Information Management and Business Review (ISSN 2220-3796)
Vol. 15, No. 1, pp. 1-13, March 2023 (SI)

Assessing Information Security Competencies of Firm Leaders towards Improving Procedural Information Security Countermeasure: Awareness and Cybersecurity Protective Behavior

Saif Hussein Abdallah Alghazo[1], Norshima Humaidi*[2], Shereen Noranee[3]
[1]Registration Authority, Abu Dhabi Global Market, Al-Maria Island, Abu Dhabi,
United Arab Emirates
[2,3]Faculty of Business and Management, Universiti Teknologi MARA (UiTM), Selangor, Malaysia
norshima958@uitm.edu.my*

Abstract: Cybersecurity threats are a serious issue faced by many organizations in this new information era. Therefore, security leaders play a significant role not only to ensure that all their employees are practicing good security behavior to protect organizational information assets but also to ensure that security technology has been installed properly to protect network infrastructure. This study aims to examine cybersecurity protective behavior (CPB) among employees in the organization and focus on the role of leadership competencies and information security countermeasure awareness. The questionnaires were distributed via email and self-administered, and the study managed to obtain 245 responses. Partial Least Squares-Structural Equation Modeling (PLS-SEM) analysis was used to analyze the final data. Confirmatory factor analysis (CFA) testing shows that all the measurement items of each construct were adequate in their validity individually based on their factor loading value. Moreover, each construct is valid based on its parameter estimates and statistical significance. The research findings show that Procedural Information Security Countermeasure (PCM) awareness strongly influences CPB compared to a leader's information security competencies (ISI). Meanwhile, ISI significantly influences PCM awareness. This study adapts the theory of leadership competencies in the context of cybersecurity, which is particularly beneficial to any industry in improving organizational information security strategic plans.

Keywords: *Cybersecurity Leaders, Cybersecurity Protection Behavior, Information Security, Information Security Competencies, Information Security Awareness*

1. Introduction and Background

Vulnerabilities may arise from the Internet-based interconnection of digital devices and information systems that can function in the cloud (Baikloy et al., 2020). Therefore, we need cybersecurity to guard against cyberthreats and vulnerabilities and protect an organization's data and information technology (IT) assets (Yeoh et al., 2022). In doing so, we need good cybersecurity strategic planning. Human errors, which result from the improper execution of an appropriate action sequence, such as poorly written communication (prescriptions, documentation, and transcribing), are the most problem in information security (Wong et al., 2022). According to Keers et al. (2013), human negligence and noncompliance with regulations are two common causes of human errors.

In both established and developing countries, there have recently been a lot of cybersecurity issues related to fraud and data breaches (Wong et al., 2022; Newman, 2019). A prominent bank in the banking sector recently issued a scam alert in Malaysia, warning consumers about a new fake bank website (which looks similar to the real website of the bank) that has been set up by fraudsters to steal financial information. Through messages delivered via WhatsApp, SMS, or emails, these scammers tried to persuade users to log into fake websites (The Star, 2021). Malicious cyberattacks have surged by 600% from 2016 to 2020, according to Symantec's Internet Security Threat report. Likewise, the Malaysia Computer Emergency Response Team (MyCERT) received reports of 10,699 cyberattacks in total in 2018 (Bernama.com, 2020).

The majority of these attacks—429 cases in total were categorized as ransomware attacks. A virus attack known as a ransomware attack encrypts files and/or locks people out of their devices. Users may be required to pay a "ransom" during a ransomware attack to recover their files (Zimba et al., 2018). More than 100,000 businesses across at least 150 countries were negatively impacted by the most well-known ransomware, "Wannacry" (Bernama.com, 2020). Recent research suggests that ransomware instances point to the likelihood that cyber attackers will target businesses to profit financially (CyberSecurity Malaysia, 2019). As a result, there have been significant financial outlays for operational costs, data recovery costs, and other related costs (Ahmad et al., 2021; Corallo, Lazoi, and Lezzi, 2020; Li et al., 2019; CyberSecurity Malaysia, 2019).

The latest security technologies, such as biometrics, firewalls, smartcards, and encryption, have been implemented by many organizations (Kreicberga, 2010), but employees' attitudes towards information security are still influenced by human error, which leads to information security problems (Park, Ruighaver and Ahamad, 2010). This is corroborated by data showing that human mistake accounts for 90% of cybersecurity issues (Kemper, 2019). Studies contend that technological advances cannot completely ensure effective information security if the information security behaviors of employees do not strongly conform to established cybersecurity norms in organizations. According to Kemper (2019), numerous firms have lost millions of dollars as a result of inadequate response times to security issues and careless employee activity. Equally, several organizations have fallen victim to cybersecurity breaches due to employee negligence, and non-compliance with their organization's information security policies (Willison and Warkentin, 2013).

Employees' cybersecurity behaviors may reflect inconsiderate actions such as not creating strong passwords, sharing passwords, leaving devices connected to the internet without any online protection, logging in to company systems through unsecured networks, and being offhand while handling organizational data and information (Akhunzada et al., 2015). Therefore, as suggested by previous studies, exploring the issues of cybersecurity protective behaviors are essential (Vance et al., 2012; Schuetz et al., 2020). Cain et al. (2018) also argued that implementing good cybersecurity behavior can promote safe cyberspace and behaviors, hence reinforcing cybersecurity protective behaviors (CPB). Moreover, driving successful CPB has been debated to also depend on the efficient use of the security manager's information security intelligence (ISI) skills to manage employee behaviors in ways that tightly underpin and inspire increased CPB (Cain et al., 2018; Kemper, 2019).

