RESEARCH IN MANAGEMENT OF TECHNOLOGY AND BUSINESS
e-ISSN: 2773-5044

RMTB

Vol. 6 No. 2 (2025) 1028-1037
https://publisher.uthm.edu.my/periodicals/index.php/rmtb

The Effect of Cyber Security Training on Job Security in Mediated with Automotive Employees Work Compliance At PT. EX

Wilda Nur Fatimah [1], Uus Mohammad Darul Fadli [1]*, Ery Rosmawati [1]

[1] *Management Study Program, Faculty of Economics and Business, Universitas Buana Perjuangan Karawang, Jl. HS Ronggo Waluyo, Teluk Jambe, Karawang 41361 West Java, INDONESIA*

*Corresponding Author: uus.fadli@ubpkarawang.ac.id
DOI: https://doi.org/10.30880/rmtb.2025.06.02.080

Article Info

Received: 30 September 2025
Accepted: 1 November 2025
Available online: 1 December 2025

Keywords

Cybersecurity training, work security, work compliance

Abstract

Rapid technological advancements in the automotive sector during the digitalization era have introduced digital security challenges, making cybersecurity training essential for individual and organizational protection. Job security and compliance enhance sustainability and operational efficiency. This research aims to explain the extent to which cybersecurity training impacts job security, with work compliance as a mediating variable. This study employs a quantitative descriptive methodology implemented at PT EX. The research involved 100 participants out of a total of 173 workers. Data collection included the distribution of questionnaires and analysis through the PLS-SEM approach, facilitated by SmartPLS 4.0 software. The findings indicate that cybersecurity training has a positive and significant impact on job security by 87.1%, with work compliance mediating 60.9% of the relationship between cybersecurity training and associated variables, while the remainder is affected by external factors not included in the research model.

1. Introduction

Digitalization in the automotive sector has progressed rapidly. Manufacturing companies have embraced various advanced technologies, such as the Internet of Things (IoT), cloud computing, big data, and automation, which are essential elements in the shift towards Industry 4.0. A study from Data Reportal shows that 77% of individuals in Indonesia have internet connections. As a result, Indonesia is among the ASEAN countries with dangerous cyber attack incidents (We Are Social & Meltwater 2024).

PT. EX is a manufacturing company that produces motorcycle and car spare parts. The digitalization developments at PT. EX include automation and data-based systems to improve efficiency, as well as analytical technology to support accurate decision-making. However, digitalization also brings the risk of cyberattacks, such as data theft and malware, which continue to increase and can cause financial losses, reputational damage, and operational disruptions (Susanto et al., 2023).

Companies must have a comprehensive understanding of the importance of cyber security (Rahmat Irawan et al., 2024). The goal of cybersecurity is to protect individuals and organizations from illicit activities that occur online. In this context, cybersecurity training is a strategic step aimed at increasing employees' awareness, knowledge, and skills in identifying and managing cyber threats effectively (Salman Farizy, 2022).

As digital threats continue to evolve, cyber security training is becoming an essential element of a cyber security strategy. Enhancing employees' cybersecurity knowledge is crucial for reducing the risk of cyberattacks and protecting important company information. It is important for companies to provide training to their employees to improve their performance (Anggi Meidita, 2019).

Work compliance is crucial for promoting organizational efficiency and effectiveness. By adhering to rules and procedures, employees can reduce the risk of errors, deviations, and potential losses, creating a structured work environment where each team member performs their responsibilities well. Training and active supervision from management influence the level of compliance with safety procedures. Furthermore, compliance is higher when employees feel the rules genuinely protect them (Mariani et al, 2020).

Monthly studies show that phishing strategies account for 42 percent of all reported scams. A comprehensive record has been compiled, documenting a total of 12,845 unique phishing emails, observed alongside the deployment of 2,560 fake websites as methods for conducting phishing attacks (Yurita et al, 2023).

The results of research conducted by Shen et al (2023) show a significant positive relationship between the effectiveness of security management (X) and the level of company security (Y). The results of Ansari's research (2022) indicate that the use of data security technology models can significantly improve students' ability to understand scientific concepts more effectively compared to traditional methods. The results of Opoku-ahene's research (2022) show a positive result between the application of cybersecurity knowledge and performance in learning in the application of cybersecurity strategies.

