

The Influence of Digital Literacy, Peer Influence, and Security Training Effectiveness on Cybersecurity Behavior in the Banking and Finance Industry

**Mozart Malik Ibrahim^{1*}, Fildzah Shabrina², Feni Marnilin³, Tyahya Whisnu Hendratni⁴,
Riesna Apramilda⁵, Judianto Tjahjo Nugroho⁶**

Perbanas Institute¹, Universitas Negeri Jakarta², Universitas Nusa Bangsa³, Universitas
Pancasila⁴, Universitas Ibnu Sina⁵, STIE GICI⁶

Correspondence Email: mozart.malik60@perbanas.id*

Abstract

The study's main goal is to investigate how the three factors, digital literacy, peer influence, and security training, affect the cybersecurity behavior of the bank and finance industry's personnel. The research applied a quantitative explanatory method with a sample of 150 employees from banks, financial institutions, and fintech companies. The sample was drawn purposefully from the population. The multiple linear regression analysis results show that the independent variables digital literacy, peer influence, and security training all have a positive and significant impact on the dependent variable, which is cybersecurity behavior. The research not only makes a theoretical contribution to the discussion about human motivations in cybersecurity but also provides recommendations for the banking and finance industry that include increasing the level of digital literacy activities, encouraging positive social influences at workplaces, and maximizing the effectiveness of security training as a risk management strategy.

Keywords: digital literacy, peer influence, security training effectiveness, cybersecurity behavior.

INTRODUCTION

It is said that the banking and finance sector is the most endangered by cybercrime and viewed as the most serious threat to the industry (Mahrani et al., 2024). The massive number of digital transactions, the cutting-edge financial technology, and the extremely high confidentiality of customer data are the major causes of this situation (Bakri et al., 2023). On the other hand, mobile banking together with e-wallets and payment services linked to the trend of digital services have made financial and banking institutions more vulnerable to threats as the very services have become the most sought after by the hackers. Phishing, malware, identity theft, and digital fraud are some of the attack methods that call for the concerned companies to upgrade the security measures (Gai et al., 2024). At the same time, research has revealed that the problem of low cybersecurity is not only a result of technology failures but also of personnel that do not meet the required standards. Employee behavior in relation to cybersecurity is a key factor in the overall security of the banking system, as even a very minor action like clicking on a suspicious link, revealing passwords, or leaving devices

unattended can create a security leak that is even bigger than what a hacker might need to break in (Purwati et al., 2025). Therefore, it is very important to identify the factors that influence employees' attitudes towards cybersecurity, as this understanding can result in compliance and, in the long run, the cyber-resilience of the highly regulated and risky industry. Hence, one can assert that the cultivation of cybersecurity behavior becomes a strategic imperative for the financial institutions to not only secure their operations but also their public trust and reputation, rather than just a possible choice (Sani et al., 2025).

The personnel with high digital skills will be the most knowledgeable about cyber-attacks and at the same time, they will be the cautious users of the digital resources in existence, hence they will not be the ones committing the unauthorized activities. Similarly, they would be the ones who would actually be worried about the security and would, thus, be the ones to report any cases of identity theft or fake digital assets (Marnilin et al., 2016). Moreover, such employees are the ones who will not even complain about the changes to the company's security policies and will quickly adapt to the new guidelines. Digital literacy is therefore the most important indicator for companies to ensure that every worker is skilled enough to battle cyber threats (Marnilin et al., 2024). Henceforth, it would be crucial to establish the relationship between digital literacy and security behavior in order to enhance the human resource capacity against the rising digital security threats (Harahap & Apramilda, 2023). Furthermore, peer pressure might occur through informal talks, for example, discussing the cyber world threats, or through daily work habits which are means of subtly influencing people's opinions and attitudes towards digital security (Hendratni et al., 2024). In the present-day scenario of global work cultures, the power of society often beats legal rules and regulations as the employees tend more to mimic their co-workers. The performance of the training for the personnel has a great impact depending on the methods used, the relevance of the content, how often the training is done, and the involvement of the participants in actual threat situations like phishing or incident response drills (Hendratni et al., 2022). Good training not only increases understanding but also elevates the good practices that are slowly and surely integrated into the everyday work of the staff. On top of this, consistent and well-structured training fosters a strong cybersecurity culture throughout the organization (Laili & Apramilda, 2023). Hence, realizing the extent to which training affects the cyber security practices of the employees is a necessary condition for the strategies to have the cyber resilience of the banking and finance sectors strengthened.

According to the description provided in the previous text, the study will be directed towards the impact of digital literacy, peer influence, and security training efficiency on the cybersecure behavior of the banking and finance businesses. The research will be considered a theoretical contribution to the literature already available about cybersecure behavior and the social and digital aspects that affect it. Besides, it will also help greatly in shedding light on the ways that digital literacy, social influence, and training effectiveness can together form safe working habits in such high-risk industry environments. On the contrary, the research will also give a great support to the institutions in terms of finance, by directing them to the source of reference for their policies, training, and internal communication strategies, thus, increasing the employee awareness concerning cybersecurity. Moreover, the study equips the security managers, HR, and organizational leaders with the information they need to not only come up with tech-based but also human behavior-oriented strategies, which, indeed, are the key to the digital security of the institution.

