Jurnal Impresi Indonesia (JII)
p-ISSN: 2828-1284 e-ISSN: 2810-062x
website: https://rivierapublishing.id/JII/index.php/jii/index

The Influence of Cybersecurity Protection Behavior: Employees of Big Four Account Firm Companies

Hasnul Qalby, Gunawan Yudi Hariyanto, Dyan Tri Utomo, Rano Kartono Rahim
Management Department, Bina Nusantara University, Indonesia
Email: hasnul.qalby@binus.ac.id, gunawan.hariyanto@binus.ac.id,
dyan.utomo@binus.ac.id, rano.kartono@binus.edu

Keywords
Cybersecurity Knowledge; Cybersecurity Awareness; Sel-Efficacy; Cybersecurity Protection Behavior; Protection Motivation Theory; Accounting Firms

Abstract
This study aims to determine the influence effect of cybersecurity protection behavior from the perspective of employees of Big Four Account Firm Companies. The method used in this research is a quantitative method. The subjects in this study were employees of the Big Four Account Firm with a sample of 150 taken using purposive sampling method. The analysis used in this study was a structural approach to the Equation Model (SEM) by using smart PLS. The results show that Cybersecurity Knowledge has a significant effect towards Self-Efficacy, Cybersecurity Awareness has a significant effect towards Self-Efficacy, and Self-Efficacy has a significant effect towards Cybersecurity Protection Behavior. The managerial implication of this research is important for the organization or management to raise awareness of security culture and can be the reference for other accounting firms.

INTRODUCTION

Accounting firms are tasked with the management of sensitive financial records, tax data, and confidential client information, making them prime targets for cyber threats. Public accountants handle substantial amounts of financial data and private client details, which is why both accounting firms and the accounting divisions within organizations are appealing targets for cybercriminals, even for Big 4 Accounting Firms. This highlights the importance of cybersecurity in defending against internal threats. Insider threats, whether due to malicious intent or unintentional actions, can significantly jeopardize financial data. Effective cybersecurity strategies, including comprehensive employee training, rigorous access controls, and frequent audits, are essential for minimizing risks and securing financial data from internal violations (Kankahalli et al, 2003; Hussain et al, 2024). As Indonesia Government release the Personal Data Protection (PDP) Law by 17th October 2022, the law is enforcing every company to sets out what should be done to make sure everyone's data is used properly and fairly. It is like regulations such as the General Data Protection Regulation (GDPR), the Sarbanes-Oxley Act (SOX), and the Gramm-Leach-Bliley Act (GLBA), the organizations are required to implement strong cybersecurity frameworks to protect privacy and financial information while ensuring its integrity and confidentiality (Hossain & Zohora, 2024).

Despite concerns raised by regulators regarding cybersecurity risks, auditors are not required by regulations to address such risks. In the absence of mandatory requirements,

auditors may be hesitant to address cybersecurity risks beyond those that impact financial statements, as this could result in potential liabilities and costs that are challenging to recuperate (Li et al, 2020). Over the past few years, the protection of personal data has emerged as a critical issue, driven by the elevated risk of data leakage during its storage, transmission, and application, which has sparked considerable public concern regarding data security and privacy (Zhang et al, 2021). While the media often focus on damage caused by hacker attacks, it is important to recognize that there are various other types of cyber-security incidents (Rosati & Gogolin, 2019). Cyber-security incidents manifest in different forms, comprising malware infections, ransomware attacks, denial-of-service incidents, card payment fraud, malicious insiders, or even human errors.

According to research conducted by (Zwilling et al, 2020) there is a strong correlation between higher cyber knowledge and cyber awareness, regardless of gender or country of the respondent. The study found that the level of awareness was directly linked to the use of protection methods and measures to safeguard devices. It was concluded that the level of awareness, rather than the amount of device usage, determined the likelihood of a cyber-attack. A study case that held by (McCormac et al, 2018) stated that there's a connection between employee's perspective and Information Security Awareness. Greater resilience demonstrated higher levels of Cybersecurity Awareness, whereas those who experienced higher levels of job stress exhibited lower levels of Cybersecurity Awareness. Furthermore, individuals with higher resilience reported lower levels of job stress, and resilience was identified as a mediator in the connection between job stress and Cybersecurity Awareness. These results suggest that individuals who possess effective stress management and adaptability skills (i.e., higher resilience) are less likely to have their Cybersecurity Awareness affected, even in the presence of significant job stress. Although academics and practitioners have acknowledged the importance of individuals in achieving security, they have also identified them as the weakest link in the security chain due to their non-compliance with security best practices (Boss et al, 2009).

Based on the above discussions, research questions for this article would be:

1. Does Cybersecurity Knowledge have a direct effect on Self-Efficacy?
2. Does Cybersecurity Knowledge significantly influence Cybersecurity Protection Behavior?
3. Does Cybersecurity Awareness have a direct effect on Self-Efficacy?
4. Does Cybersecurity Awareness significantly influence Cybersecurity Protection Behavior?
5. Is there a significant direct effect of Self-Efficacy on Cybersecurity Protection Behavior?
6. Does Self-Efficacy mediate the relationship between Cybersecurity Knowledge and Cybersecurity Protection Behavior?
7. Does Self-Efficacy have a mediating effect on the relationship between Cybersecurity Awareness and Cybersecurity Protection Behavior?

This study aims to determine the influence effect of cybersecurity protection behavior from the perspective of employees of Big Four Account Firm Companies based on the use case of Protection Motivation Theory (PMT) in cybersecurity behavioral research. While many studies have applied the Theory of Planned Behavior (TPB) to analyze cybersecurity behaviors, it mainly highlights behavioral intentions rather than the actual protective actions taken by individuals. PMT theory has been used in cybersecurity behavior research, such as

research by (Warkentin et al, 2011) related to behavior intention that comply with information privacy policies and by (Boehmer et al, 2015) for research how protective behavior applied in online safety behavior. The broad application of the protection motivation theory lies in its ability to analyze employees' perceptions of cybersecurity threats and their adaptive responses from different viewpoints. Focusing on cybersecurity knowledge and awareness contributes to the cybersecurity literature by promoting protection behavior and highlighting the importance of self-efficacy in accounting firms.

