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. 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 dependent variable, Sense of security, in this research represents the confidence level of employees about the strategic organizational activities of security. The proposed research model is illustrated in Figure 1.

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 [23]. 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. However, 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.

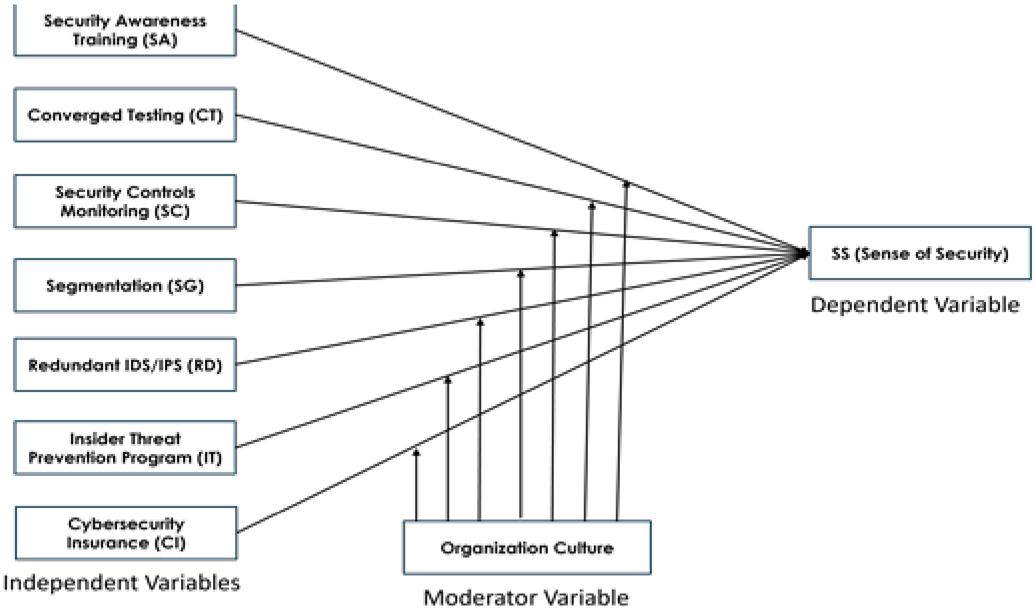


Figure 1: Research Model for Evaluating Sense of Security

Information security culture is a subculture of an organization's culture [24]. To enhance an organization's cybersecurity culture, management must implement the latest technology and invest in the organizational culture [24]. Organizations with a medium to high-security risk profile need to embed the information security culture to influence employee actions and behaviors about information security practices[25]. In this research, we considered organizational culture as a moderator variable to find out how organizational culture influences the relationship between the independent and dependent variables. The following subsections describe our research constructs.

A. Security Awareness and Training (SA)

"Security awareness training is a usually overlooked factor in most of implemented information security programs" [12]. In the context of Information Technology (IT), security awareness and training programs are the typical means used to communicate security requirements and appropriate behavior [26]. Industry compliance standards/requirements make organizations run security awareness programs. However, IT security awareness and training programs can quickly become obsolete if not updated with the technology advancements, IT infrastructure, and organizational changes, and shifts in organizational mission and priorities [13]. If organizations do not keep their security awareness and training programs current, employees find no value in the security awareness and training program and lose motivation.

B. 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" [27]. Examples of technical or logical 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" [27]. Examples of administrative controls include policies, procedures, hiring practices, background checks, data classifications, and labeling. The focus is on technical controls during security testing (penetration testing, blue team testing, purple team testing, or red team testing). Our literature review did not find any testing methodology that includes administrative controls in the security testing scope. We selected converged (administrative and technical controls) testing as an independent variable.

C. Security Controls (SC)

The countermeasures organizations implement to detect, prevent, reduce, counteract, or minimize security risks are called security controls [28]. 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 [29]. It is important to note that most data breaches in recent years have happened at compliant businesses [30]. Setting up the security controls is one challenge and effectively monitoring and auditing them is another challenge.

D. Segmentation (SG)

Network segmentation is an architectural approach that involves dividing a more extensive network into smaller network segments, which can be accomplished through firewalls, virtual local area networks, and other separation techniques. 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. Data center design includes segmentation as a fundamental information security principle, however, 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 [31].