Although there are many studies on cybersecurity, there aren't many studies that evaluate ISI skills (Corallo et al., 2020), especially in developing nations like Malaysia. Due to a lack of employee security awareness, poor security skills, inadequate security monitoring and enforcement, as well as inappropriate cybersecurity behaviors, cybersecurity threats still exist in many companies from various sectors (Ameen et al., 2021; Safa et al., 2019). Thus, deploying ISI skills is important to train and equip employees with adequate knowledge of cybersecurity and help them better understand the consequences of exhibiting pro-security actions in handling organizational data and information (Kimani et al., 2019). Congruent with the debates of Ameen et al. (2021), effective implementation of ISI skills can aid employees in developing their self-awareness towards cybersecurity issues. This can be more effective if the leaders implement efficient information security procedures and guidelines (Safa et al., 2019). Providing effective information security training and education (SETA Program) that is also known as procedural information security countermeasure (PCM), is essential since several employees are still negligent in complying with information security policies (ISPs) accordingly (da Veiga et al., 2020). However, given the distinct and continued volatility of the business in the cyberspace and security environment of organizations, it is yet unclear from the literature how ISI skills directly predict PCM and CPB. These clear gaps in the literature necessitate this study's motivation and thus, call for closer attention.

Based on the above review, this study is conducted to explore the skills of organizational security leaders relevant to combating cybersecurity threats and enhancing cybersecurity protective behavior among employees in today's era. ISI and PCM concepts have been adapted to develop a holistic cybersecurity protective behavior model because both components are essential in enhancing employee behavior to practice cybersecurity adequately. Thus, this study aims to contribute by exploring and providing an integrative framework that reflects the roles of PCM awareness and ISI skills to predictively influence CPB. The subsequent sections discuss both concepts and the research findings.

2. Literature Review

Leadership Competencies

Northouse (2010) defined leadership as having the authority and capacity to persuade people to accomplish shared objectives. Leadership was defined by another researcher as "the process of influencing others to understand and agree about what needs to be done and how to do it and the process of facilitating individual and collective efforts to accomplish shared objectives" (Yulk, 2006, p. 8). Rowley and Sherman's (2003) additional definition emphasizes that leadership is a critical component of any organization since it influences the accomplishment of goals and objectives. In contrast, leadership was characterized by Bratton and Gold (2012) in terms of intrapersonal and interpersonal attributes (behavior, traits, role, influence, position, and interaction between members or groups). Implicit in these definitions of leadership are the competencies a leader should have to achieve the desired organizational goals and objectives.

Good leaders often have the right leadership competencies. Cleveland and Cleveland (2018) contended that competent leaders usually have the passion to help others and are considered inspired leaders by their subordinates. According to earlier research, people's skills, abilities, cognitive intelligence, and social intelligence can all be used to measure a person's competencies (Boyatzis, 2011). Additionally, Korzynski et al. (2021) claimed that for staff to engage in both strategic and daily planning, they needed to possess leadership qualities. They assist in making an organization, department, or team's vision a reality in this way. Therefore, a leader with the right competencies will be able to improve the firm’s performance. Today’s business leaders are often assessed by their ability to relay brand consistency, authenticity and company transparency. They are judged on their corporate values, strategic vision, management practices and community contributions. However, forward-thinking leaders will keep information security on their priority list. Among the competencies that leaders should possess in guaranteeing business information security are business acumen, resilience, team-building skills, problem-solving skills, communication skills, collaboration skills, and strong interpersonal skills (Cleveland and Cleveland, 2018; Sussman, 2021; Triplett, 2022). A leader needs to be seen by the employees that their leader has the right cybersecurity competencies. Hassan (8 Mar 2022, Cybrary) argued that effective business leaders should take seriously on security compliance as an element of operations. Hassan further explained that leaders should be protective and able to manage thoroughly to guarantee business information security. This would relay confidence among the staff that their leaders are serious about growth and they are mindful of what is required to build a successful business.

Leaders who have the right cybersecurity competencies would reduce cybersecurity risk (Triplett, 2022). These highly competent leaders build and strengthen the cybersecurity workforce. These skilled cybersecurity leaders are critical for leading effective cybersecurity teams and defending organizations against ever-increasing cyber threats (McFadden, 2021). Furthermore, the employees’ cybersecurity behavior is the outcome of how the firms’ leader channels attention to their decision (Shaikh and Siponen, 2022). The decision made depends on the leader’s intelligence to deal with indicated situations.

Information Security Intelligence (ISI) Competencies and Cybersecurity Protective Behavior

Depending on the size or culture of the business, the security leaders responsible for managing information security hold a variety of titles, including Chief Information Security Officer (CISO), Information Security Director (ISD), and Information Security Manager (ISM), among others. The job of this role, which is distinct from that of an information security expert, is dedicated to managing information security. According to Haqaf and Koyunchu (2018), they are typically in charge of ensuring the establishment of security processes, systems, policies, standards, and guidelines, communicating with all organization members about how to protect information assets, making security-related decisions, working with internal and external stakeholders for all operations, and supervising the security expert teams.

According to earlier research, a leader is crucial in raising employees' understanding of information security (Khando et al., 2021; Hwang et al., 2019). According to Hwang et al. (2019), managerial security participation appeared to have the strongest correlation with workers' awareness. From planning to implementation, the firm's CEO must be actively involved in all facets of cyber governance. Investments in cybersecurity must be treated as strategic investments, and this competency's growth must be closely supervised (Abraham et al., 2019). In earlier studies, the researchers recommended that businesses invest more in human capital rather than technology. This is due to the fact that most security events are brought on by internal personnel who are sloppy, negligent, or incapable of using security tools appropriately (Hong and Furnell, 2021; da Veiga et al., 2020). The management may support information security wholeheartedly, but if the internal employees do not understand the value of modeling information security behavior and do not care about it, the security goals will not be met.