The foundation of enhancing protective behavior within organizations, especially in accounting firms, lies in cybersecurity knowledge and awareness. Wang et al, (2019) assert that cybersecurity knowledge management is characterized by the ongoing acquisition and utilization of intellectual resources to foster organizational value. However, there exists a considerable difference in knowledge levels between IT and non-IT personnel. Abawajy et al. (2014) emphasized that even a basic level of awareness does not automatically equate to actionable knowledge that can effectively mitigate risks. For non-IT staff, particularly those in accounting, it is crucial to comprehend cybersecurity concepts that are relevant to their specific roles. Training programs that blend theoretical and practical components (Herath et al., 2009) can empower employees to act decisively. Gist et al, (1987) identified self-efficacy as a strong predictor of performance, and procedural knowledge has been shown to enhance it (Arachchilage & Love, 2014). However, informal or unstructured knowledge may hinder this effect (Raineri & Fudge, 2019). Consequently, structured training not only improves understanding of cybersecurity but also fosters self-efficacy, which is essential for maintaining consistent protective behavior.

Knowledge provides the "what" while awareness explains the "why," but it is self-efficacy that influences "how" confidently individuals act on this information. According to Shaw et al. (2009), cybersecurity awareness is defined as the understanding users have of their responsibilities and the actions, they undertake to secure organizational systems. The spectrum of awareness—from low to high—reflects the level of appropriate behavioral response (Klein et al, 2022). Research by Hanus & Wu (2016) and Torten et al, (2018) indicates that awareness training can significantly improve both self-efficacy and protective behavior. When individuals are armed with the necessary knowledge and skills, their confidence in addressing cyber threats is enhanced (Shillair et al., 2022; Taherdoost, 2024). Additionally, the tendency to share cybersecurity awareness is closely associated with one's self-efficacy level (Shaari & Rahman, 2014), highlighting the necessity for organizational strategies that cultivate this psychological resource. Thus, fostering self-efficacy serves as a link between knowledge, awareness, and the practical application of protective behavior, establishing it as a crucial factor in enhancing cybersecurity posture, particularly in high-risk, data-sensitive fields such as accounting firms.

RESEARCH METHODS

Elements of Research Design

For this research the quantitative methods will be used with a research strategy using survey research. The topic of focus should be narrowed to focus on the specific research question that a study can answer (Neuman et al, 2014). The minimal interference is used so that the results are maintained without any manipulation to know the behavior of the employees. It was not created as a study setting to ascertain the real situation of how cyber

security policies apply to employees of Big 4 Accounting Firms in Indonesia. The unit of analysis for this research is the population of employees of the Big 4 Accounting Firms in Indonesia, while the samples that determined are individuals from companies included in the Big 4 Audit Firms, most of whom carry out their daily activities using endpoint devices such as PCs or laptops. The online survey was conducted for IT-related. The time horizon for this research was cross-sectional, by using the sample of Audit Firm employees at one point in time due to the researcher's limited time.

Proposed Sampling Method/Procedure and Sample Size

The relevant minimum for target population is 100 Indonesian Big 4 Account Firm employees to investigate the behavior of Indonesian employees. The sampling frame are the employees who work using endpoint devices (PC/laptop). Rule of thumb method is used for sample size for survey research based on the specified level of confidence, according to (Hair et al, 2019) that the minimum number of individuals for the recommendation of sample observations to variables is a ratio of 4:1. Purposive Sampling is a method for selecting a sample of 150 Big 4 Firm employees who work using endpoint devices. This method provides the flexibility to balance the sample based on characteristics that may be relevant to the research, ensuring diversity and a comprehensive understanding of the cybersecurity behavior of Big 4 Account Firm employees in Indonesia who use endpoint devices.

Data Collection Methods and Data Collection Techniques

The sampling technique in the non-probability sampling category used in this study by using the questionnaire of online basis. Non-probability sampling was chosen to obtain data quickly and efficiently because data can be obtained from individuals in the population whose criteria the researcher has determined and when the total number of respondents needed has been met, data collection can be stopped (Sekaran, U. & Bougie, R., 2019). The non-probability sampling technique in this study uses purposive sampling with the judgment sampling type because the sampling taken is limited to certain individuals who can provide information according to the desired criteria set by the researcher (Sekaran, U. & Bougie, R., 2019). The sampling design in judgment sampling requires specific information input on very important research topic areas, where other sampling designs will not offer the opportunity to obtain specific information. Therefore, the researcher held discussions with the employees of Big 4 Accounting Firms and Indonesian Institute of Public Accountants in determining the number of samples taken so that it was decided to take samples of 150 employees who could specifically meet the criteria of the researcher. Using Likert Scale by 5 points of scales (from 1 as very unaware to 5 as very aware).

Proposed Data Analysis

In this study, we use regression analysis to find the correlation between dependent and independent variables. For models that are complex in nature, PLS-SEM is a viable option that doesn't have as many constraints on data distribution and sample size (Lowry et al, 2014) (Vinzi et al, 2009) using Smart PLS software. By analysis with PLS, assessing the outer model or measurement model should be done (Hair et al, 2020). The evaluation of the outer model is based on three key criteria: Convergent Validity, Discriminant Validity, and Composite Reliability. Convergent validity for measurement models featuring indicator reflection is assessed by investigating the correlation between the scores of the items and the component scores calculated using Partial Least Squares (PLS) techniques. An individual reflection is classified as large if its correlation with the measured construct is greater than 0.70. Discriminant validity for measurement models that employ reflective indicators is determined by examining the cross-loadings associated with each construct and using Fornel-

Larcker criterion. If the correlation between the construct and its measurement item is greater than that of other constructs, it implies that the latent construct is a superior predictor of its block's size in comparison to the sizes of other block. A different technique for measuring discriminant validity is to analyze the root of the average variance extracted (AVE) for each construct in relation to its correlation with other constructs present in the model. A construct demonstrates good Discriminant Validity if its AVE is greater than the correlation values with other constructs in the model, and the value should be greater than 0.5 value.
Based on the data analysis, questions will be prepared for the sample as follows:

Table 1. Questionnaire List

Construct	Code	Questions	Source
Cybersecurity Knowledge (CK)	CK1	I'm familiar with cybers security through internet?	Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2020). Cyber security awareness, knowledge, and behavior: A comparative study. Journal of Computer Information Systems, 62(1), 82-97. https://doi.org/10.1080/08874417.2020.1712269
	CK2	I attend many of IT security training in the past	
	CK3	I know about the cybersecurity risks in my workplace	Gerdenitsch, C., Wurhofer, D., & Tscheligi, M. (2023). Working conditions and cybersecurity: Time pressure, autonomy and threat appraisal shaping employees' security behavior. Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 17(4). https://doi.org/10.5817/cp2023-4-7
	CK4	I know how to work cybersecurity aware	
	CK5	I know about how to avoid cybersecurity risks in my workplace	
Cybersecurity Awareness (CA)	CA1	I realized how acceptable it is to use IT products and services described in company policies	Grassegger, T., & Nedbal, D. (2021). The role of employees' information security awareness on the intention to resist social engineering. Procedia Computer Science, 181, 59-66. https://doi.org/10.1016/j.procs.2021.01.103
	CA2	I am aware of how the installation of software is regulated in our policies	Grassegger, T., & Nedbal, D. (2021). The role of employees' information security awareness on the intention to resist social engineering. Procedia Computer Science, 181, 59-66. https://doi.org/10.1016/j.procs.2021.01.103
	CA3	I know how our policies govern the management of sensitive and confidential information	
	CA4	I am aware of the potential threats and negative consequences that inadequate information security can cause in my work	
	CA5	I understand the risks that inadequate information poses to security in general	
	CA6	I am aware of my obligations under our policy regarding the use and management of passwords for my work computer	
Self-Efficacy (SE)	SE1	I feel confident in setting the Web browser to different security levels	Li, L., Xu, L., & He, W. (2022). The effects of antecedents and mediating factors on cybersecurity protection behavior. Computers in Human Behavior Reports, 5, 100165. https://doi.org/10.1016/j.chbr.2021.100165
	SE2	I feel confident in handling virus-infected files	
	SE3	I feel confident in getting rid of spyware and malware from my computer	
	SE4	I would be able to follow most of	Herath, T., & Rao, H. R. (2009). Protection

		the IS security policies even if there was no one around to help me	motivation and deterrence: A framework for security policy compliance in organizations. European Journal of Information Systems, 18(2), 106-125. https://doi.org/10.1057/ejis.2009.6
	SE5	I would feel comfortable following most of the Information security policies on my own.	
Cybersecurity Protection Behavior (CP)	CP1	I aim to continue to comply with the Company's cybersecurity rules	Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Computers & Security, 31(1), 83-95. https://doi.org/10.1016/j.cose.2011.10.007
	CP2	I am confident that I will comply with the Company's cybersecurity rules	
	CP3	It is possible that I will comply with corporate cybersecurity with the aim of protecting the Company's information systems	
	CP4	I tend to follow the company's cybersecurity rules in the future	
	CP5	I will follow company cybersecurity policies whenever possible	

RESULTS AND DISCUSSION

The number of respondents who participated filling out the questionnaire for this research total of 150 respondents, and sorted based on category of Big 4 Accounting Firms. With the 21 statements of descriptive statistics, five statements regarding Cybersecurity Knowledge, six statements regarding Cybersecurity Awareness, five statements regarding Self-Efficacy, and five statements regarding Cybersecurity Protection Behavior.

From the Table 1 reveals the demographic information for the responders of gender were women 64.67 per cent and men by 35.33 per cent. The age percentage for under 25 by 40.67 per cent, between 25 until 34 are 42.47 per cent, and more than 34 are 16.67 per cent. Job position at junior staff by 49.33 per cent, senior staff by 37.33 per cent, supervisor by 10.67 per cent, and manager by 2.67 per cent. Working experience with less than 1 year by 19.33 per cent, between 1 – 3 years by 26.00 per cent, and more than 3 years by 54.67 per cent. For the education level based on the latest, bachelor's degree by 84.67 per cent, and master's degree by 15.33 per cent. Based on the working location of the employee, most employees that work in the office by 25.33 per cent, and the other employees that spend their working time outside the office by 74.67 per cent. Based on the involvement of the employees that join the security training program from their company, the employees that joined the session by 87.33 per cent, and the other employees by 12.67 per cent that did not join the session.

Table 2. Demographic Information

Information	Frequency (N = 150)	Percent (%)
Gender		
Man	97	64.67
Woman	53	35.33
Age		
Under 25	61	40.67
Between 25 – 34	64	42.67
More than 34	25	16.67
Job Position		
Junior Staff	74	49.33
Senior Staff	56	37.33

Supervisor	16	10.67
Manager	4	2.67
Working Experience		
Less than 1 Year	29	19.33
Between 1 – 3 Years	39	26.00
More than 3 Years	82	54.67
Latest Education		
Bachelor's degree	127	84.67
Master's degree	23	15.33
Most Frequent of Working Location		
In the Office	38	25.33
Outside of the Office	112	74.67
Involvement in Security Training		
Joined the session	131	87.33
Not yet join the session	19	12.67

Outer Model Results

The analysis of data using SmartPLS software involves evaluating the outer model through three distinct methods: Convergent Validity, Average Variance Extracted (AVE)., Discriminant Validity, and Composite Reliability.

Convergent Validity

Convergent validity is a measurement concept that involves two instruments (variables and indicators) that need to be valid and aligned with each other. The function of outer loading is to evaluate the strength of the relationship between the latent variables and the indicators being analyzed. To ensure data validity, an outer loading value greater than 0.7 is required. Based on the table below, the results of outer loadings are > 0.7. The outer loading result is shown in Table 3.