E. Redundant IDS/IPS (RD)

Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS) are the first line of defense for organizations against cyberattacks. The war between attackers and IDS/IPS developers never ends [32]. Even though an IDS/IPS system is mostly reliable, there is a possibility that an attacker can evade, which creates a significant gap in cybersecurity. IDS/IPS systems are improved continuously against evasion techniques, but new evasion techniques that can bypass IDS/IPS systems are still evolving [33]. Implementing redundant IDS/IPS systems is crucial in setting up defenses against APT attacks. If one IDS/IPS cannot detect data exfiltration, another IDS/IPS from a different vendor may detect data exfiltration. Having multiple IDS/IPS systems to monitor the same activity makes it easier for analysts to confirm the validity of alerts and identify false positives. It also provides redundancy should one product fail for any reason [34].

F. 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” [35]. 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 [36]. 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: 1) user activity monitoring, 2) data loss prevention, 3) security information and event management, 4) analytics, and 5) digital forensics and investigations [37].

G. Cybersecurity Insurance (CI)

Cybersecurity and Infrastructure Security Agency (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” [38]. Since APT attacks involve data exfiltration and an organization can go bankrupt after a successful cyberattack, we selected cybersecurity insurance as an independent variable to verify organizations' preparedness for APT attacks.

H. Sense of Security (SS)

Sense of security can be better explained with the Japanese word, Anshin. Anshin is formed by “An” which means to ease, and “Shin,” which is to mind. Someone feels Anshin when they are free from worry and fear [39]. Confidence keeps someone away from worry and fear, which means having confidence equals Anshin. Sense of security in our research represents the confidence level of employees about the strategic organizational activities of security.

I. 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” [40]. 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 [41].

Table 1 summarizes the operational definition of our constructs.

TABLE 1: Constructs and Hypotheses Definition

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) [41]

This research aims to find answers for 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.

VI. Research Methodology

A. Research Method

Our research approach is quantitative using the survey method. The quantitative approach is the best choice when the study's objective is to identify factors that influence an outcome, the utility of an intervention, or understanding the best predictors of outcomes [42]. We designed a survey that 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.” This research received IRB approval from the Dakota State University.

There are seven constructs in the proposed model, as shown in Figure 1. Five of the constructs, including security controls, insider threat prevention, cybersecurity insurance, segmentation, and security awareness and training, need to be measured with a group of observable variables. Both converged testing and redundant IDS/IPS have only one observable variable. The survey questions are regarding cybersecurity controls, and practices followed in the industry. The data collected is participants’ perceptions of cybersecurity controls and practices followed in the industry. The survey subjects are cybersecurity professionals with five or more years of work experience working for a private (for-profit) organization.

B. *Data Collection*

The Survey Monkey platform was used to administer the survey questionnaire and collect responses from the survey participants. The survey is anonymous. Using the Anonymous Responses collector option provided by Survey Monkey, we eliminated the possibility of tracking and storing identifiable respondent information in survey results. The survey was distributed to 600 qualified participants using email and LinkedIn in spring 2021. There were 253 returned questionnaires out of 600 distributed. 207 out of 253 returned questionnaires were useable, with an 82% completion rate.