Previous research has shown a positive relationship between cybersecurity knowledge and job security, but there are still gaps in understanding the relationship between training and organizational security. No research has specifically explored the direct relationship between the effectiveness of cybersecurity training and the improvement of organizational security, as well as the integration of new technologies in training, while this research has novelty by including work compliance variables as a mediator, which has not been the focus in previous studies. The method used is Smart PLS 4, which is effective in processing primary and secondary data without requiring strict data distribution assumptions.

The problem at PT. EX is the rise of phishing attacks in the name of PT. EX, since 2024, where these attacks have caused leaks of sensitive data such as customer personal information, employee data, and company secrets. Therefore, the company conducts a comprehensive training program to increase awareness of the importance of cybersecurity and how to maintain data security. This study aims to assess the extent to which cybersecurity training affects job security, mediated by employee compliance at PT. EX

2. Review Library

2.1 Human Resource Management

Hasibuan, as quoted in Trisnawati et al. (2021), defines human resource management as a comprehensive methodology for managing the workforce, including skills, motivation, and development. Human resource management (HRM) is the science and art of managing employee relations and activities effectively to achieve business, employee, and community goals. Hadi et al. (2022) defines human resources (HR) as a group of workers working within an organization to achieve specific goals, often referred to as employees. Human resource management can be characterized as a science, based on several concepts that have been explained previously. Human resource management is the process of overseeing the roles and interactions of personnel (employees) within a company to achieve business goals effectively and efficiently.

2.2 Cyber Security Training

Training is a planned systematic effort to transfer knowledge, values, attitudes, and skills to individuals to strengthen and develop human potential and change (Iswan, 2021). Training is a company's planned effort to improve employees' competencies, knowledge, skills, and behavior, so they can master and apply what they have learned in daily activities (Noe, 2020).

Cybersecurity training is a comprehensive program that educates employees about the importance of data privacy and security threats, as well as best practices for protecting sensitive information, so it is concluded that training is a structured activity aimed at improving certain competencies in a short time. The dimensions and indicators of cybersecurity training include: (1) Cybersecurity awareness, with indicators (a) Number of training participants (b) Percentage of employees in identifying cybersecurity; (2) Knowledge of Policies and Procedures, with indicators (a) Level of employee understanding (b) Frequency of cybersecurity policy updates; (3) Practical skills in security threats, with indicators (a) Simulation of cybersecurity threats, (b) Response time to incidents; (4) Application of security practices, with indicators (a) Use of passwords (b) Number of reported cybersecurity incidents; (5) Security culture in the organization, with indicators (a) Employee satisfaction (b) Employee feedback (Ali & guibas, 2024)

2.3 Job Security

Puhakainen and Siponen (2020) define job security as a sense of security in the workplace, including physical and technological dimensions. This feeling of security can increase employee motivation and compliance with business standards. With job security and safety, it is hoped that the parties can carry out their duties safely and

pleasantly. Kurnia et al.'s research in 2021 shows that workers who experience significant job uncertainty often show declining performance levels. Based on the facts mentioned above, it can be concluded that job security is related to deliberate actions by the organization to protect its employees from potential work hazards.

According to Yusuf (2020), the dimensions and indicators of job security are: (1) Job stability, with indicators (a) Level of workload (b) Comfortable and supportive work environment; (2) Security in the job, with indicators (a) Risk management (b) Training and awareness of cyber threats; (3) Security in the organization, with indicators (a) Protection of sensitive data (b) Level of integrity.

2.4 Work Compliance

Work compliance, as defined by Herath & Rao (2021), includes employee behavior in complying with company rules and procedures, including cybersecurity policies. According to Hasibuan in Noorma Yunia et al., (2022:13) Compliance refers to an individual's understanding and commitment to comply with all relevant regulations and social customs. Based on this understanding, it can be concluded that compliance is behavior determined by an individual's awareness to comply with all applicable norms.

According to Blass et.all (2024), the dimensions and indicators of compliance include: (1) Belief, with indicators (a) Belief in company policies (b) Employee perceptions; (2) Accept, with indicators (a) Commitment to policies; (b) Positive support in policies; (3) Act, with indicators (a) Percentage of employees who comply with policies (b) Response to job training.