In order to boost employees' information security compliance intention behavior, Kim, Hovav and Han (2020) also recommended that the company's security executives exhibit information security expertise and problem-solving skills. Other studies have shown that the information security leader is crucial to supporting information security initiatives and ensuring the success of the organization's information security awareness programs (Hong and Furnell, 2021; Ameen et al., 2021). Employee engagement in adopting good cybersecurity behavior will decline if top management does not support the adoption of security rules and processes (Hasan et al., 2021). The company's top management should be proactive in its cybersecurity efforts. Previous research (Khando et al., 2021; Kim et al., 2020; Li et al., 2019) demonstrated a favorable effect of top management participation on the information security awareness program, which functions as a catalyst for the information security awareness of the employees.

The effectiveness of security decision-making will also be impacted by the security leaders' lack of cybersecurity knowledge and expertise (Ani et al., 2018). Additionally, it causes a decline in the effectiveness of information security management. According to other empirical studies (Khando et al., 2021; Humaidi and Balakrishnan, 2018), employees' shared understanding is determined by how they view management's role in the workplace and how persuasive security managers' communication is. Therefore, this study examined how security leaders' ISI influenced employees' understanding of information security procedures and how that aspect may have an impact on how they behave in terms of cybersecurity protection. The ability of security leaders to influence their subordinates to practice information security behavior, the ability to use accumulated knowledge from experience or training to detect security threats and techniques, as well as the degree to which the leader can respond promptly with appropriate countermeasures are all examples of information security competencies according to the current study. To that end, the ensuing hypotheses were created.

H1: Information security competencies of security leaders positively affect employees' cybersecurity protective behavior. (This is a valuable ability to be had in a firm's security leader, which can make very valuable contributions towards raising positive cybersecurity protective behavior amongst the employees.)

H2: Information security competencies of security leaders positively affect employees' procedural information security countermeasure awareness. (In this case, if the information security leader has adequate competencies in handling cybersecurity issues in the organization, it will be able to improve employees' awareness of how to combat the issues.)

Procedural Information Security Countermeasure Awareness and Cybersecurity Protective Behavior

If the employees are unaware of the information security policies and procedures, they cannot be effectively applied. According to a study by Li et al. (2019), employees who are knowledgeable about their company's information security policy and procedures are more equipped to handle cybersecurity activities than those who are not. Therefore, it is essential that these policies are implemented accurately and appropriately across the company and that they are actually communicated to all employees (Ahmad et al., 2021). Alghamdi (2021) asserts that it is crucial to make sure that every employee in the company is aware of the information security policies as this would improve their comprehension of information security. Thus, this will improve employees' information security protection behavior. According to earlier research, employees' behavior regarding cybersecurity compliance was directly influenced by their awareness of cybersecurity countermeasures (Donalds and Osei-Bryson, 2020; Kim et al., 2020). Employee security awareness can be raised and this can help to reduce human error and harmful behavior (Parsons et al., 2014). According to Safa et al. (2015), the organization should effectively develop security awareness programs and ensure that they are relevant and consistent because these factors are crucial for the effectiveness of this program.

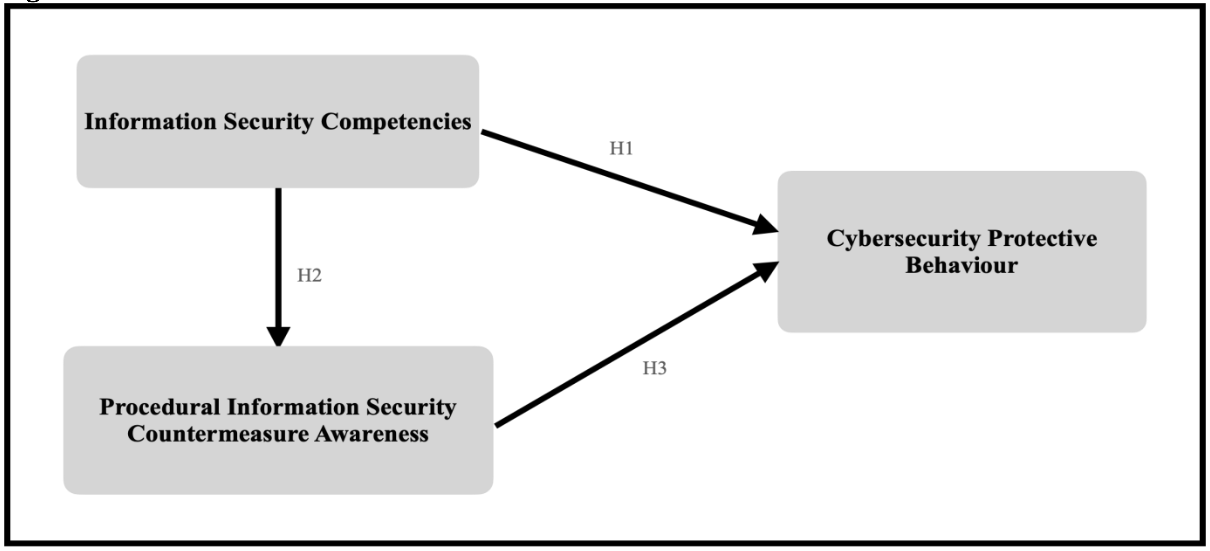
In this study, the procedural information security countermeasure awareness (PCM) was adopted from a study by Kim et al. (2020) that has provided the rules and guidelines to help employees understand their roles and responsibilities in complying with standards for the use of organizational information and technology resources. In addition, PCM has a deterrent effect through ongoing organizational efforts that reinforce acceptable usage guidelines and emphasize the potential punishment for misuse of information assets (D'Arcy, Hovav and Galletta, 2009; Puhakainen and Siponen, 2010). Thus, the following hypothesis was constructed:

H3: Procedural information security countermeasure (PCM) awareness positively affects employees' cybersecurity protective behavior. (Under this dimension, if the employees have good knowledge of cybersecurity countermeasure procedures, it will lead them to protect organizational assets properly in the cyber world.)