C. *Data Analysis Method*

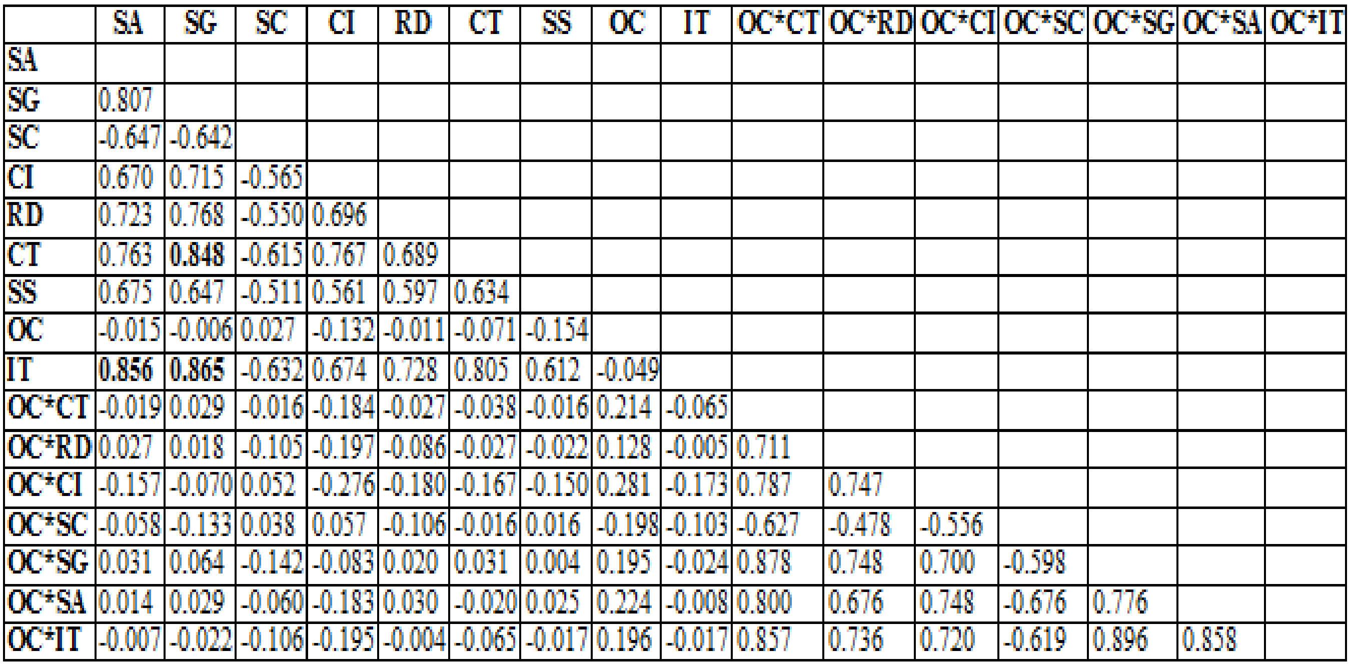
Confirmatory Factor Analysis (CFA) allows for more precise testing of an instrument's factor structure. CFA addresses construct validity by assigning the items in an instrument to their respective factors according to theoretical expectations [43]. CFA helps to determine the model fit. The result of CFA analysis provides several model fit indices such as root mean square error of approximation (RMSEA), comparative fit index (CFI), and Tucker–Lewis index (TLI) to determine model fit for further analysis [44]. 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 modeling (PLS-SEM). Warp PLS was used to conduct PLS-SEM.

V. Data Analysis and Results

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. Factor loading value of ≥ 0.7 indicates a strong relationship between the item (observable variable) and the factor [45]. 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 [44]. 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 [46], [47].

TABLE 2. 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	

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 2 shows the correlations among the constructs. As shown in Table 2, 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 2.

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.

A. 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 [48]. Factor loadings of all constructs are above the recommended value of 0.708, as shown in Table 3.