Table 3. Outer Loadings

Variable	Indicator	Outer loadings
Cybersecurity Awareness	CA1	0,907
	CA2	0,903
	CA3	0,785
	CA4	0,921
	CA5	0,795
	CA6	0,909
Cybersecurity Knowledge	CK1	0,899
	CK2	0,937
	CK3	0,821
	CK4	0,903
	CK5	0,899
Cybersecurity Protection Behavior	CP1	0,938
	CP2	0,772
	CP3	0,942
	CP4	0,798
	CP5	0,898
Self-Efficacy	SE1	0,899
	SE2	0,802

	SE3	0,942
	SE4	0,750
	SE5	0,890

Source: Data processed (2025)

Composite Reliability and Average Variance Extracted (AVE)

Composite reliability evaluates the consistency and interrelatedness of constructs, requiring a value above 0.7 to be classified as reliable. Concurrently, Cronbach's alpha should also surpass 0.7 to be considered an acceptable standard as per research criteria. Average variance extracted (AVE) is a measure of the total variance explained by various indicators linked to a latent construct. It indicates a more favorable comparison of success against error variance, with a minimum value of 0.5 recommended as a standard for convergent validity. This means that the variation of a latent variable is considered successful if it accounts for at least 50% of the variance in the indicators assessed.

Table 4. Construct Reliability and Average Variance Extracted

Variable	Cronbach's Alpha	Composite Reliability (rho_a)	Average Variance Extracted (AVE)
Cybersecurity Awareness	0.936	0.942	0.760
Cybersecurity Knowledge	0.936	0.944	0.796
Cybersecurity Protection Behavior	0.920	0.933	0.761
Self-Efficacy	0.910	0.923	0.739

Source: Data processed (2025)

Based on the table above, the results of the analysis show that all constructs have Cronbach's alpha and composite reliability (rho_a) values greater than 0.7, and the constructs meet the reliable criteria and indicate AVE are above 0.5.

Analysis Discriminant Validity

Discriminant validity is a critical measure that stipulates that a variable should not correlate with other variables that are theoretically examined, with the purpose of differentiating various concepts, by using Fornell Larcker criterion and finding the cross loading. The Fornell-Larcker criterion indicates that discriminant validity is satisfactory if the square root of the Average Variance Extracted (AVE) for a given construct is greater than its correlation with other latent constructs. Analyzing the cross-loading values for each variable reveals that the indicator values for each construct are greater than those of the indicators in other constructs. A correlation coefficient between constructs should remain below 0.9; exceeding this threshold could suggest multicollinearity issues between the constructs.

Table 5. Fornell Larcker Criterion

	Cybersecurity Awareness	Cybersecurity Knowledge	Cybersecurity Protection Behavior	Self-Efficacy
Cybersecurity Awareness	0,872			
Cybersecurity Knowledge	0,709	0,892		
Cybersecurity Protection Behavior	0,721	0,672	0,872	

Self-Efficacy	0,692	0,667	0,756	0,859

Source: Data processed (2025)

The results displayed in the table above regarding the discriminant validity test demonstrate that every construct has a square root of the Average Variance Extracted (AVE) that surpasses the correlation values with other constructs. Thus, it is evident that all constructs assessed meet the requisite standards for discriminant validity.

Table 6. Cross Loadings

Indicators	Cybersecurity Awareness	Cybersecurity Knowledge	Cybersecurity Protection Behavior	Self-Efficacy
CA1	0,907	0,651	0,668	0,623
CA2	0,903	0,640	0,658	0,679
CA3	0,785	0,503	0,526	0,550
CA4	0,921	0,697	0,653	0,636
CA5	0,795	0,567	0,567	0,515
CA6	0,909	0,636	0,681	0,602
CK1	0,676	0,899	0,665	0,666
CK2	0,696	0,937	0,678	0,636
CK3	0,529	0,821	0,550	0,477
CK4	0,635	0,903	0,558	0,555
CK5	0,610	0,899	0,530	0,617
CP1	0,669	0,628	0,938	0,716
CP2	0,523	0,466	0,772	0,579
CP3	0,717	0,644	0,942	0,748
CP4	0,568	0,492	0,798	0,555
CP5	0,646	0,676	0,898	0,675
SE1	0,561	0,579	0,638	0,899
SE2	0,525	0,457	0,650	0,802
SE3	0,664	0,636	0,743	0,942
SE4	0,486	0,517	0,500	0,750
SE5	0,706	0,655	0,690	0,890

Source: Data Processed (2025)

The table of cross loadings presented above indicates that there is no multicollinearity among the variables, as each construct measures distinct aspects and the values are below 0.9.

Inner Model Results

The analysis of data using SmartPLS software involves evaluating the inner model through the R-square value. This analysis is performed to evaluate how significantly the independent variable can impact the dependent variable. The R-squared value, which spans from 0 to 1, implies that a value nearer to 1 denotes a more pronounced influence, while a value closer to 0 indicates a lesser effect.

Table 7. R Square Values

	R-square
Cybersecurity Protection Behavior	0.659
Self-Efficacy	0.541

Source: Data processed (2025)

The data presented in Table 5 indicates a relationship between the dependent and independent variables, as reflected in the R-square value for Cybersecurity Protection Behavior (CP). This behavior is shaped by Cybersecurity Knowledge (CK), Self-Efficacy (SE), and Cybersecurity Awareness (CA), which collectively account for 65.9% (0.659) of the variance, leaving 34.1% influenced by other variables that were not analyzed. For Self-Efficacy (SE), the influence of Cybersecurity Knowledge (CK) and Cybersecurity Awareness (CA) is noted at 54.1% (0.541), while 45.9% is attributed to other unstudied variables.