2.5 Framework

Cybersecurity training is a short-term structured activity to increase employee understanding of cyber threats and prevention. Cybersecurity training is measured by dimensions/indicators, namely security awareness, policies and procedures, practical skills in security threats, application of security practices, security culture in the organization (Ali & Guibas 2024). Job security, which includes job stability, job security, and organizational security, employee compliance with company regulations (Yusuf, 2020). Compliance is a person's awareness and willingness to comply with all applicable regulations and social norms. Work compliance is measured by dimensions/indicators, namely Believing (Belief), Accepting (Accept), Acting (Act) (Blass et all, 2024). Effective cybersecurity training increases understanding, creates a safe work environment, and encourages rule compliance.

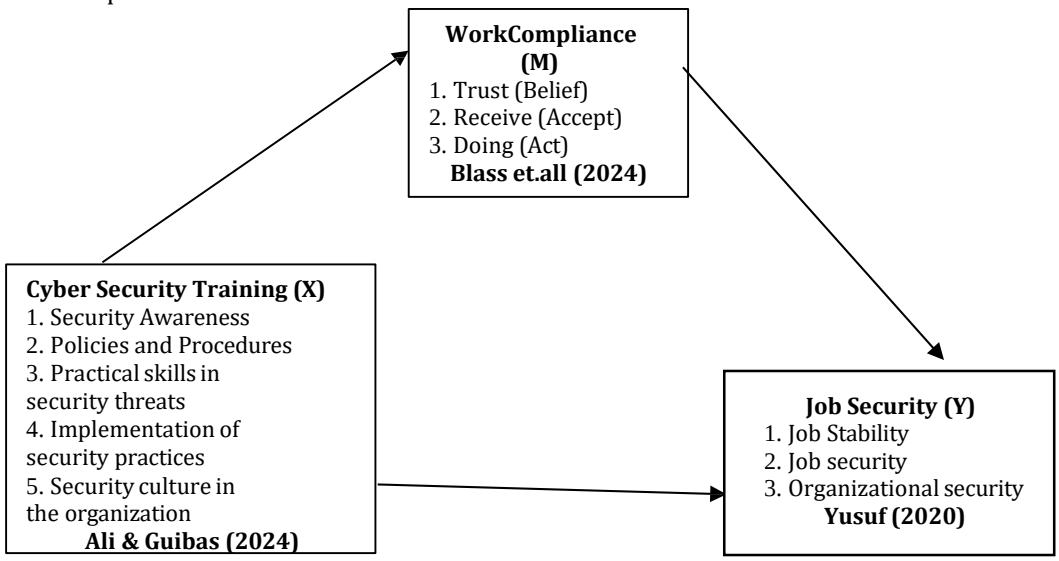

Figure 1 *Framework*

Research Hypothesis:

H1 : It is suspected that *cyber* security training has an impact on employee job security.

H2 : It is suspected that *cyber* security training has an effect on work compliance

H3 : It is suspected that work compliance has an impact on job security.

H4 : It is suspected that work compliance mediates *cyber* security training on employee job security.

Research in Management of Technology and Business Vol. 6 No. 2 (2025) p. 1028-1037

3. Research Methodology

This study uses a quantitative descriptive design and was conducted at PT EX located in Karawang Regency. The population of this study was former employees of PT EX who participated in the cybersecurity training program. A total of 173 workers participated in the program. Hair et al. (2014) suggest that the sample size can be determined by adding the number of indicators by five to ten. This method depends on the quantity of indications. The researchers concluded that they would use 16 indications multiplied by 5, resulting in 80 respondents. Nevertheless, the researcher determined the sample size for this study was one hundred workers who participated in the survey at PT. EX. This was done to reduce and prevent errors

