IJESE
(International Journal of Econimics, Science, and Education)
Volume 3 Number 2 2026
ISSN : 3046-689X (ONLINE)

CYBERSECURITY RISK MANAGEMENT: INTEGRATING TECHNOLOGY AND DIGITAL SECURITY AWARENESS

Ni Wayan Lasmi[1]*, Komang Widhya Sedana Putra P[2], Wayan Sri Maitri[3]

[1,2,3]Economy Departement, Universitas Pendidikan Nasional, Denpasar, Bali, Indonesia
Jl. Bedugul No. 39, Sidakarya, South Denpasar, Denpasar City, Bali 80224, Indonesia
Email: [1]wayanlasmi@undiknas.ac.id, [2]widhyasedana@undiknas.ac.id, [3]srimaitri@undiknas.ac.id
Correspondence Author Email: wayanlasmi@undiknas.ac.id

ABSTRACT

Purpose: This study examines how cybersecurity resilience can be strengthened by integrating technological capabilities and human factors. Specifically, it explores the role of cybersecurity technology and digital security awareness in enhancing cybersecurity risk management, using a combined perspective of the Technology Acceptance Model (TAM) and Resource-Based View (RBV).

Design/methodology/approach: A quantitative approach was employed using Partial Least Squares–Structural Equation Modeling (PLS-SEM). Data were collected from digital companies operating in Denpasar to test the proposed relationships and moderating effects.

Findings: The results indicate that cybersecurity technology significantly improves cybersecurity risk management. In addition, digital security awareness strengthens this relationship, suggesting that higher awareness enhances the effectiveness of technological tools.

Research limitations/implications: The study is limited by its focus on a single geographic area and a cross-sectional design, which may limit broader applicability. Future research is encouraged to involve multiple regions and longitudinal data.

Practical implications: Organizations should not rely solely on technological investments but also prioritize improving employees' digital security awareness to achieve stronger cybersecurity resilience.

Originality/value: This study contributes by integrating TAM and RBV to highlight the interaction between technological and human capabilities in cybersecurity risk management.

Paper type: Research paper

Keyword: Cybersecurity Technology, Cybersecurity Risk Management, Digital Security Awareness

A. INTRODUCTION

The way organizations function and engage with their stakeholders has changed due to digital technology advancements (Cheng et al., 2024). There are new opportunities for growth and efficiency because of automation, cloud computing, AI, and big data analytics (Hakimi et al., 2024). However, new digital technology develops to meet the needs of automation and artificial intelligence (Bukartaite & Hooper, 2023). With these rapid changes, industries will encounter a new set of cyber risks such as data breaches, identity theft, ransomware, phishing, and attacks against critical infrastructures. These are no longer standalone occurrences, and the public and private sectors will have to deal with these recurring risks. These risks call for the implementation of effective cyber-attack risk management systems that can predict, mitigate, and respond effectively to the challenges posed by the digitized world (Slapničar et al., 2022). The absence of any disruption caused by cyber incidents continues to be one of the foremost challenges in any business organization, irrespective of the considerable investments made in the security infrastructure of organizations. Although the use of advanced technologies like encryption, AI-based monitoring, and intrusion detection systems have improved security, the use of technology alone is not enough to solve the entire problem (Kayode Saheed et al., 2022). Many cyber incidents are successful not because of any weakness in the system, but due to mistakes, negligence, and lack of awareness on the part

of the user (Colabianchi et al., 2025). Therefore, the problem of cybersecurity must be understood not purely as a technological problem, but a behavioral and organizational problem as well.