Hypothesis Test

From the SmartPLS software, to ensure that model has no abnormalities, researchers did the bootstrapping and analysis as follows:

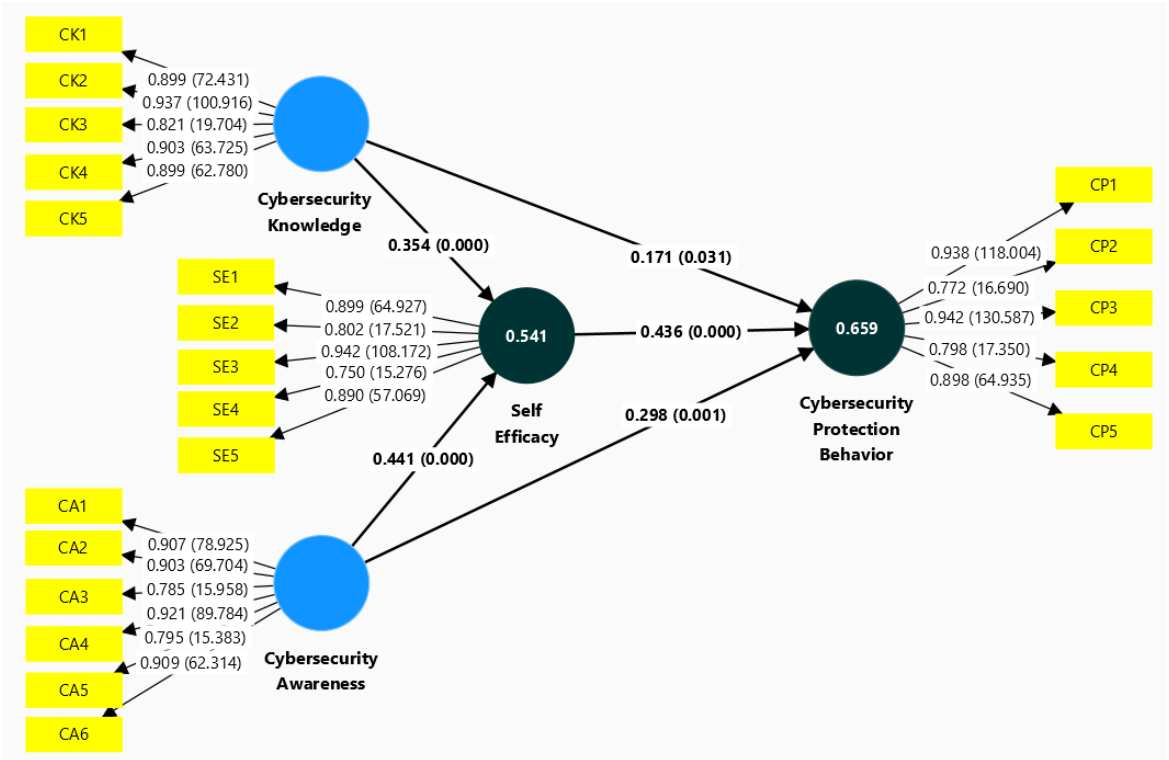

Diagram 2. SEM Model

The purpose of bootstrapping testing is to reduce the issues associated with irregularities in research data**.** In hypothesis testing, the level of significance is assessed through the value of the path coefficient parameters. This examination focuses on the estimated path coefficient and the t-statistic value, assessing significance at a level of α=5%. If the t-statistic value is higher than the t-table value of 1.96 for two tailed test, then the hypothesis is accepted. As for the following are the values path coefficient in testing the main hypothesis of the study for direct effects and indirect effects:

Table 8. Path Coefficient

Correlation	Original Sample	Sample Mean (M)	Standard Deviation	T-Statistics	P Values	Results
CA → CP	0.298	0.296	0.086	3.468	0.001	Accepted
CA → SE	0.441	0.443	0.068	6.524	0.000	Accepted
CK → CP	0.171	0.170	0.079	2.161	0.031	Accepted
CK → SE	0.354	0.353	0.068	5.223	0.000	Accepted
SE → CP	0.436	0.439	0.069	6.330	0.000	Accepted
CA → SE → CP	0.192	0.195	0.045	4.288	0.000	Accepted
CK → SE → CP	0.154	0.154	0.036	4.255	0.000	Accepted

Source: Data Processed (2025)

For the Cybersecurity Awareness (CA) towards Cybersecurity Protection Behavior (CP) has the significant effect with the p value 0.001 < 0.05 and t statistic 3.468 > 1.96 and positive path coefficient of 0.298. With the direction of this positive influence indicates that the higher the CA, the higher the CP, conversely the lower the CA, the lower the CP. CA in this study is proven to be a factor that has a significant impact on CP, so that efforts to increase CP can be made from increasing CA. The results for Cybersecurity Awareness (CA) on Self Efficacy (SE) are significant with a p value of 0.000 < 0.05, t statistic 6.524 > 1.86 and the positive path coefficient of 0.441. With the direction of this positive influence indicates that the higher the CA, the higher the SE and conversely the lower the CA, the lower the SE. CA in this study is proven to be a factor that has a significant impact on SE, so that efforts to increase SE can be made from increasing CA.

For the Cybersecurity Knowledge (CK) towards Cybersecurity Protection Behavior (CP) has the significant effect with the p value 0.031 < 0.05 and t statistic 2.161 > 1.96 and positive path coefficient of 0.171. With the direction of this positive influence indicates that the higher the CK, the higher the CP, conversely the lower the CK, the lower the CP. CK in this study is proven to be a factor that has a significant impact on CP, so that the efforts to increase CP can be made from increasing CK. The results for Cybersecurity Knowledge (CK) on Self Efficacy (SE) are significant with a p value 0.000 < 0.05, t statistic 5.223 > 1.96 and a positive path coefficient of 0.354. The direction of this positive influence shows that the higher the CK, the higher the SE, conversely the lower the CK, the lower the. CK in this study is proven to be a factor that has a significant impact on SE, so that efforts to increase SE can be made by increasing CK.

The results for the analysis show that the influence of Self Efficacy (SE) on Cybersecurity Protection Behavior (CP) is significant with a p value of 0.000 < 0.05, t statistic 6.330 > 1.96 and a positive path coefficient of 0.436. The direction of this positive influence indicates that the higher the SE, the higher the CP, conversely the lower the SE, the lower the CP. SE in this study is proven to be a factor that has a significant impact on CP, so that efforts to increase CP can be made from increasing SE.