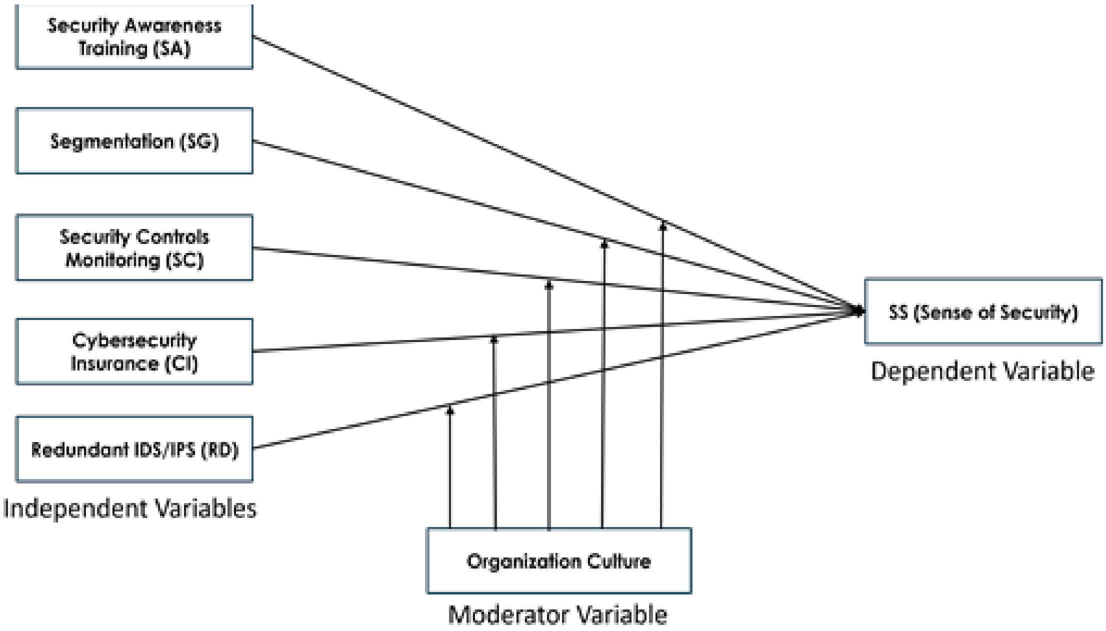


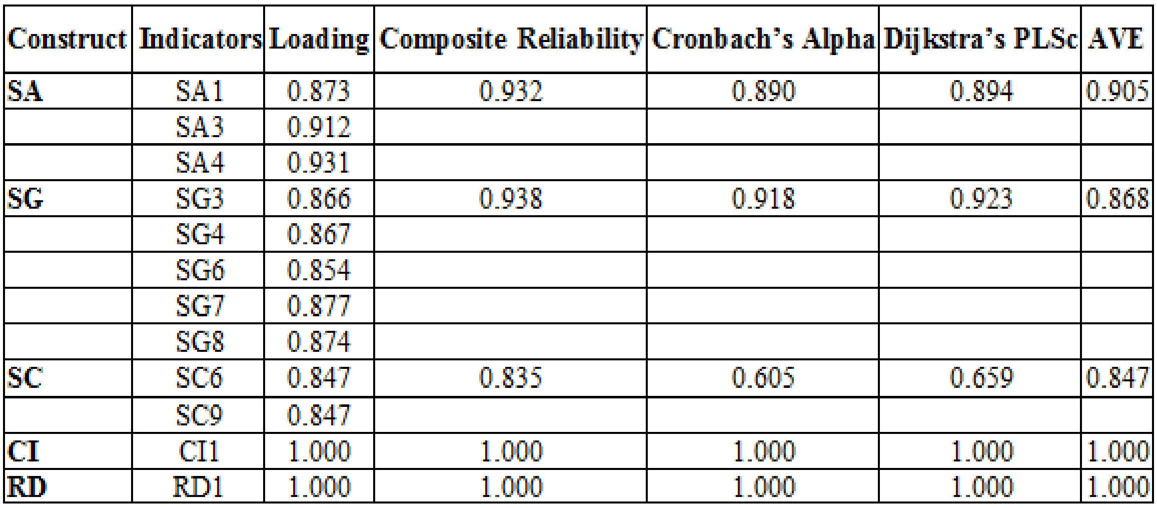
Figure 2: Refined Research Model for Evaluating Sense of Security

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 [48]. 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, The 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 [48]. 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) [49]. The

Cronbach’s alpha values of all the constructs are shown in Table 3. The Cronbach’s alpha values of the constructs under study are in the excellent to the reliable range.

“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” [48]. 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[50].

TABLE 3: FACTOR LOADINGS, CR, CRONBACH’S ALPHA, DIJAKSTRA’S PLSC, AVE



Construct	Indicators	Loading	Composite Reliability	Cronbach’s Alpha	Dijkstra’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

The Dijkstra’s PLSc values of all constructs lie between Cronbach’s alpha value and CR value, as shown in Table 3. Internal consistency reliability of constructs was verified with factor loadings, composite reliability, Cronbach’s alpha, and Dijkstra’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” [48]. 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 [48], [51], [52].

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 [48]. 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 [48]. The threshold value for HTMT is 0.90, and HTMT value above 0.90 suggests lack of discriminant validity[53]. The HTMT ratio values for the constructs in our model are below the threshold value of 0.90, as shown in Table 4, confirming that discriminant validity is present.

TABLE 4: HTMT RATIOS

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

.

B. 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 [48], [54]. The VIF values of predictor variables in our model are below, as shown in Table 5. Therefore, there is no collinearity issue.

TABLE 5: VIF VALUES

	SA	**SG**	**SC**	**CI**	**RD**
VIF	3.902	4.447	2.014	2.855	3.156

Since there is no collinearity issue, 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 [48].

The coefficient of determination (R^2) is considered in the case of endogenous constructs [48], 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 [54], [55]. The R^2 value of our research model is 0.52, as shown in Figure 3. 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" [48]. The Q^2 value of our research model is 0.622. Thus, our research model's predictive relevance is high.