Table 1 *Operational Variables*

Variable	Dimensions	Indicator	Source
Cyber Security Training (X)	*Cyber* security awareness	a. Number of training participants b. Percentage of employees in identifying *cyber security*	Ali and Guibas (2024)
	Knowledge of Policies and Procedures	a. Employee understanding level b. Frequency of cyber security policy updates	
	Practical skills in security threats	a. *Cyber* security threat simulation b. Response time to incidents	
	Implementation of security practices	a. Password usage b. *cyber* security incident reports	
	Security culture in organizations	a. Employee satisfaction b. Employee feedback	
Job Security (Y)	Job stability	a. Workload level b. Comfortable and supportive working environment	Joseph (2020)
	Job Security	a. Risk management b. *Cyber* threat training and awareness	
	Security in organizations	a. Sensitive data protection b. Level of integrity	
Work Compliance (M)	Belief	a. Confidence in company policies b. Employee perception	Blass et.all (2024)
	Acceptance *(Accepted)*	a. Commitment to policy b. Positive support in policy	
	Do *(action)*	a. Percentage of employees complying with policies b. Response to job training	

Primary data was obtained from observations and the distribution of questionnaires with a Likert scale of 1-5. Analysis with SmartPLS 4 begins with data collection and preparation, determining latent variables, indicators, and relationships between variables. The model is then evaluated through reliability and validity tests (Outer Model), analysis of the coefficient of determination, path tests, effect size, and predictive relevance (Inner Model). The results of the analysis are interpreted in the form of models, tables, and graphs.

4. Results and Discussion

4.1 Responden Profile

The profile of respondents who participated in this study based on department of origin and position is explained in the table. 2 below.

Table 2 *Respondent Characteristics Data*

Karateristik	Frekuensi	Presentase
Usia		
20 - 30 Tahun	60	60%
30 - 40 Tahun	22	22%
41 - 50 Tahun	10	10%
51 - 60 Tahun	8	8%
Total	100	100%
Jenis Kelamin		
Laki - Laki	56	56%
Perempuan	44	44%
Total	100	100%

Karateristik	Frekuensi	Presentase
Jabatan		
Supervisor	5	5%
Line Leader	25	25%
Staff	15	15%
Operator	55	55%
Total	100	100%
Lama Bekerja		
1-5 Tahun	62	62%
6-10 Tahun	24	24%
>10 Tahun	14	14%
Total	100	100%

The table explains that the respondents were dominated by male employees as many as 56 employees, employees who have an age range of 20-30 years dominated as many as 60 employees, based on position dominated by employees who have the position of operator as many as 55 employees. And based on length of work, it is dominated by employees who have a length of work range of 1-5 years, namely as many as 62 employees.

4.2 Outer Loading value

The following table shows the results of *outer loading data* using SmartPLS4.

Table 3 *Convergent Validity Test* through *Outer Loading Values*

Indicator	Job Security (Y)	Work Compliance (M)	Cyber Security Training (X)	Information
PKC.1			0.750	Valid
PKC.2			0.830	Valid
PKC.3			0.746	Valid
PKC.4			0.856	Valid
PKC.5			0.753	Valid
PKC.6			0.772	Valid
PKC.7			0.741	Valid
PKC.8			0.764	Valid
PKC.9			0.773	Valid
PKC.10			0.839	Valid
KK.1	0.811			Valid
KK.2	0.780			Valid
KK.3	0.727			Valid
KK.4	0.863			Valid
KK.5	0.814			Valid
KK.6	0.731			Valid
KP.1		0.816		Valid
KP.2		0.894		Valid
KP.3		0.789		Valid
KP.4		0.718		Valid
KP.5		0.781		Valid
KP.6		0.844		Valid

Table 3 above explains that each indicator in each variable in this study meets the *convergent validity criteria* with a value > 0.70. According to Ghozali (2021:68) individual indicators with correlation values above 0.70 are considered valid.

4.3 Validity Test , Composite Reliability, Average Variance Extracted (AVE)

The following are the results of AVE calculations using smartPLS4 software for the variables Cyber Security Training, Job Security, and Job Compliance.

Research in Management of Technology and Business Vol. 6 No. 2 (2025) p. 1028-1037

Table 4 *Cronbach's Alpha Validity Test , Composite Reliability, Average Variance Extracted (AVE)*

Variables	Cronbach's alpha	Composite reliability (rho_a)	Composite reliability (rho_c)	Average variance extracted (AVE)
Cyber Security Training	0.930	0.933	0.941	0.614
Job Security	0.879	0.890	0.908	0.623
Work Compliance	0.893	0.898	0.919	0.654

Hair et al (2017) stated that to ensure validity, the AVE *(Average Variance Extracted) value* must exceed 0.50. Table 4 above shows that the three variables in this study have an AVE value > 0.5, so it is concluded that the three variables are reliable and have a high level of accuracy. Each construct must have a *Cronbach's Alpha* and *Composite Reliability value* > 0.7. Based on the table above, it is concluded that the three variables in this study have a *Cronbach's Alpha* and *Composite Reliability value* > 0.7. Therefore, it can be said that all question items in each construct are reliable.