Research Model

As discussed in the previous section, this study posits information security competencies of the security leaders and procedural information security countermeasure awareness as an independent variable. Meanwhile, the dependent variable of this study was cybersecurity protective behavior which is focused on behavior related to device securement behavior, updating behavior and proactive behavior related to handling cybersecurity threats. The proposed model is shown in Figure 1.

Figure 1: Research Model


Information Security Competencies
H1
H2
Cybersecurity Protective Behaviour
H3
Procedural Information Security Countermeasure Awareness

3. Research Methodology

The study's target respondents were employees from various companies in Klang Valley, Malaysia. A purposive sampling technique was utilized to find the ideal respondent for the study. The minimum sample size was determined using GPower calculating software. The minimum sample size needed was 40 because the model (Figure 1) had a maximum of three predictors, the effect size was big (0.35), and the power needed was 0.85. However, this study manages to receive a total of 245 data. Several difficulties have been taken into account for ethical considerations, including the confidentiality statement and informed consent for the respondents.

Using the IBM Statistical Package for Social Sciences (SPSS) version 26, the respondent profile was examined to begin the data analysis for the study. The IBM SPSS was also used to test data normality and any data error has been cleaned up. The measurement and structural model were investigated using the statistical method of partial least squares (PLS)-Structural Equation Modeling (SEM) utilizing the SmartPLS 3.3.6 version (Ringle et al., 2015). When examining proposed theoretical models, PLS-SEM focuses on explaining the variance in the dependent variable because it is primarily intended for exploratory research (Hair et al., 2014). PLS is the preferred data analysis method for the current study's context since it prioritizes prediction above parameter accuracy (Gefen, Rigdon and Straub, 2011). The following part goes through the study's measuring model and structural model.

4. Results

The majority of the respondents are female (n = 137) compared to male (n = 108). In terms of age, the majority of the respondents (n = 212) are under or equal to 40 years old, as opposed to the respondents who are above 40 (n = 33). The majority of respondents (n = 58) come from the education sector, which is followed by finance and banking (n = 45), and the transportation and automated (n = 28) sectors. The majority of respondents (n = 136) had a bachelor's degree or higher, which was followed by a diploma (n = 56), a master's degree (n = 27), and a professional degree (n = 12), among other levels of education. Other categories of respondents (n = 4) only completed their primary and secondary education.

In terms of their jobs, 64 respondents have managerial roles, while 75 hold executive positions. Academicians (n = 58), low-level positions (n = 9) and others (n = 39) made up the remaining slots. Compared to respondents with more than 10 years of experience, the majority of respondents (n = 147) have less than or equal to 10 years of work experience. In contrast to 93 respondents who said they had never faced an attack, the majority of respondents (n = 152) said they have encountered cybersecurity threats. The characteristics of the entire sample of respondents who took part in the study are summarized in Table 1.

Table 1: Demographic Details

Demographic Variable		Frequency	Percentage
Gender			
	Male	108	44.1
	Female	137	55.9
Age			
	Less than or equal to 40 years old	212	86.5
	More than 40 Years old	33	13.5
Type of Industry			
	Education	58	23.7
	Utilities	19	7.8
	Construction	10	4.1
	Health	13	5.3
	Finance/Banking	45	18.4
	Transport/Automotive	28	11.4
	Manufacturing	11	4.5
	Media	5	2.0
	ICT	6	2.4
	Food	10	4.1
	Electric and Electronic	4	1.6
	Others	36	14.7
Qualification			
	Professional Certificate	2	0.8
	Diploma	56	22.9
	Advanced Diploma	6	2.4
	Bachelor Degree	136	55.5
	Professional Degree	12	4.9
	Master Degree	27	11.0
	PhD	2	0.8
	Other	4	1.6
Position			
	Administrative Staff	9	3.7
	Executive Level	75	30.6
	Assistant Manager	10	4.1
	Manager	18	7.3
	Senior Manager	25	10.2
	Assistant Engineer	1	0.4
	Engineer	9	3.7
	Senior Engineer	1	0.4
	Academic Staff/Academician	58	23.7
	Others	39	15.9
Working Experience			
	Less than or equal to 10 years	147	60.0
	More than 10 years	98	40.0
Do you have experience with cybersecurity threats?			
	Yes	93	38%
	No	152	62%
	Total (n)	245	100

A common method bias (CMB) assessment was conducted because this study's data were acquired from a single source, as proposed by Podsakoff et al. (2003). To measure the presumed source of method variance as a covariate in the statistical analysis, this study employed the marker variable technique. The marker variable used in this study is made up of three unrelated items using the methods suggested by Rönkkö and Ylitalo (2010). According to the CMB findings, adding marker variables had no discernible impact on either the Beta (β) value or R^2 changes.

The composite reliability (CR) index and the average variance extracted (AVE) index were used in this study to calculate the reliability of the measures. Both indices—0.7 for the CR index and 0.5 for the AVE index—were greater than the evaluation requirement for all measurements. Convergent validity evaluates the coherence between many constructs. According to Table 2, all values fell within the suggested range, suggesting convergent validity and internal consistency reliability (Hair et al., 2014).

The Heterotrait-Monotrait Ratio of Correlations (HTMT) was employed to evaluate the discriminant validity (Henseler, Ringle and Sarstedt, 2015). An HTMT value greater than 0.85 indicates a problem with discriminant validity. Referring to the recommendations made by Gold et al. (2001), who stated that the validity of the concept is still acceptable if the score is higher than the HTMT value of 0.90 and lower than 1. All of the HTMT values (Table 2) results are below the threshold level of 0.90, and the HTMT inference also demonstrates that none of the constructs' confidence interval levels showed a value of 1. These findings clearly reported that the discriminant validity of the constructs has been deemed acceptable and was not a serious threat in this study.