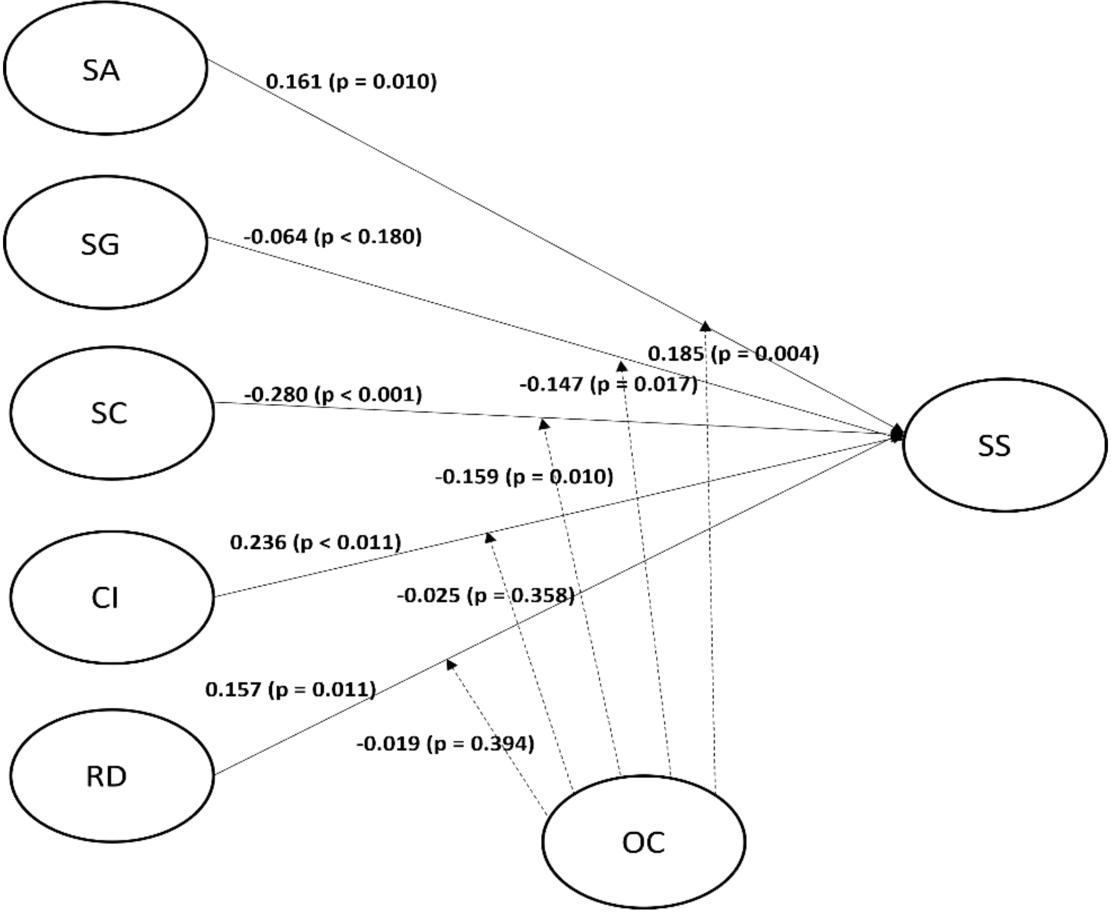


Figure 3: Coefficient of Determination

C. Hypotheses Testing

H1 states that successful implementation of security awareness and training positively impacts the sense of security. Table 6 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 converged 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 6 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 positively impacts the sense of security. Table 6 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 greater than 0.05 (significance > 0.05). Therefore, it can be concluded that the successful implementation of segmentation does not positively impact the sense of security.

H5 states that successful implementation of redundant IDS/IPS positively impacts the sense of security. Table 6 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 6 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 6 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 converged testing was dropped from the study.

H10 states that organizational culture moderates the relationship between security controls and the sense of security. Table 6 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 6 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 6 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 greater 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 6 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 greater 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 6: 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

VI. 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 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 are important factors that influence employees' sense 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, converged testing and insider threat prevention, from the initial model.

We suggest the following recommendations for the constructs contributing to false sense of security to improve the effectiveness of the controls in combating APTs:

A. *Security Awareness and Training:*

Security awareness and training campaigns should measure the impact of the awareness sessions rather than only tracking who attended those sessions, the number of users who passed the exams, etc. We recommend a cyber security awareness measurement model: Analyze, Predict, Awareness, and Test (APAT) [56]. 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.