4.4 R-Square Test (R^2)

Structural Model is a model that connects latent variables through a system of simultaneous equations. Assessment of the structural model can be done by looking at *the R-square* of each dependent latent variable.

Table 5 R-Square test (coefficient of determination)

Variables	R-square	R-square adjusted
Job Security	0.871	0.869
Work Compliance	0.609	0.605

Table 5 above explains that the job security variable has an impact of 87.1% on *cyber security training* and compliance. work, while the remaining 12.9% is caused by other factors not included in this research model. The Work Compliance variable has an impact of 60.9% on *cyber security training* and work security, while the remaining 39.1% is influenced by other factors not included in this research structural model.

4.5 Effect Size Test (f^2)

f-Square value (f2) shows the magnitude of the partial influence of each predictor variable on the endogenous variable. If the *f-square value* is > 0.35, it can be interpreted that the latent variable predictor has a large influence. If the f-square value is 0.15, it has a medium influence. If the *f-square value* is 0.02, it has a small influence (Mulyanto et al., 2023).

Table 6 Effect Size Test (f2)

Variables	Job Security	Work Compliance
Cyber Security Training	0.050	1,557
Work Compliance	2,097	

Table 6 above explains that the value of f^2 = 0.050 shows that the contribution of *cyber security training* to changes in job security is relatively small. The value of f^2 = 1.557 shows that *cyber security training* is very significant in increasing work compliance. This influence is dominant compared to other variables. The value of f^2 = 2.097 shows a very large effect of job security on work compliance.

4.6 Predictive Relevance Test (Q^2)

The Q^2 test is conducted to determine and measure how good or ideal the observation results and parameters are. Q2 value > 0 indicates that the model has *predictive relevance* , while Q2 < 0 indicates that the model lacks *predictive relevance* (Ghozali, 2021:74).

Square Test Results	
Variables	**Q^2**
Job Security	0.584
Work Compliance	0.587

Table 7 shows that the Q^2 value for the job security variable is 0.584 and the work compliance variable is 0.587, which means that the value is above 0. Therefore, the observation value produced in this research model has a good predictive correlation.

4.7 Hypothesis Testing Results

Hypothesis testing aims to determine the direct influence between independent and dependent variables. The results of the analysis can be seen in Figure 1.