METHOD

In the present research, a quantitative explanatory approach was adopted, which is a method that defines the causal link between digital literacy, peer influence, and security training effectiveness as the primary factors determining the cybersecurity behavior of workers in the banking and finance sectors. The population of the study included employees from the banking and finance sectors such as central banks, micro finance companies, technological innovations, digital financial services, and even those in technology support for such entities. The sample method that was chosen was purposive sampling, and the eligible participants had to satisfy the specific requirements laid down by the researchers. The requirements were: (1) workers who have been at the organization for a minimum of one year; (2) taking part in the digitized process such as internal banking system access, financial application use, or being on technology-based platforms; (3) having been trained in cybersecurity in the past 12 months; and (4) being knowledgeable about their company's information security policies. Among the 150 respondents meeting the above-listed preconditions, the present study considered them as the representative sample of the financial industry's cybersecurity behavior. The survey adopted a 5-point Likert scale questionnaire, with the lowest point for agreement being 1 (strongly disagree) and the highest point being 5 (strongly agree). The analysis was performed with the help of multiple linear regression. The value of the coefficient of determination (R^2) was calculated to ascertain the extent to which the independent variables accounted for the variation in cybersecurity behavior that was explainable.

RESULT AND DISCUSSION

The results of the F-test reveal that the regression model is significant at the same time with an F-count value of 67.41 which surpassed the F-table of 3.05 at a $0.000 < 0.05$ significance level. This together with the large impact of digital literacy, peer influence, and security training effectiveness on cybersecurity behavior. The coefficient of determination (R^2) value of 0.69 means that the three independent variables account for 69% of the variability in employee cybersecurity behavior while the remaining 31% is subject to the influence of other factors such as organizational culture, security policies, system quality, and psychological factors of individuals. The partial t-test indicates that all independent variables possess a t-count greater than t-table (1.97) and a significance value below 0.05, thereby confirming positively and significantly the three, all the variables. This implies that digital literacy, peer influence, and security training effectiveness are the primary factors affecting how people behave in terms of security in the banking and financial sector.

The results of the research highlighted digital literacy as a key and positive predictor of employee cybersecurity behavior in the banking and finance sector. This means that had the worker been better acquainted with and skilled in using digital technology, he or she would have chosen the right security measures. Digital literacy receives people to have wider sight of the possible security threats, namely, phishing, counterfeit links, and viruses or unauthorized programs that may have access to and eventually ruin the company data. The skilled users are in a position to distinguish easily between true and false information, are well aware of the security measures being in place, and do follow the digital security policy. Besides, in the case of banks, digital literacy assists in the detection of coinage of unusual transactions, proper management of passwords, usage of secure networks, and reporting of cyber incidents. The academic results support the Digital Competence Framework theory which asserts that digital literacy consists of the technology-related skills and also the mental and behavioral aspects which are the most important area of digital security that determines

the mortality rate of this aspect. The ongoing innovation and sophistication of financial technologies will ultimately make the digital literacy skill an indispensable trait that determines the employees' capability to combat the always changing and diverse kinds of cyber threats.

The research pointed out that peer influence resulted in an increase and a significant impact on the cybersecurity behavior. This means that the workplace interactions are also contributing to the individual and their corresponding cybersecurity behavior skills. Employees often follow the patterns of their colleagues and if the latter are viewed as getting better training or having a good reputation for compliant digital security, they would do it even more. If coworkers are always in the same routine, such as changing passwords, being super careful when handling external files or reporting any unusual activities, these behaviors might then be gradually acknowledged as the new rules that will be accepted by others. Peer influence can also be noticed when there are casual talks about cyber threats, sharing of security incidents and digital activities being warned about in an encouraging way. This study supports the social influence theory which claims that social pressure, the need to belong, and group norms are the main ways to control individual behavior. In the strictly regulated banking sector, peer influence becomes the factor that collectively secures the maintenance of cybersecurity. Thus, peer influence plays the role of a social instrument that not only fortifies the digital resilience of the organization but also makes the behavior secure in all work-related activities.

Security training implementation, according to the research findings, significantly and positively affects cybersecurity conduct. Thus, security behavior will be practiced more and more in the employees' daily work as the security training becomes more and more effective. An absolutely effective cybersecurity training course is not only theoretical input but also includes simulating cyberattacks, showing real cases, and letting the trainees practice how to cope with digital threats. When the staff participating in the training become aware of the risks, understand the security policy better, and are the ones who take both preventive and reactive measures against cyber incidents, they will be the best trained people in that area. The impact of training also depends on various factors such as the frequency, quality of instructors, relevance of the content, and the organization's capability to provide a continuous learning process. This research finding also supports the Human Firewall Theory, which states that the employees trained can be the first line of defense in the digital security of an organization. Thus, the security training done right not only reinforces the cybersecurity behavior but also strengthens the whole organization's digital resilience.