B. *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" [57]. We recommend redundancy in setting up IDS/IPS. 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 [34].

C. *Security Controls*

Security controls are the countermeasures that organizations implement to detect, prevent, reduce, counteract, or minimize security risks are called security controls [28]. 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 [29]. We recommend considering a CTI platform because of its agility without much human intervention. 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.

D. *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 [58]. It pays for the legal services required after the attack. APT attacks involve data exfiltration. Hence, it is possible that an organization can go bankrupt after a successful cyberattack. We recommend adding cybersecurity insurance to the organization's security program.

Table 7 below shows our recommendation for enhancing controls based on NIST 800-53 Security and Privacy Controls [59]. We selected the NIST 800-53 set of controls to enhance security because it is more complex, more restrictive, and contains more security controls than necessary for any business sector [60].

Table 7: Security and Privacy Controls to Remediate False Sense of Security

Independent Variable	NIST Control	Action Item
Security Controls	CA-2 Control Assessments	Enhance the security control by ensuring 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 appropriate 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.

VII. 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 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) Cybersecurity is a vast domain. It is hard to select and limit the number of independent variables in the research.

VIII. Conclusion and 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 security budget at the right place. The research confirms that organizations need a paradigm shift on protecting themselves against APTs. We dropped two independent variables, converged testing and insider threat prevention, due to correlations with segmentation. In further research, the two constructs we dropped may need to be reevaluated to find out what caused correlations due to their presence. Further, additional independent variables could be considered in the research model.

References:

[1] R. Betlich, “Demystifying APT,” *Information Security*, no. August. 2010.

[2] A. Ahmad, J. Webb, K. C. Desouza, and J. Boorman, “Strategically-motivated advanced persistent threat: Definition, process, tactics and a disinformation model of counterattack,” *Comput. Secur.*, vol. 86, no. July, pp. 402–418, 2019.

[3] P. Chen, L. Desmet, and C. Huygens, “A study on advanced persistent threats,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 8735 LNCS, pp. 63–72, 2014.

[4] A. Pilkey, “Technology giving companies a false sense of security, says F-Secure Red Team.” 2017.

[5] Merriam-Webster, “False Sense Of Security | Definition of False Sense Of Security by Merriam-Webster.” .

[6] FireEye, “M-Trends 2020.” p. 60, 2020.

[7] S. Vuggumudi and Y. Wang, “Sophisticated Tools Alone Cannot Prevent Advanced Persistent Threats: What’s Next?,” *Inf. Syst. Secur. Assoc. J.*, vol. 18, no. 6, pp. 33–39, 2020.

[8] R. A. Grimes, “Prepare for advanced persistent threats, or risk being the next RSA,” *CSO Online*. 2011.

[9] AV-Test, “APT: Strategic Attacks Require Strategic Tests.” 2020.

[10] P. Technologies, “Hack at all costs Putting a price on APT attacks.” 2019.

[11] N. Virvilis-Kollitiris, “Detecting Advanced Persistent Threats through Deception Techniques,” no. October. p. 174, 2015.

[12] M. M. Al-Daeef, N. Basir, and M. M. Saudi, “Security awareness training: A review,” *Lect. Notes Eng. Comput. Sci.*, vol. 2229, pp. 446–451, 2017.

[13] M. Wilson and J. Hash, “Building an Information Technology Security Awareness and Training Program,” *NIST SP-800-50*, no. October. p. 70, 2003.

[14] C. Herring, “An Ounce of Prevention is Worth a Pound of SOAR,” *Charles Herring’s blog*. 2020.

[15] Verizon, “2019 Data Breach Investigations.” 2019.

[16] H. N. Security, “Cybercriminals are becoming more methodical and adaptive.” 2019.

[17] C. Valli, A. Woodward, P. Hannay, and M. Johnstone, “Why Penetration Testing Is a Limited Use Choice for Sound Cyber Security Practice,” *ADFSL Conf. Digit. Forensics, Secur. Law*, no. c, pp. 35–40, 2014.

[18] M. Bromiley, “What Security Practitioners Really Do When It Comes to Security Testing.” 2020.

[19] W. T. Yue, M. Çakanyildirim, Y. U. Ryu, and D. Liu, “Network externalities, layered protection and IT security risk management,” *Decis. Support Syst.*, vol. 44, no. 1, pp. 1–16, 2007.