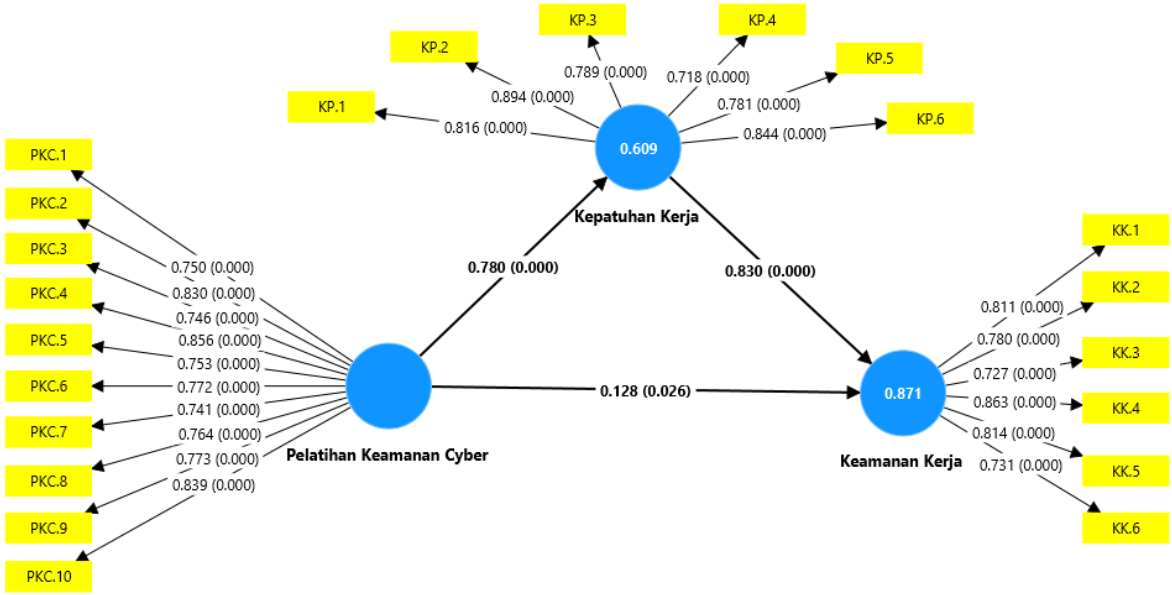

Figure 1 *Bootstraping Output Results*

Significant assessment was tested using the *bootstrapping method* by referring to the parameter coefficient values and t-statistics from the algorithm results. *bootstrapping* . According to Yurindera (2022) in Anggraini et al., (2024) hypothesis testing in SEM-PLS involves t-statistics and probability, where the hypothesis is accepted if the t-statistic > 1.984 and probability < 0.05.

Table 7 *Path Coefficients*

Variables	Original sample (O)	Sample mean (M)	Standard deviation (STDEV)	T statistics (|O/STDEV|)	P values
Cyber Security Training -> Job Security	0.128	0.123	0.057	2.233	0.026
Cyber Security Training -> Work Compliance	0.780	0.788	0.039	19,883	0.000
Work Compliance -> Job Security	0.830	0.837	0.044	19,081	0.000

Table 7 above shows that the effect of *Cyber security training* on job security has a t-statistic value of 2.233> 1.984 , with a p-value of 0.001<0.5. The hypothesis of the effect of *cyber security training* on job security is positive and significant. Furthermore, the t-statistic of the effect of *cyber security training* on job compliance of 19.883> 1.984 with a p value of 0.00<0.5. This shows that the hypothesized *cyber security training* has a positive and significant effect on work compliance. While the t-statistic value of work compliance on work security is 19.081, which means that the hypothesis of the effect of work compliance on work security is also positive and

significant.

4.8 Test Indirect Effects

Table 8 *Indirect Effects Test*

	Original sample (O)	Sample mean (M)	Standard deviation (STDEV)	T statistics (|O/STDEV|)	P values
Cyber Security Training -> Work Compliance -> Work Security	0.648	0.659	0.047	13,866	0.000

Table 8 above explains that the t-statistic value of *Cyber security training* on job security through work compliance is 13.866 exceeding 1.984 , with a p value of 0.000 less than 0.5. The hypothesis of the effect of *Cyber security training* on job security through work compliance is positive and significant.

4.9 The Impact Of Cyber Security Training On Job Security

The data shows a significant correlation between cybersecurity training and job security. The level of job security for PT.EX employees is closely correlated with the amount of training they choose to do. The results of this test support research by Shen et al, (2023) showing the results of a significant positive relationship between the effectiveness of security management (X) and the level of corporate security (Y). Research by Kamalia et al, (2024) shows that cyber security training effectively increases knowledge, awareness, and ability to identify cyber threats and implement security practices. The main influential factor is the frequency of cyber security policy updates, with an outer loading value of 0.856. This confirms that the training successfully improved employees' understanding of security procedures, threat detection, and policy implementation in work operations.

4.10 Cyber Security Training on Work Compliance

The results showed that cybersecurity training significantly improved regulatory compliance among personnel at PT. EX. There is a good relationship between the level of job security and the level of employee compliance. The findings of Onumo et al. (2021) show that cybersecurity training (X) increases knowledge and awareness of security hazards, thereby motivating employees to comply with established rules and procedures (Y), which aligns with the results of the study. Deep understanding of cyber security, leadership support, and security technology play a role in improving employee compliance. Cyber security training not only strengthens knowledge of policies and procedures, but also increases awareness of security risks (Ripa., 2023). The main influential factor is employee perception, with an outer loading value of 0.894, which indicates that training increases awareness and compliance with security procedures. The training not only improves understanding of security risks, but also encourages compliance with organizational policies.