Table 2: Convergent and Discriminant Validity

				Discriminant Validity (HTMT)		
Variables	Cronbach's Alpha	Composite Reliability	Average Variance Extracted (AVE)	1	2	3
(1) Cybersecurity Protective Behaviour	0.865	0.894	0.517			
(2) Manager's Infosec Competencies	0.946	0.965	0.903	0.586		
(3) Procedural Inforsec Countermeasure Awareness	0.933	0.946	0.691	0.811	0.644	

The values of the corresponding loadings and cross-loadings were then assessed to see whether there were any issues with any specific variable indicators in the complete model. To find out if the items were equally loaded on all the constructs in addition to their own, cross-loadings were computed. For loadings to be deemed significant in the current study, a cut-off value of 0.7 or above was employed (Hair et al., 2014). According to the findings (Table 3), the majority of the indicators measuring a given construct had loading values of more than 0.6 for that construct. This led to results, which supported the validity of the indicators for each concept.

Table 3: Cross Loadings

Measurement Items	**Procedural Inforsec Countermeasure Awareness**	**Cybersecurity Protective Behaviour**	**InfoSec Competencies**
Email Policies	0.693	0.625	0.638
Website Policies	0.843	0.569	0.499
Computer resources policies	0.912	0.735	0.496
Information system policies	0.812	0.493	0.485
Infosec Policies Training	0.924	0.607	0.579
Infosec threat briefing	0.914	0.661	0.544
Infosec education program	0.614	0.490	0.266
Consequences of IS Misuse	0.885	0.732	0.507
Updating behavior	0.593	0.613	0.180
Updating behavior	0.424	0.728	0.461
Device securement behavior 1	0.389	0.612	0.154

Measurement Items	Procedural Inforsec Countermeasure Awareness	Cybersecurity Protective Behaviour	InfoSec Competencies
Device securement behavior 2	0.519	0.753	0.381
Proactive awareness behavior 1	0.692	0.774	0.398
Proactive awareness behavior 2	0.577	0.778	0.496
Proactive awareness behavior 3	0.471	0.638	0.521
Proactive awareness behavior 4	0.548	0.823	0.476
Perceived Infosec Knowledge	0.587	0.462	0.937
Perceived Infosec Problem Solving	0.625	0.589	0.958
Perceived Social Competence	0.538	0.484	0.956

T-values, p-values, and bootstrapped confidence intervals were obtained using the bootstrapping process with a resampling rate of 500. Table 4 displays the final results. The direct relationship between information security competencies and PCM awareness and CPB was examined in this study. Furthermore, the direct relationship of PCM awareness was also tested on CPB. There were three (3) hypotheses tested. The results have shown that all the hypotheses (H1 until H3) were supported. PCM awareness strongly influences CPB (β = .669, t = 13.668, p < .000, f^2 = .647) compared to information security competencies (β = .131, t = 2.154, p < .016, f^2 = .025). The results also indicated that PCM awareness explained 37.9% of the variance in information security competencies of the manager. This has shown that other possible variables can influence PCM awareness. Meanwhile, the information security competencies of the security leaders and PCM awareness explained 57.2% of the variance in CPB.

Table 4: Hypotheses Testing Result

Hypotheses	Relationship	Beta Weight	Std Dev	T-Value	P-Value	5.00%	95.00%	f^2	R^2	Result
H1	Infosec Competencies -> Cybersecurity Protective Behaviour	0.131	0.061	2.154	0.016	0.036	0.233	0.025	57.2%	Supported
H2	Infosec Competencies -> Procedural Inforsec Countermeasure Awareness	0.616	0.039	15.636	0.000	0.547	0.677	0.612	37.9%	Supported
H3	Procedural Inforsec Countermeasure Awareness -> Cybersecurity Protective Behaviour	0.669	0.049	13.668	0.000	0.576	0.741	0.647	-	Supported

The blindfolding method, as shown in Table 5, was used to assess the predictive validity of the research model. Based on the blindfolding procedure, Q^2 evaluates the predictive validity of a large complex model using PLS. While estimating parameters for a model under the blindfolding procedure, this technique omitted data for a given block of indicators and then predicted the omitted part based on the calculated parameters. As a result, Q^2 demonstrates how well the model and PLS parameters may be used to reconstruct the empirically acquired data. According to the results, using an omission distance (D) of 7, this study obtained a Q^2 of 0.281, which is more than the cut-off value of 0.0 (Hair et al., 2014), thereby indicating that the research model in this study has predictive relevance. The relative impact of the research model calculated by obtaining Q^2 showed that PCM has a strongly impacted

(0.445) on CPB, while information security competencies of the manager indicated a small impact (0.014) on CPB.

Table 5: Predictive Relevance Result

Dependent Variable	Q^2	Q^2 *(excluded ISI)*	Q^2 *(excluded PCM)*	q^2 *(excluded ISI)*	q^2 *(excluded PCM)*
Cybersecurity Protective Behaviour	0.281	0.277	0.156	0.014	0.445

Discussion

It has been demonstrated that procedural information security countermeasure (PCM) awareness is a crucial element in improving the cybersecurity protective behavior (CPB) of employees. The current finding is consistent with earlier research on human behavior and information security (Mausavi et al., 2020; Kim et al., 2020). According to Li et al. (2019), companies can be far more cautious about making sure that their employees are more responsible in cyberspace if they are aware of cyber security protection. Other studies that strongly showed how crucial it is for an organization to plan its security awareness program successfully (Hadlington et al., 2018) also lend credence to this. According to Mausavi et al. (2020), increased knowledge of cybersecurity protection has been a powerful motivation for excellent cybersecurity protective behavior.