For the indirect effects result test of Cybersecurity Awareness (CA) on Cybersecurity Protection Behavior (CP) through Self Efficacy (SE) showed a significance of 0.000 with a path coefficient of 0.192. Therefore, the p value obtained < 0.05, it is concluded that SE is proven to mediate the influence of CA on CP. An increase in CA will have an impact on an increase in SE which will then have an impact on an increase in CP. As for the indirect effects result test of Cybersecurity Knowledge (CK) on Cybersecurity Protection Behavior (CP) through Self Efficacy (SE) showed a significance of 0.000 with a path coefficient of 0.154. Therefore, the p value obtained < 0.05, it is concluded that SE is proven to be able to mediate

the influence of CK on CP. An increase in CK will have an impact on an increase in SE which will then have an impact on an increase in CP.

Discussion

The first hypothesis H1 was carried out with the aim of testing the effect of Cybersecurity Knowledge on Self Efficacy with the results of positive significant effect. These results aligned with previous research. This finding is aligned with (De Kimpe et al, 2021) that by having the cybersecurity knowledge, the employee that has more information and is well informed is more likely to counter the threats effectively. It is aligned with the research by (Li et al, 2016) that peer behavior and employees own action experiences of cybersecurity are the important factors for improving the coping appraisal process for improving cybersecurity in organizations. The characteristics of respondents indicate that individuals possessing over one year of work experience are likely to face a greater number of cybersecurity-related situations, thereby augmenting their knowledge and boosting their confidence in managing threats. Moreover, the perspective of all position levels, along with the minimum requirement of a bachelor's degree, enhances the ability to effectively process and implement cybersecurity principles. This evidence emphasizes the necessity of specialized training and the sharing of knowledge across different roles and experience levels to nurture a strong sense of cybersecurity self-efficacy throughout the organization.

The second hypothesis H2 for the relationship between Cybersecurity Knowledge and Cybersecurity Protection Behavior has the positive significant result. This finding is related to the research by (Gerdenitsch & Wurhofer, 2023) that individuals with limited understanding who perceive an attack as having a significant impact may experience fear or hesitation in addressing the issue. On the other hand, this finding is aligned with (Khan et al, 2023) that knowledge that obtained through training can lead to enhance the behavioral intentions to engage in protective cybersecurity practices. From the characteristc respondent shown that high proportion of respondents for the involvement in Security Training involvement in Security Training not only contributed to their understanding of cybersecurity but also fostered stronger protective actions such as vigilant email handling, maintaining password hygiene, and following organizational guidelines. Individuals with extensive work experience are likely to have gained practical knowledge in cybersecurity throughout their careers. Their encounters with previous incidents or modifications in company policies may enhance their ability to make informed decisions and exhibit more robust protective behaviors.

The third hypothesis of H3 is to testing the effect of Cybersecurity Awareness of Self Efficacy that has the positive significant effect, and similar with the previous research. This finding is like research by (Hanus & Wu, 2015; Torten et al, 2018) that the impact of awareness of cybersecurity can anticipate the cybersecurity incident. Big 4 Accounting Firms that implement the adoption of cybersecurity awareness by covering a variety of topics and training based on information security policies. This significant positive relationship may be further understood through the characteristic respondents. Many respondent had participated in Security Training from all job function levels which likely contributed to greater security awareness. The understanding of awareness appear to cultivate a stronger belief from their capacity to respond adeptly to cybersecurity challenges. Additionally, the educational level of all Big 4 Accounting Firms employee and the longer working experience could demonstrate in increase capacity for grasping and adopting the cybersecurity measures, which in turns foster greater awareness and confidence in handling the potential risks.

The finding of fourth hypothesis H4 is shown that Cybersecurity Awareness has the positive significant effect towards the Cybersecurity Protection Behavior. Similar of previous research by (Posey et al, 2015; Taherdoost et al, 2024) demonstrated that increased of cybersecurity awareness correlates with higher levels of proactive security among both employees and public. By investing in continuous cybersecurity training and committing to it and allocating the time and resources, cybersecurity awareness of the employee for Big 4 Account Firm can be enhanced to secure the organization's defense against cyber threats. From the characteristic of respondents, the significant number of respondents indicated their involvement in cybersecurity training programs, which are recognized for improving both knowledge and awareness of risks, as well as fostering suitable behavioral responses. Employees with longer work experience might have observed earlier incidents or modifications in policies, which progressively enhances their understanding of cybersecurity. This ongoing awareness fortifies their inclination to implement protective strategies. And individuals who frequently work remotely may exhibit increased cybersecurity awareness as a result of continuous prompts regarding digital threats and the necessity for self-regulated security practices, rendering them more vigilant and adherent to protective actions.

The fifth hypothesis H5 that results the positive significant effect between Self-Efficacy and Cybersecurity Protection Behavior. It is consistent with the finding from the previous research. Finding result by (Tsai et al, 2016; Li et al, 2022) that observed higher self-efficacy leads to a better strategy for cybersecurity protection behavior. Furthermore, the positive relationship that identified in this study highlights the need for organizations by building confidence through hands-on training and empowerment strategies for Big 4 Accounting Firms. Many individuals surveyed had completed security training, which likely played a role in fostering their confidence in their ability to tackle cyber threats. Additionally, self-efficacy was probably strengthened by their work experience and organizational hierarchy, those with greater years of service or higher positions may have acquired the necessary confidence to deal with real-world security challenges. Remote or hybrid work environments typically demand that individuals independently manage security tasks, such as utilizing secure VPNs, performing device updates, or reporting incidents. This independence can foster self-efficacy and promote protective behaviors, especially when training and support are easily accessible.

The six hypothesis for H6 for the effect of Self-Efficacy as mediation between Cybersecurity Knowledge and Cybersecurity Protection Behavior gives the positive significant result. It is aligned with the research of (Anwar et al, 2017; De Kok et al, 2020) that self-efficacy plays as critical psychological mechanism that translates the knowledge into action. This implies that just offering information does not suffice, it is essential for employees to feel assured in their ability to utilize that knowledge effectively in practice. The significant effect for this meditation is supported by the high numbers of respondents that involved in Security Training that boost the confidence level of employees through the simulation training and hands-on exercises. Moreover, the experience working level may foster the sense of competence through reinforcing the self-efficacy and facilitates the translation of knowledge into protective behavior. Respondents who frequently operate from home or in a hybrid context are likely to lean more on their individual knowledge and self-confidence to navigate cybersecurity threats, thereby reinforcing the recognized mediation pathway. This strategy will enable Big 4 firms to effectively align employees' knowledge with their actions, significantly strengthening their cybersecurity defenses.