The role of awareness in the use of security systems is paramount. Employees and users are the first line of defense in any organization, and their actions, both positive and negative, will determine the successful implementation of any organizational strategy, including the security strategy (Grassegger & Nedbal, 2021). Ignoring security system alerts, falling prey to phishing scams, and intentionally or accidentally leaking sensitive information are all actions that nullify the advanced security measures that are in place, irrespective of the security systems employed. The presence, or absence, of awareness constitutes a moderating effect on the relationship that exists between the implementation of cybersecurity technologies and the effective management of cybersecurity risk (Murad & Qudah, 2025). Historically, the investigation in this field has concentrated on two different, non-overlapping, strands. One of these examines the technology side, concentrating on advanced devices and systems for diminished probability of cyber incidents (Cremer et al., 2022), while the other focuses on the various facets of the human side, outlining the value of training, culture, and organizational behavior for building organizational resilience (Assoratgoon & Kantabutra, 2023). Integrating the two into one cohesive approach, centered on the convergence of technology and human consciousness, remains an unaddressed need. In the absence of this, cyber security risk management approaches may lack completeness and may, therefore, ignore one of the major components of the cyber security value chain, namely the interplay between the technology and the people.

The uniqueness of this research is primarily based on the integration of digital security awareness as a moderating variable in the nexus of cyber security technologies and cyber security risk management. It stresses the proposition that the management of cyber risks is contingent upon not just the availability of advanced systems, but also on the awareness consciousness, and the practice of safe behavior of individuals within an organization. It is a considerable value expansion of the perspective on organizational resilience towards the risks of cyber threats, as it places the human element of responsibility together with technological systems in countering cyber risks. Consequently, this study aims to understand how cybersecurity technologies affect the effectiveness of risk management, examine the impact of digital security awareness on this relationship, and provide practical recommendations that help organizations integrate technological and psychosocial investments. In this way, the study aims to make a dual contribution to the body of knowledge and the body of practice by providing a rationale in which technology and human awareness simultaneously mitigate risks in a digital ecosystem, achieving the fundamental principle of sustainable cyber risk management.

The Technology Acceptance Model (TAM) describes how people accept and use technology and focuses on two primary factors: perceived usefulness and perceived ease of use (Aljarrah et al., 2016). In considering cybersecurity, the understanding and use of protective technologies like encryption, intrusion detection, and AI monitoring depend on how users assess their effectiveness and ease of operation (Parambil et al., 2024). When employees consider the protective technologies user-friendly and value-adding, their consistent use and responsible handling will follow. Such congruence on perception of technology and user capabilities considerably enhances system efficiency in managing risks (Loske et al., 2014). This reflects the importance of the human element described by Technology Acceptance Model in the deployment of complex cybersecurity measures.

The Resource-Based View (RBV) emphasizes that the unique resources possessed by an organization—including physical, technological, and human capabilities—can form the basis for sustainable competitive advantage (Mailani et al., 2024). In the field of cybersecurity, the advanced technologies of a potential competitor constitute valuable and rare resources. However, the strategic value of these technologies can be fully realized only when advanced human competencies are integrated. Technologies and human competencies can be integrated when employees possess digital security awareness, training, and proactive behavioral practices, thus becoming intangible assets of the organization. Organizations that integrate advanced cybersecurity technologies with an adaptive

workforce are more resilient to digital threats (Ussher-eke, 2025). From the RBV perspective, the synergy between technology as a tangible resource and awareness as an intangible capability strengthens the resilience of the organization's risk management systems, thereby ensuring its sustainability in the digital environment.

The Technology Acceptance Model (TAM) provides a comprehensive foundation for the understanding of technology usage and adoption by individuals and organizations (Jiang et al., 2025). At the root of TAM are two constructs: perceived usefulness and perceived ease of use. Applied to cybersecurity, these constructs explain why some technologies are successfully adopted while others are resisted. If employees believe that security features such as encryption, intrusion detection systems, or AI-driven monitoring tools will allow them to perform their job more securely and efficiently, they will be more willing to accept and utilize them on a regular basis. Likewise, if the technologies are perceived as being simple to utilize rather than awkward, adoption is far more probable. Thus, TAM emphasizes that the efficacy of cybersecurity measures depends not only on the advancement of technology tools but also on how users view and are ready to utilize them (Wandira & Fauzi, 2022). By aligning technological innovation with user needs and perceptions, organizations make the technology for cybersecurity an effortless component of daily risk management practices.