4.11 Work Compliance and Workplace Safety

The data shows that compliance with work laws positively and significantly affects job security. The level of job security is directly related to worker performance. The results of this test corroborate the conclusions of Al-Alawi and AlBassam (2019), who determined that cybersecurity compliance had the highest mean score (4.28), while cybersecurity culture had the lowest mean score (4.24). Nonetheless, these variables significantly influenced the level of cybersecurity awareness. All respondents agreed that these aspects are needed in the banking sector. The need for cyber security culture training confirms that increased awareness compliance and effective training contribute significantly to employee compliance as well as strengthening work security systems in the digital era (Khoironi, 2020). The main influential indicators are training and cyber threat awareness, with an outer loading value of 0.863. This finding confirms that the implemented work security system is effective in improving work security through employee compliance.

4.12 Cyber Security Training On Job Security Through Employee Compliance

The results showed that cyber security training on job security through employee compliance showed a significant influence between cyber security training (X) on job security (Y) with employee compliance (M) as mediation. Job security contributed 87.1%, and job compliance 60.9% to cyber security training. This indicates that employee compliance acts as a mediator that connects cyber security training to job security at PT. EX. These

results are supported by Renaud et al.'s research, (2021) cyber training is designed to improve employee abilities, such as threat detection skills (e.g. phishing), creative thinking, curiosity, and the ability to analyze situations. With consistent application of work compliance and adaptation to technological changes and threats, organizations can increase their readiness and ability to respond to evolving cyber threats (Hoshmand et al., 2023). Based on the results of the analysis, the employee perception indicator has the highest value of 0.894, indicating very high compliance. This proves the success of the cybersecurity training program in increasing employee compliance.

5. Conclusion

The research findings show a positive correlation between cybersecurity training and workplace security, a positive correlation between cybersecurity training and workplace compliance, and a positive impact of cybersecurity training on workplace security. Furthermore, employee compliance acts as a mediating variable that facilitates the relationship between cybersecurity training and workplace security in HEIs. The information provided shows that workplace cybersecurity training and compliance are not only influenced by the training itself but also by other factors. This illustrates that cybersecurity training and workplace compliance significantly influence workplace security outcomes.

6. Implications

The implications of this study suggest that companies can improve the cybersecurity training offered to their employees. In addition, job security is not only influenced by cybersecurity training and labor compliance, but also by other aspects that have not been studied, so further research is needed. Good support in policy has a relatively smaller impact compared to other factors. Therefore, companies need to evaluate and strengthen these aspects, for example by improving employee compliance in security procedures and clarifying occupational security standards to increase the effectiveness of training programs.

Acknowledgement

The author would like to thank the Faculty of Economics and Business, Buana Perjuangan University, Karawang for its support.

Conflict of Interest

The authors declare no conflict of interest regarding the publication of this paper.

Author Contribution

The authors confirm contributions to the paper as follows: conception and design of the study: WNF,, UMD., and ER; data collection: WNF., UMDF., and ER; analysis and interpretation of results: WNF., UMDF., and ER; drafting of the manuscript: WNF., UMDF., and ER. All authors reviewed the results and approved the final version of the manuscript.

References

Ali, W., & Guibas, L. (2024, July). Human resources compliance with cybersecurity principles: Legal and ethical dimensions. https://doi.org/10.13140/RG.2.2.34731.25128

Hasani, T., O'Reilly, N., Dehghantanha, A., Rezania, D., & Levallet, N. (2023). Evaluating the adoption of cybersecurity and its influence on organizational performance. *SN Business & Economics, 3.* https://doi.org/10.1007/s43546-023-00477-6

Hendrawan, M. M. M., & Rahayu, A. (2021). Konformitas dan kontrol diri perannya terhadap kepatuhan pada protokol kesehatan menjaga jarak. *Psikologi Kreatif Inovatif, 1(1),* 21–29.

Herdadi, A., & Ayu, I. S. (2024). Pelatihan penggunaan keamanan dan komunikasi internal training on the use of cybersecurity of corporate information. *Puan Indonesia, 6(1),* 371–376.