For the seventh hypothesis H7 was aimed at the mediation of Self-Efficacy between Cybersecurity Awareness and Cybersecurity Protection Behavior with the positive significant as the results. Although an increase in cybersecurity awareness enhances individuals' comprehension of potential threats, mere awareness does not ensure that employees will take protective actions. Rather, those who acknowledge cybersecurity risks and possess confidence in their capacity to respond effectively are more inclined to adopt proactive security measures. It is supported by research from (Chen et al, 2023; Shang et al, 2022) that self-efficacy as the bridge role between awareness and actual behavior. The mediation effect from the respondents with high frequency of involvement for security training are not only increase the awareness of risks, but also practical confidence to take appropriate action, where self-efficacy becomes the key factor for translating the awareness into protective behaviour. While the longer working experience may contribute to develop the self-efficacy through repeated exposure to real world threats, the employees that working remotely may develop higher awareness due to increased exposure and needs to manage the risks independently, thereby strengthening their confidence in applying protection practices. Enhancing self-efficacy can therefore amplify the effectiveness of cybersecurity awareness programs and provide better protection for organizational assets.

CONCLUSION

This research elaborates on literature and findings based on surveys to get a deeper understanding of the practical of cybersecurity knowledge, awareness, and behavior from the management perspective and how to apply it. The importance of cybersecurity for accounting firms and how the Big 4 applied not only from technology readiness, but also preparing the knowledge and awareness of the people and having the process to apply it in day-to-day working activities. By giving knowledge to the people of accounting firm’s staff, it will help them to protect their jobs to mitigate the risk, and by giving them awareness it will help to pay attention to how important cybersecurity is. So, it will make them believe that their action is right to do based on their capabilities and high self-efficacy level.

This study underscores the pivotal role of employee behavior in enhancing cybersecurity resilience within the Big Four accounting firms. The results indicate that cybersecurity protection behaviors are significantly influenced by factors such as perceived threat severity, self-efficacy, and the broader organizational cybersecurity climate. Effective awareness programs, comprehensive training initiatives, and the implementation of clear cybersecurity policies were found to positively increase self-efficacy that impacted to gain employees' protective behaviors.

The Cybersecurity Protection Behavior towards the Big 4 Accounting Firms employees are strongly influenced by Cybersecurity Knowledge, Self-Efficacy, and Cybersecurity Awareness. The better of knowledge and awareness from the employees about cybersecurity, the more employees will have good attitudes for having the protection behavior when faced with the cyber threat. On the other hand, self-efficacy, influenced by Cybersecurity Knowledge and Awareness, plays an important role and gives the strongest effect towards the Cybersecurity Protection Behavior. The employees can evaluate the action what he/she needs to do based on the knowledge and awareness from the organization to handle the cybersecurity threats.

REFERENCES

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. Behavior & Information Technology, 33(3), 237-248. https://doi.org/10.1080/0144929x.2012.708787

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

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. Computers in Human Behavior, 38, 304–312. https://doi.org/10.1016/j.chb.2014.05.046

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, i'll do what I'm asked: Mandatoriness, control, and information security. European Journal of Information Systems, 18(2), 151-164. https://doi.org/10.1057/ejis.2009.8

Boehmer, J., LaRose, R., Rifon, N., Alhabash, S., & Cotten, S. (2015). Determinants of online safety behaviour: towards an intervention strategy for college students. Behaviour & Information Technology, 34(10), 1022–1035. https://doi.org/10.1080/0144929x.2015.1028448

Chen, S., Yang, Y., & Dai, L. (2023). The relationship between network fraud and network security awareness: The mediation role of network social self-efficacy. Atlantis Highlights in Computer Sciences, 222-235. https://doi.org/10.2991/978-94-6463-172-2_25

De Kimpe, L., Walrave, M., Verdegem, P., & Ponnet, K. (2021). What we think we know about cybersecurity: An investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context. Behaviour & Information Technology, 41(8), 1796-1808. https://doi.org/10.1080/0144929x.2021.1905066

De Kok, L. C., Oosting, D., & Spruit, M. (2020). The influence of knowledge and attitude on intention to adopt cybersecure behaviour. Information & Security: An International Journal, 46(3), 251-266. https://doi.org/10.11610/isij.4618

Gerdenitsch, C., Wurhofer, D., & Tscheligi, M. (2023). Working conditions and cybersecurity: Time pressure, autonomy and threat appraisal shaping employees' security behavior. Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 17(4). https://doi.org/10.5817/cp2023-4-7

Gist, M. E. (1987). Self-efficacy: Implications for organizational behavior and human resource management. The Academy of Management Review, 12(3), 472. https://doi.org/10.2307/258514

Grassegger, T., & Nedbal, D. (2021). The role of employees' information security awareness on the intention to resist social engineering. Procedia Computer Science, 181, 59-66. https://doi.org/10.1016/j.procs.2021.01.103

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. European Business Review, 31(1), 2-24. https://doi.org/10.1108/ebr-11-2018-0203

Hair, J. F., Howard, M. C., & Nitzl, C. (2020). Assessing measurement model quality in PLS-SEM using confirmatory composite analysis. Journal of Business Research, 109(1),

101–110. https://doi.org/10.1016/j.jbusres.2019.11.069

Hanus, B., & Wu, Y. “. (2015). Impact of users’ security awareness on desktop security behavior: A protection motivation theory perspective. Information Systems Management, 33(1), 2-16. https://doi.org/10.1080/10580530.2015.1117842

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organizations. European Journal of Information Systems, 18(2), 106-125. https://doi.org/10.1057/ejis.2009.6

Hossain, M. Z., & Zohora, F. T. (2024). Cybersecurity in accounting: Protecting financial data in the digital age. https://doi.org/10.2139/ssrn.4868132