This study has also found that information security competencies among firm leaders (ISI) can enhance employees' CPB. Information security leaders such as Chief Information Security Officers (CISO) or security managers are responsible for ensuring that the necessity for information security intelligence and the protection motivation for cybersecurity behavior is instilled in the organization's employees (Kim et al., 2020). The role of the CISO is even more crucial for organizations operating in modern business environments since the use of IoT in operating the business exposes a major security risk (Pang and Tanriverdi, 2022). In addition, from strategy to implementation, the CISO must actively participate in all facets of cyber governance (Hina, Selvam and Lowry, 2019). Investments in cybersecurity must be treated as strategic investments, and this competency's growth must be closely supervised. According to previous studies (Jeong and Zo, 2021; Balapour et al., 2020), companies should invest more in human capital rather than technology. This is due to the fact that the majority of security events are brought on by internal members who are careless or incapable of using security tools effectively (Wong et al., 2022). Although the top management fully supports information security, the security goals will not be met if the employees are ignorant of or uninterested in performing good information security behavior.

5. Managerial Implications and Recommendations

In terms of theoretical views, this study has highlighted the role of information security intelligence skills among security leaders in enhancing employees' cybersecurity motivation to practice cybersecurity behavior adequately, especially in this modern era. This study extended the concept of PMT by introducing a new construct (information security intelligence skills) that is essential in combating cyber-attack in this new era. The COVID-19 pandemic has forced many businesses to change their work lifestyles from working at the office to a hybrid work environment (Yeoh et al., 2022). These new work environments create new vulnerabilities for businesses and the rise of sophisticated cyber-attacks is very disturbing. Thus, organizations need to adapt their security management accordingly (Ahmad et al., 2021).

In terms of practical view, this study lies in the fact that it will help business organizations to determine the flaws that are present in the system, for example, cases of data security theft or compromise of encrypted information. It would also help them understand how these flaws make their system vulnerable. Thereby, it will help the organizations develop measures that can help them determine how these issues can be resolved. Therefore, it is important of strategizing information security planning in the organization before developing and implementing information security policies and the SETA program. It depends on the success of adopting information security policy and organizational strategies to combat cyber-attacks, according to Li et al. (2019), to ensure that information security technology solutions are implemented successfully. Therefore, information security should be prioritized at the board level of a corporation so that technical or information security officers are also responsible for cybersecurity in addition to everyone else. This is urgent when previous findings had found that most internal security incidents are a consequence of misuse actions including privilege abuse, unapproved hardware, embezzlement, ignorance of information security policies and data mishandling (Torten, Reaiche and Boyle, 2018). The top management needs to consider how to make this better to raise employee understanding of procedural information security countermeasures. The effectiveness of security approaches and processes (Hwang et al., 2019) adopted in the organization, particularly in metropolitan areas, can be increased as a result, reducing security-related negligence.

Conclusion

This study has been conducted to achieve a few important things.

First of all, the results of the study help future researchers to better understand the factors motivating the awareness of employees and cybersecurity protective behavior, particularly the employees who work in today's business environments. In this direction, the study will also try to understand the role of the managers who have a responsibility to play in enhancing information security awareness and how it translates into better attitudes and behavior towards this issue.

Secondly, this study analyzed the current situation in today's business environment, concerning the necessity for cybersecurity awareness since cybersecurity threats are rapidly evolving. The management of the company should organize and design information security training, awareness programs (SETA Programs), and implement ISPs to demonstrate support for information security behavior. Employees can learn about organizational ISPs through information security training, awareness campaigns, and the implementation of ISPs (Ameen et al., 2021; Koskosas et al., 2011). These initiatives aim to introduce and inform employees about the significance of using security countermeasures to avert information security threats and the impact of these threats on the organization.

In addition, top management should ensure that ISPs during training and awareness programs clearly define employee responsibilities, authorized and prohibited uses of the systems, reporting procedures for system threats, definitions of penalties for violations, and the availability of a mechanism to update ISPs (Whitman, 2004). Moreover, the firm's management is also responsible to ensure that the employees working in the organization have a high sense of cybersecurity protective awareness. To ensure that, the firm's security management team led by Chief Information Security Officer (CISO) must take proactive steps to educate the employees about cybersecurity protective measures. The security management team is also responsible to determine what constitutes good cybersecurity behavior for the employees. It is then their responsibility to take feedback on whether these behavior points are being followed or not by all the employees (Whitman and Mattord, 2019).

The most important role of the security management team is to promote a positive cybersecurity protective attitude amongst the employees. They achieve this by educating the employees, providing them with training and organizing workshops (Humaidi and Balakrishnan, 2018). In addition to that, they are responsible to ensure the fact that the necessity for information security intelligence and the protection motivation for cybersecurity behavior is instilled among the employees of the organization (Kim et al., 2020). The role of the security management team is even more crucial especially in modern business environments, since the use of IoT and cloud computing is evolving (Lee, 2021).

Nevertheless, future studies should conduct a quantitative analysis of the present situation and the measures that have been taken by the organizations operating in the digitalization business environment. The study helps the current researcher to better understand the issue at hand, namely the importance of information security intelligence skills and the factors motivating the behavior of employees in the organization, towards cybersecurity and protection. It is also hoped that future researchers will explore further the role of several factors including the role of the ISIs and the firm's management in influencing the attitude and behavior of the employees towards developing awareness about cybersecurity protection and countermeasures to be made.

This study can prove to be very useful in serving as a basis for broader and more detailed research about the current issue for getting a more generalized perception. It has also proven useful in addressing the various issues; hence it can be utilized for solving any flaws that exist, effectively and efficiently. Lastly, through this study, an attempt will be made to increase focus on the ways in which the current flaws can be improved. Thus, the future study will encourage to exploration other methods through which the modern organizations will be able to address this situation in a better manner and introduce improvements to their current situation.

Acknowledgment

We would like to thank Universiti Teknologi MARA (UiTM) for awarding us this project grant [600-RMC/GPK 5/3 (094/2020)].

References

Ahmad, A., Maynard, S. B., Desouza, K. C., Kotsias, J., Whitty, M. T., Baskerville, R. L. (2021). How can organizations develop situation awareness for incident response: A case study of management practice? Computers & Security, 101, 1-15.