[20] F. D. Davis, “A technology acceptance model for empirically testing new end-user information systems: Theory and results,” Massachusetts Institute of Technology, 1985.

[21] I. Ajzen, "From Intentions to Actions: A Theory of Planned Behavior," in *Action Control: From Cognition to Behavior*, J. Kuhl and J. Beckmann, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 1985, pp. 11–39.

[22] M. H. Becker, "The health belief model and personal health behavior," *Health Educ. Monogr.*, vol. 2, pp. 324–473, 1974.

[23] O. Adelaiye, A. Ajibola, and S. Faki, "Evaluating Advanced Persistent Threats Mitigation Effects : A Review," *Int. J. Inf. Secur. Sci.*, vol. 7, no. 4, pp. 159–171, 2018.

[24] K. Huang and K. Pearlson, "Building a Model of Organizational Cybersecurity Culture." pp. 1–25, 2019.

[25] J. S. Lim, S. Chang, S. Maynard, and A. Ahmad, "Exploring the Relationship between Organizational Culture and Information Security Culture," *Proc. 7th Aust. Inf. Secur. Manag. Conf.*, 2009.

[26] M. Bada, A. Sasse, and S. A. N. Jason Bada M., "Cyber Security Awareness Campaigns: Why They Fail to Change Behavior," *Int. Conf. Cyber Secur. Sustain. Soc.*, p. 11, 2014.

[27] M. Chapple, J. M. Stewart, and D. Gibson, *(ISC)2 CISSP Certified Information Systems Security Professional Official Study Guide, 8th Edition*, 8th Editio. Sybex, 2018.

[28] I. B. M. C. Education, "What are Security Controls?" 2019.

[29] M. Muckin and S. C. Fitch, "A Threat-Driven Approach to Cyber Security." pp. 1–45, 2019.

[30] J. Lefkowitz, "Compliance is Not Synonymous With Security," *SecurityWeek*, 2018.

[31] M. De Vincentis, *Micro-segmentation for Dummies, 2nd Vmware Special Edition*, 2nd ed. John Wiley & Sons, 2017.

[32] T. H. Cheng, Y. D. Lin, Y. C. Lai, and P. C. Lin, "Evasion techniques: Sneaking through your intrusion detection/prevention systems," *IEEE Commun. Surv. Tutorials*, vol. 14, no. 4, pp. 1011–1020, 2012.

[33] N. S. S. Ali Aydin Kilic Hakan Katal, "Evasion Techniques Efficiency Over The IPS / IDS Technology," *UBMK 2019 - Proceedings, 4th Int. Conf. Comput. Sci. Eng.*, pp. 542–547, 2019.

[34] K. Scarfone and P. Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS)," *Recommendations of the National Institute of Standards and Technology*. 2007.

[35] S. Ben and A. Bhat, "Insider Threat Report by Securonix." p. 67, 2020.

[36] F. L. Greitzer, J. Purl, Y. M. Leong, and P. J. Sticha, "Positioning Your Organization to Respond to Insider Threats," *IEEE Eng. Manag. Rev.*, vol. 47, no. 2, pp. 75–83, 2019.

[37] D. Spooner, G. Silowash, D. Costa, and M. Albrethsen, "Navigating the insider threat tool landscape: Low cost technical solutions to jump start an insider threat program," *Proc. - 2018 IEEE Symp. Secur. Priv. Work. SPW 2018*, pp. 247–257, 2018.

[38] "Cybersecurity Insurance | CISA," *Cybersecurity & Infrastructure Security Agency*. .

[39] Y. Murayama, N. Hikage, C. Hauser, B. Chakraborty, and N. Segawa, "An Anshin model for the evaluation of the sense of security," *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, vol. 8, no. C, pp. 1–10, 2006.

[40] R. Farooq and S. Vij, "Moderating Variables in Business Research," *IUP J. Bus. Strateg.*, vol. 14, no. 4, pp. 34–54, 2017.

[41] K. Maloney, K. Antelman, K. Arlitsch, and J. Butler, "Future leaders' views on organizational culture," *Coll. Res. Libr.*, vol. 71, no. 4, pp. 322–347, 2010.

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

[43] M. M. Ahmad, "Psychometric evaluation of the Cognitive Appraisal of Health Scale with patients with prostate cancer," *J. Adv. Nurs.*, vol. 49, no. 1, pp. 78–86, 2005.