Hossain, M. S., Belina, H., Hasan, M. M., & Kim, M. M. (2024). The Effects of Auditor-level Cybersecurity Breaches on Auditor-Client Relationships. European Accounting Review, 1–28. https://doi.org/10.1080/09638180.2024.2435389

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Computers & Security, 31(1), 83-95. https://doi.org/10.1016/j.cose.2011.10.007

Kankanhalli, A., Teo, H., Tan, B. C., & Wei, K. (2003). An integrative study of information systems security effectiveness. International Journal of Information Management, 23(2), 139-154. https://doi.org/10.1016/s0268-4012(02)00105-6

Khan, N. F., Ikram, N., Murtaza, H., & Javed, M. (2023). Evaluating protection motivation based cybersecurity awareness training on Kirkpatrick’s Model. Computers & Security, 125, 103049. https://doi.org/10.1016/j.cose.2022.103049

Klein, G., Zwilling, M., & Lesjak, D. (2022). A comparative study in Israel and Slovenia regarding the awareness, knowledge, and behavior regarding cyber security. Research Anthology on Business Aspects of Cybersecurity, 424-439. https://doi.org/10.4018/978-1-6684-3698-1.ch020

Li, H., No, W. G., & Boritz, J. E. (2020). Are external auditors concerned about cyber incidents? Evidence from audit fees. AUDITING: A Journal of Practice & Theory, 39(1), 151-171. https://doi.org/10.2308/ajpt-52593

Li, L., Xu, L., He, W., Chen, Y., & Chen, H. (2016). Cyber security awareness and its impact on employee’s behavior. Lecture Notes in Business Information Processing, 103-111. https://doi.org/10.1007/978-3-319-49944-4_8

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees’ cybersecurity behavior. International Journal of Information Management, 45, 13-24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Li, L., Xu, L., & He, W. (2022). The effects of antecedents and mediating factors on cybersecurity protection behavior. Computers in Human Behavior Reports, 5, 100165. https://doi.org/10.1016/j.chbr.2021.100165

Lowry, P. B., & Gaskin, J. (2014). Partial least squares (PLS) structural equation modeling (SEM) for building and testing behavioral causal theory: When to choose it and how to use it. IEEE Transactions on Professional Communication, 57(2), 123-146. https://doi.org/10.1109/tpc.2014.2312452

McCormac, A., Calic, D., Parsons, K., Butavicius, M., Pattinson, M., & Lillie, M. (2018). The effect of resilience and job stress on information security awareness. Information & Computer Security, 26(3), 277-289. https://doi.org/10.1108/ics-03-2018-0032.

Neuman, W. L. (2014). Social research methods: Qualitative and quantitative approaches

Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. Journal of Management Information Systems, 32(4), 179-214. https://doi.org/10.1080/07421222.2015.1138374

Raineri, E. M., & Fudge, T. (2019). Exploring the Sufficiency of Undergraduate Students' Cybersecurity Knowledge Within Top Universities' Entrepreneurship Programs. Journal of Higher Education Theory and Practice, 19(4). https://doi.org/10.33423/jhetp.v19i4.2203

Rosati, P., Gogolin, F., & Lynn, T. (2019). Audit firm assessments of cyber-security risk: Evidence from audit fees and SEC comment letters. The International Journal of Accounting, 54(03), 1950013. https://doi.org/10.1142/s1094406019500136

Sekaran, U. & Bougie, R. (2019). Research Methods For Business: A Skill 8th Edition. New Jersey: Wiley

Shaari, R., Rahman, S. A., & Rajab, A. (2014). Self-efficacy as a determined factor for knowledge sharing awareness. International Journal of Trade, Economics and Finance, 39-42. https://doi.org/10.7763/ijtef.2014.v5.337

Shang, Y., Wu, Z., Du, X., Jiang, Y., Ma, B., & Chi, M. (2022). The psychology of the internet fraud victimization of older adults: A systematic review. Frontiers in Psychology, 13. https://doi.org/10.3389/fpsyg.2022.912242

Shaw, R., Chen, C. C., Harris, A. L., & Huang, H. (2009). The impact of information richness on information security awareness training effectiveness. Computers & Education, 52(1), 92-100. https://doi.org/10.1016/j.compedu.2008.06.011

Shillair, R., Esteve-González, P., Dutton, W. H., Creese, S., Nagyfejeo, E., & Von Solms, B. (2022). Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise. Computers & Security, 119, 102756. https://doi.org/10.1016/j.cose.2022.102756

Taherdoost, H. (2024). A critical review on cybersecurity awareness frameworks and training models. Procedia Computer Science, 235, 1649-1663. https://doi.org/10.1016/j.procs.2024.04.156

Torten, R., Reaiche, C., & Boyle, S. (2018). The impact of security awareness on information technology professionals' behavior. Computers & Security, 79, 68-79. https://doi.org/10.1016/j.cose.2018.08.007

Tsai, H. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. Computers & Security, 59, 138-150. https://doi.org/10.1016/j.cose.2016.02.009

Vinzi, V. E., Trinchera, L., & Amato, S. (2009). PLS path modeling: From foundations to recent developments and open issues for model assessment and improvement. Handbook of Partial Least Squares, 47-82. https://doi.org/10.1007/978-3-540-32827-8_3

Warkentin, M., Johnston, A. C., & Shropshire, J. (2011). The influence of the informal social learning environment on information privacy policy compliance efficacy and intention.

European Journal of Information Systems, 20(3), 267–284. https://doi.org/10.1057/ejis.2010.72

Wang, S., & Wang, H. (2019). Knowledge management for cybersecurity in business organizations: A case study. Journal of Computer Information Systems, 1-8. https://doi.org/10.1080/08874417.2019.1571458

Zhang, Y., Zhang, C., & Xu, Y. (2021). Effect of data privacy and security investment on the value of big data firms. Decision Support Systems, 146, 113543. https://doi.org/10.1016/j.dss.2021.113543

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2020). Cyber security awareness, knowledge, and behavior: A comparative study. Journal of Computer Information Systems, 62(1), 82-97. https://doi.org/10.1080/08874417.2020.1712269