CONCLUSION

The study's results show that the digital literacy of employees, the effect of their colleagues, and the security training all together have a very strong and significant connection with the cyber behavior of people working in the financial and banking sectors. Besides, security training is important in giving the employees awareness, skills, and readiness to meet the challenges posed by the constantly changing cyber threats. In short, these three factors are the major ones that contribute to the development of a strong cybersecurity culture; an aspect that is very much needed for the survival of the banking and finance industry, which is characterized by high digital risk and sensitive data. This study thus supports the continuous banking and finance industry's digital literacy initiatives through regular training, flexible learning modules, and disseminating information about the latest security trends. Social and cultural managers should make full use of the positive peer influence by adopting policies for mutual reminders, internal security teams, and the appointment of digital security role

models in each department of the company. Moreover, the classic methods of training might not be sufficient to maintain the participants' interest, therefore the training program should include interactive elements such as attack simulations, case studies, phishing simulation, and assessments so that the intended change in behavior is permanent.

REFERENCES

- Bakri, A. A., Wandanaya, A. B., Violin, V., & Fauzan, T. R. (2023). The Application of UTAUT Modified Model to Analyze the Customers Use Behavior of Shopee Paylater. *Jurnal Sistim Informasi dan Teknologi*, 96-101.
- Gai, A. M., Chatra, A., Ibrahim, M. M., Anantadjaya, S. P., & Nawangwulan, I. M. (2024). Analysis of The Influence of Information Availability, Economic Factors and Changing Trends on Travel Agent Business Sustainability in Digital Era. *Jurnal Sistim Informasi dan Teknologi*, 6-11.
- Purwati, S., Asmarany, A. I., Akbar, M., Suroso, A., Ibrahim, M. M., & Orias, M. (2025). ANALISIS PENGARUH MANAJEMEN PELATIHAN BERKELANJUTAN, ORGANIZATIONAL CULTURE DAN DIGITAL PERFORMANCE MANAGEMENT TERHADAP KINERJA KARYAWAN. *JURNAL LENTERA BISNIS*, 14(2), 1963-1971.
- Gai, A. M., Purwati, S., Violin, V., & Ibrahim, M. M. (2024). The Application of Plural Panelist Synthesis Method in Identifying Determinant Factors That Influence Economic Growth. *Jurnal Sistim Informasi dan Teknologi*, 18-22.
- Sani, A., Shabrina, F., Dana, W. P., Hardini, I. R., Juansa, A., Zulfikar, Z., ... & Angin, J. T. K. P. (2025). *PENGANTAR TEKNOLOGI INFORMASI: Dampak dan Peluang Perkembangan Teknologi Informasi dalam Dunia Kerja dan Bisnis*. Star Digital Publishing.
- Marnilin, F., Mulyadi, J. M. V., & Darmansyah, D. (2016). ANALISIS DETERMINAN TERHADAP PERSISTENSI LABA PADA PERUSAHAAN JASA DI BEI. *JURNAL LENTERA AKUNTANSI*, 2(2), 14-25.
- Marnilin, F., Irawan, R., & Widjaja, I. R. (2024). The Effect of Debt-to-Equity Ratio (DER) and Inflation on Profit Growth of Building Construction Companies Listed on the Indonesia Stock Exchange in 2020. *Journal of Social Science and Business Studies*, 2(4), 277-285.
- Hendratni, T. W., Soemarsono, D. W., & Harsono, H. (2024). Peran perbankan yang terdaftar di bursa efek Indonesia dalam implementasi bisnis hijau dan pembangunan berkelanjutan. *JPPi (Jurnal Penelitian Pendidikan Indonesia)*, 10(3), 729-745.
- Hendratni, T. W., Soemarsono, D. W., & Harsono, H. (2022). Strategi sektor perbankan menghadapi ancaman non performing loan pada masa pandemic COVID-19. *AKURASI: Jurnal Riset Akuntansi dan Keuangan*, 4(3), 201-210.
- Laili, N. I., & Apramilda, R. (2023). Analisis Pengaruh Ukuran Perusahaan, Leverage, Dan Profitabilitas Terhadap Pengungkapan Corporate Social Responsibility (Studi Kasus Pada Perusahaan Pertambangan Yang Terdaftar di Bursa Efek Indonesia Pada Tahun 2015-2019). *Realible Accounting Journal*, 2(2), 27-38.
- Mahrani, S. W., Nurdiani, T. W., Pramono, S. A., Aulia, M. R., & Apramilda, R. (2024). Driving Employee Performance in Agribusiness: The Role of Technology Adoption, Emotional Intelligence, and Digital Competence. *Jambura Agribusiness Journal*, 6(1).
- Harahap, B., & Apramilda, R. (2023). Pengaruh Company Size, Inventory Value Dan Profit Margin Terhadap Value Of The Company Pada Perusahaan Manufaktur Sub Sektor Industri Barang Konsumsi Yang Terdaftar Di Bei Tahun 2017-2021. *Realible Accounting Journal*, 2(2), 1-10.