Akhunzada, A., Sookhak, M., Anuar, N. B., Gani, A., Ahmed, E., Shiraz, M. (2015). Man-At-The-End attacks: Analysis, taxonomy, human aspects, motivation and future directions. *Journal of Network and Computer Applications*, 48(0), 44-57.

Alghamdi, M. I. (2021). Determining the impact of cyber security awareness on employee behavior: A case of Saudi Arabia. Materials Today: Proceedings, Retrieved from https://doi.org/10.1016/j.matpr.2021.04.093

Ameen, N., Tarhini, A., Mahmood Hussain Shah, Madichie, N., Paul, J. & Choudrie, J. (2021). Keeping customers' data secure A cross-cultural study of cybersecurity compliance among the Gen-Mobile workforce. Computers in Human Behavior, 114, 1-19.

Ani, U. D., He, H. & Tiwari, A. (2018). Human factor security: evaluating the cybersecurity capacity of the industrial workforce. Journal of Systems and Information Technology, 21(1), 2-35.

Baikloy, E., Praneetpolgrang, P., Jirawichitchai, N. (2020). Development of cyber re-salient capability maturity model for cloud computing services. TEM Journal, 9(3), 915–923.

Bernama.com (2020). Gov't actively addressing cyber threats, crimes – DPM. Retrieved on 13 Feb 2020 from https://www.kkmm.gov.my/en/public/news/16471-bernama-11-feb-2020-gov-t-actively-addressing-cyber-threats-crimes-dpm

Boyatzis, R. E. (2011). Managerial and leadership competencies: a behavioral approach to emotional, social and cognitive intelligence. *The Journal of Business Perspective*, 15(2), 91-100.

Bratton, J. and Gold, J. (2012). Human Resource Management. Theory and Practice, 5th ed., Palgrave McMillan, New York, NY.

Cain, A., Edwards, M. E. & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications*, 42, 36-45.

Corallo, A., Lazoi, M. & Lezzi, M. (2020). Cybersecurity in the context of Industry 4.0: A structured classification of critical assets and business impacts. *Computers in Industry*, 114, 1-15.

Cleveland, M. & Cleveland, S. (2018). Building Engaged Communities—A Collaborative Leadership Approach. Smart Cities, 1, 155-162.

CyberSecurity Malaysia (2019). E-Security: The first line of digital defense begins with knowledge. CyberSecuirty Malaysia, 46 (1), 1-44. Retrieved on 24 January 2020 from https://www.cybersecurity.my/data/content_files/12/1971.pdf

da Veiga, A., Astakhova, L. V., Botha, A. & Herselman, M. (2020). Defining organizational information security culture – Perspectives from academia and industry. Computers & Security, 92, 1-23.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasure and its impact on information systems misuse: a deterrence approach. *Information Systems Research*, 20(1), 79-98.

Donalds, C. & Osei-Bryson, K-M. (2020). Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents. *International Journal of Information Management*, 51, 1-16.

Gefen, D., Rigdon, E. E. & Straub, D. W. (2011). Editor's Comment: An Update and Extension to SEM Guidelines for Administrative and Social Science Research. MIS Quarterly, 35(2), iii-xiv.

Gold, A. H., Malhotra, A. & Segars, A. H. (2001). Knowledge management: an organizational capabilities perspective. *Journal of Management Information Systems*, 18(1), 185–214.

Hadlington, Lee, & Murphy. (2018). Is media multitasking good for cybersecurity? Exploring the relationship between media multitasking and everyday cognitive failures on self-reported risky cybersecurity behaviors. Cyberpsychology, Behavior, and Social Networking, 21(3), 168-172.

Hair, F. J., Sarstedt, J. 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.

Haqaf, H. & Koyuncu, M. (2018). Understanding key skills for information security managers. *International Journal of Information Management*, 43, 165-172.

Hasan, S., Ali, M., Kurnia, S. & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications*, 58, 1-16.

Hassan, N. (Mar 8, 2022), 8 leadership skills every cybersecurity professional must have, Cybrary. https://www.cybrary.it/blog/8-leadership-skills-every-cybersecurity-professional-must-have/x

Henseler, J., Ringle, C. & Sarstedt, M. (2015). A New Criterion for Assessing Discriminant Validity in Variance-based Structural Equation Modeling. *Journal of the Academy of Marketing Science*, 43, 115-135.

Hina, S., Selvam, D. D. D. P. & Lowry, P. B. (2019). Institutional governance and protection motivation: Theoretical insights into shaping employees' security compliance behavior in higher education institutions in the developing world. Computers & Security, 87, 1-15.

Hong, Y. & Furnell, S. (2021). Understanding cybersecurity behavioral habits: Insights from situational support. Journal of Information Security and Applications, 57, 1-9.

Humaidi, N. & Balakrishnan, V. (2018). Indirect effect of management support on users' compliance behavior towards information security policies. Health Information Management Journal, 47(1), 17-27.

Hwang, I., Wakefield R., Kim, S. & Kim, T. (2019). Security Awareness: The First Step in Information Security Compliance Behavior. Journal of Computer Information System, 61(4), 345-356.

Jeong, M. & Zo, H. (2021). Preventing insider threats to enhance organizational security: The role of opportunity-reducing techniques. Telematics and Informatics, 63, 1-17.

Keers, R. N., Williams, S. D., Cooke, J., & Ashcroft, D. M. (2013). Causes of Medication Administration Errors in Hospitals: a Systematic Review of Quantitative and Qualitative Evidence. Drug Safety, 36 (11), 1045-1067.

Kemper, G. C. (2019). Improving employees' cyber security awareness. Computer Fraud & Security, 2019(8), 11-14.