Husain, B. A. A., & Santoso, A. B. (2022). Analisis kepatuhan karyawan terhadap pemberlakuan prosedur operasional standar (SOP) pada perusahaan baru (studi kasus pada PT. Prina Duta Rekayasa) Kota Tangerang Selatan. *Jurnal Tadbir Peradaban, 2(2),* 105–113. https://doi.org/10.55182/jtp.v2i2.154

Kamalia, A. Z., Herlianto, H. R., Rozikin, Z., & Suwarno, A. (2024). Pelatihan cyber security untuk perlindungan data dan privasi pada karyawan PT CKD Manufacturing Indonesia. *Madaniya, 5(3),* 1181–1186.

Khoironi, S. C. (2020). Pengaruh analisis kebutuhan pelatihan budaya keamanan siber sebagai upaya pengembangan kompetensi bagi aparatur sipil negara di era digital. *Jurnal Studi Komunikasi dan Media,*

24(1), 37. https://doi.org/10.31445/jskm.2020.2945

Machlul, M. (2024). Peningkatan kualitas SDM melalui pelatihan cyber security pada anggota polisi daerah Jawa Timur. *Parta: Jurnal Pengabdian Kepada Masyarakat, 4(2),* 150–155. https://doi.org/10.38043/parta.v4i2.4655

Mohammad, H., & Alam, G. (2022). Cybersecurity awareness and training (CAT) framework for remote working employees. *Sensors, 22(22),* 8663. https://doi.org/10.3390/s22228663

Oluwaseun Abrahams, T., Farayola, O. A., Kaggwa, S., Uwaoma, P. U., Hassan, A. O., & Dawodu, S. O. (2024). Cybersecurity awareness and education programs: A review of employee engagement and accountability. *Computer Science & IT Research Journal, 5(1),* 100–119. https://doi.org/10.51594/csitrj.v5i.708

Onumo, A., Ullah-Awan, I., & Cullen, A. (2021). Assessing the moderating effect of security technologies on employees compliance with cybersecurity control procedures. *ACM Transactions on Management Information Systems, 12(2).* https://doi.org/10.1145/3424282

Opoku-Ahene, A. R. (2022). The influence of cyber security implementation strategy on organizational knowledge management and performance – A case study of Sinapi Aba Savings and Loans in Ghana (pp. 217–228).

Politeknik Siber dan Sandi Negara. (2021). Badan siber dan sandi negara. *3(0251),* 1–2.

Renaud, K., Flowerday, S., & Dupuis, M. (2021). Moving from employee compliance to employee success in the cybersecurity domain. *Computer Fraud and Security, 2021(4),* 16–19. https://doi.org/10.1016/S1361-3723(21)00043-9

Saad, A., Renaud, K., & Omoronyia, I. (2022). Moving beyond cyber security awareness and training to engendering security knowledge sharing. *Information Systems and E-Business Management, 21,* 123–158. https://doi.org/10.1007/s10257-022-00575-2

Shen, Y., & Turner, C. (2023). Cybersecurity training in organization as human capital investment: A qualitative grounded theory analysis. *International Journal of Business and Management, 18(4),* 38. https://doi.org/10.5539/ijbm.v18n4p38

Sitanggang, Y. L. (2016). Pengaruh keamanan kerja dan persepsi dukungan organisasi pada kinerja dengan kepuasan kerja sebagai variabel pemediasi. *Skripsi,* 1–23.

Study, Z. C., Anggraini, F., Mohammad, U., Fadli, D., & Rosmawati, E. (2024). Research in management of technology and RMTB customer perception and literacy regarding the implementation of green banking at BCA Bank Tbk. *5(1),* 1871–1884.

Tan, T. H., Sama, T., Wibowo, G., Wijaya, G., et al. (2024). Kesadaran keamanan siber pada kalangan mahasiswa universitas di Kota Batam. *Jurnal Teknologi dan..., 14(2),* 163–173. https://doi.org/10.34010/jati.v14i2

Wiratama, A. D. (2023). Cyber security in 2023: The latest challenges and solutions. *Jurnal Komputer Indonesia, 2(1),* 47–54. https://doi.org/10.37676/jki.v2i1.569

Wibowo, B., & Hidayat, T. (2024). Strategi efektif dalam meningkatkan kesadaran keamanan siber terhadap ancaman phishing di lingkungan perusahaan PT. XYZ. *Jurnal Pengabdian Masyarakat Sultan Indonesia, 2(1),* 1–9. https://doi.org/10.58291/abdisultan.v2i1.294