[44] H. Kim, B. Ku, J. Y. Kim, Y. J. Park, and

Y. B. Park, “Confirmatory and exploratory factor analysis for validating the phlegm pattern questionnaire for healthy subjects,” *Evidence-based Complement. Altern. Med.*, vol. 2016, 2016.

[45] I. Park, J. Cho, and H. R. Rao, “The effect of pre- and post-service performance on consumer evaluation of online retailers,” *Decis. Support Syst.*, vol. 52, no. 2, pp. 415–426, 2012.

[46] D. Hooper, J. Coughlan, and M. R. Mullen, “Structural Equation Modelling: Guidelines for Determining Model Fit,” *Electron. J. Bus. Res. Methods*, vol. 6, pp. 53–60, 2008.

[47] J. H. Steiger, “Understanding the limitations of global fit assessment in structural equation modeling,” *Pers. Individ. Dif.*, vol. 42, no. 5, pp. 893–898, 2007.

[48] J. F. Hair, J. J. Risher, M. Sarstedt, and C. M. Ringle, “When to use and how to report the results of PLS-SEM,” *European Business Review*, vol. 31, no. 1. Emerald Group Publishing Ltd., pp. 2–24, 2019.

[49] K. S. Taber, “The Use of Cronbach’s Alpha When Developing and Reporting Research Instruments in Science Education,” *Res. Sci. Educ.*, vol. 48, no. 6, pp. 1273–1296, 2018.

[50] T. K. Dijkstra and J. Henseler, “Consistent partial least squares path modeling,” *MIS Quarterly: Management Information Systems*, vol. 39, no. 2. University of Minnesota, pp. 297–316, 2015.

[51] M. Kante, C. K. Chepken, R. Oboko, and C. Chepken, “Partial Least Square Structural Equation Modelling ’ use in Information Systems : an updated guideline of practices in exploratory settings,” *Kabarak J. Res. Innov.*, vol. 6, no. 1, pp. 49–67, 2018.

[52] J. F. Hair, G. T. M. Hult, C. M. Ringle, and M. Sarstedt, “A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM) Second Edition.” p. 137, 2017.

[53] J. Henseler, C. M. Ringle, and M. Sarstedt, “A new criterion for assessing discriminant validity in variance-based structural equation modeling,” *J. Acad. Mark. Sci.*, vol. 43, no. 1, pp. 115–135, 2015.

[54] J. F. Hair, C. M. Ringle, and M. Sarstedt, “PLS-SEM: Indeed a silver bullet,” *J. Mark. Theory Pract.*, vol. 19, no. 2, pp. 139–152, 2011.

[55] J. Henseler, C. M. Ringle, and R. R. Sinkovics, “The use of partial least squares path modeling in international marketing,” *Adv. Int. Mark.*, vol. 20, pp. 277–319, 2009.

[56] A. H. Khan, P. Bahl Sawhney, S. Das, and D. Pandey, “SartCyber Security Awareness Measurement Model (APAT),” in *2020 International Conference on Power Electronics & IoT Applications in Renewable Energy and its Control (PARC)*, 2020, pp. 298–302.

[57] C. Tankard, “Advanced Persistent threats and how to monitor and deter them,” *Netw. Secur.*, vol. 2011, no. 8, pp. 16–19, 2011.

[58] A. Morris, “First the attack, then the lawsuits: Why every business should have cybersecurity insurance,” *benefitspro*, 2021. [Online]. Available: https://www.benefitspro.com/2021/07/09/lawyers-say-every-business-should-buy-cybersecurity-insurance-412-118395/?slreturn=20220522205512.

[59] NIST, “Security and Privacy Controls for Information Systems and Organizations,” 2020.

[60] K. J. Slonka, “MANAGING CYBER SECURITY COMPLIANCE ACROSS BUSINESS SECTORS.,” *Issues Inf. Syst.*, vol. 21, no. 1, 2020.

How to cite this article: Vuggumudi, S., Wang, Y., Liu, J., Noteboom, C., & Muthusamy Ragothaman, K. N. (2022). A False Sense of Security—Organizations Need a Paradigm Shift on Protecting Themselves against APTs . International Journal of Contemporary Research and Review, 13(07), 21851-21867. Retrieved from https://ijcrr.info/index.php/ijcrr/article/view/964