Khando, K., Gao, S., Islam, S. M. & Salman, A. (2021). Enhancing employees' information security awareness in private and public organizations: A systematic literature review. Computers & Security, 106, 1-22.

Kim, H.L., Hovav, A. & Han, J. (2020). Protecting intellectual property from insider threats: A management information security intelligence perspective. Journal of Intellectual Capital, 21(2), 181-202.

Kimani, K., Oduol, V. & Langat, K. (2019). Cyber security challenges for IoT-based smart grid networks. International Journal of Critical Infrastructure Protection, 25, 36-49.

Korzynski, P., Kozminski, A.K., Baczynska, A. & Haenlein, M. (2021). Bounded leadership: an empirical study of leadership competencies, constraints, and effectiveness. European Management Journal, 39(2), 226-235.

Koskosas, I., Kakulidis, K., & Siomos, C. (2011). Examining the linkage between information security and end-user trust. International Journal of Computer Science & Information Security, 9(2), 21-31.

Kreicberge, L. (2010). Internal threat to information security - countermeasures and human factor with SME. Unpublished Master, University of Technology.

Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. Business Horizons, https://doi.org/10.1016/j.bushor.2021.02.022

Li, L., He, W., Xu, L., Ash, I., Mohd Anwar & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. International Journal of Information Management, 45, 13-24.

McFadden, M. L. (2021). Cybersecurity experiential leadership learning (Doctoral dissertation, Northeastern University).

Mousavi, R., Chen, R., Kim, D. J. & Chen, K. (2020). Effectiveness of privacy assurance mechanisms in users' privacy protection on social networking sites from the perspective of protection motivation theory. Decision Support Systems, 135, 113323. https://doi.org/10.1016/j.dss.2020.113323.

Newman, L. H. (2019). The Biggest Cybersecurity Crises of 2019 So Far: Ransomware attacks, supply chain hacks, escalating tensions with Iran—the first six months of 2019 have been anything but boring. Retrieved on 24 January 2020 from https://www.wired.com/story/biggest-cybersecurity-crises-2019-so-far/

Northouse, P.G. (2010), Leadership: Theory and Practice, 5th ed., Sage, London.

Pang, M-S. & Tanriverdi, H. (2022). Strategic roles of IT modernization and cloud migration in reducing cybersecurity risks of organizations: The case of U.S. federal government. The Journal of Strategic Information Systems, 31(1), 1-19.

Park, S., Ruighaver, A. B., & Ahamad, A. (2010). Factors influencing the implementation of information systems security strategies in organization. Paper presented at the International Conference on Information Sciences and Application.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security*, 42 (0), 165-176.

Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y. & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology,* 88, 879-903.

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. *MIS Quarterly*, 34(4), 757-778.

Ringle, C. M., Wende, S., & Becker, J.-M. 2015. "SmartPLS 3." Boenningstedt: SmartPLS GmbH, http://www.smartpls.com.

Rönkkö, M. & Ylitalo, J. (2010). Construct Validity in Partial Least Squares Path Modeling. ICIS 2010 Proceedings. Paper 155. Retrieved from http://aisel.aisnet.org/icis2010_submissions/155.

Rowley, D.J. and Sherman, H. (2003). The special challenges of academic leadership. *Management Decision*, 41(10), 1058-1063.

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behavior formation in organizations. *Computers & Security*, 53, 65-78.

Safa, N., Maple, C. Furnell, S., Azad, M., Perera, C., Dabbagh, M. & Sookhak, M (2019). Deterrence and prevention-based model to mitigate information security insider threats in organizations. *Future Generation Computer Systems*, 97, 587-597.

Schuetz, S. W., Lowry, P. B., Pienta, D. A. & Thatcher, J. B. (2020). The Effectiveness of Abstract Versus Concrete Fear Appeals in Information Security. *Journal of Management Information Systems*, 37(3), 723-757.

Shaikh, F. A. & Siponen, M. (2023). Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity. Computers & Security, 124, 102974.

Sussman, L. L. (2021). Exploring the value of non-technical knowledge, skills, and abilities (KSAS) to cybersecurity hiring managers. Journal of Higher Education Theory & Practice, 21(6).

TheStar.com (2021). Maybank warns of new fake banking website created to steal customer details. Retrieved on April 15, 2021, from https://www.thestar.com.my/tech/tech-news/2021/04/14/maybank-warns-of-new-fake-banking-website-created-to-steal-customer-details

Torten, Reaiche, Boyle. (2018). The impact of security awareness on information technology professionals' behavior. Computers & Security, 79, 68-79.

Triplett, W. (2022). Addressing Human Factors in Cybersecurity Leadership. Journal of Cybersecurity and Privacy, 2, 573-586.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information & Management*, 49(3–4), 190-198.

Whitman, M. E. & Mattord, H. J. (2019). Management of Information Security, 6th Edition. Stamford, CT: Cengage Learning.

Whitman, M. E. (2004). In defense of the realm: understanding the threats to information security. *International Journal of Information Management*, 24(1), 43-57.

Willison, R. & Warkentin, M. (2013). Beyond Deterrence: An Expanded View of Employee Computer Abuse. *MIS Quarterly*, 37(1), 1-20.

Wong, L-W., Lee, V-H., Tan, G. W-H., Ooi, K-B. & Sohal, A. (2022). The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities. *International Journal of Information Management*, 66, 1-15.

Yeoh, W., Wang, S., Popoviˇc, A. & Chowdhury, N. H. (2022). A systematic synthesis of critical success factors for cybersecurity. *Computers & Security*, 118, 1-17.

Yukl, G. (2006), Leadership in Organizations, 6th ed., Pearson-Prentice Hall, Upper Saddle River, NJ.

Zimba, A., Wang, Z. & Chen, H. (2018). Multi-stage crypto ransomware attacks: A new emerging cyber threat to critical infrastructure and industrial control systems. *ICT Express*, 4(1), 14-18.