The Resource-Based Perspective (RBV) contributes to this debate by framing cybersecurity as not simply a matter of tool adoption, but rather as an outcome of combining tangible and intangible resources to achieve sustained advantages (Ahavi, 2023). The RBV posits that competitive advantage is achieved when organizations possess at their disposal valuable, rare, inimitable, and non-substitutable resources. Cybersecurity technologies such as firewalls, real-time threat monitoring systems, and advanced authentication protocols undoubtedly are useful and, in certain instances, limited resources. However, their strategic potential depends on how firms integrate them with human capabilities, that is, employees' digital security awareness and skills. Human capital is the abstract element that transforms technology from a passive tool into an active defense (Russ, 2017). Employees who are conscious of threats, follow best practices, and proactively support security policies turn into technology more effective, thereby making the company's overall resilience better. In this context, RBV stresses that it is the convergence of superior technological assets and advanced human skills that devises a unique and sustainable defense system against cyber threats.

The growing sophistication of cyber threats also warrants the synthesis of the two theoretical models. Modern organizations are faced with increasingly complex attacks, ranging from phishing and ransomware to highly targeted intrusions that exploit both technical vulnerabilities and human weaknesses. While technological controls such as multi-factor authentication, encryption, and AI-driven threat detection can counter many of these threats, they are not foolproof when implemented in a siloed fashion. The majority of cybersecurity breaches happen not because of the absence of tools but rather because of human errors such as negligence, poor passwords, failure to follow established procedures, or unawareness of emerging threat types (Yeo & Banfield, 2022). That reality puts digital security awareness at the forefront of maximizing technological investment return. Awareness transforms the employees into the first line of defense rather than the weakest link in organizational security.

The integration of TAM and RBV provides a strong theoretical foundation for examining how cybersecurity technologies and human awareness jointly influence risk management outcomes. TAM focuses on individual adoption and usage of technology, while RBV focuses on the strategic integration of technological resources and human capabilities. Taken together, these frameworks suggest that organizations cannot rely on technology alone; they must cultivate a culture of vigilance and security-conscious behavior in order to achieve effective cybersecurity risk management. Practically, this would mean that as much as it is necessary to invest in frontier technologies, it must be followed up with training, awareness, and organizational policies that foster compliance and vigilance among employees. According to this rationale, the following hypotheses are formulated:

H1: Cybersecurity Technology has a positive impact on Cybersecurity Risk Management.

Cybersecurity Technology is expected to have a positive impact on Cybersecurity Risk Management. Organizations that invest in advanced security systems are better positioned to detect, prevent, and respond to cyber threats effectively (Haapamäki & Sihvonen, 2019). These technologies strengthen organizational resilience, protect sensitive information, and reduce system vulnerabilities (Fatima et al., 2024). When properly implemented, they significantly improve the efficiency and reliability of risk management practices. Therefore, the adoption of cybersecurity technologies is hypothesized to enhance the overall effectiveness of managing cyber risks.

H2: Digital Security Awareness moderates the relationship between Cybersecurity Technology and Cybersecurity Risk Management.

Cybersecurity technologies provide essential tools to prevent, detect, and mitigate threats, but their effectiveness depends largely on how they are used by employees (Pankajakshan & Maheshwari Bangur, 2024). Digital Security Awareness ensures that staff understand the importance of these technologies, follow security protocols, and recognize potential risks. When awareness is high, technologies such as firewalls, authentication systems, and monitoring tools are utilized more effectively, strengthening overall risk management (Tambwe et al., 2023). Conversely, when awareness is low, employees may neglect or misuse these tools, reducing their protective value. Therefore, Digital Security Awareness acts as a key moderating factor that amplifies the benefits of cybersecurity technologies in managing risks.

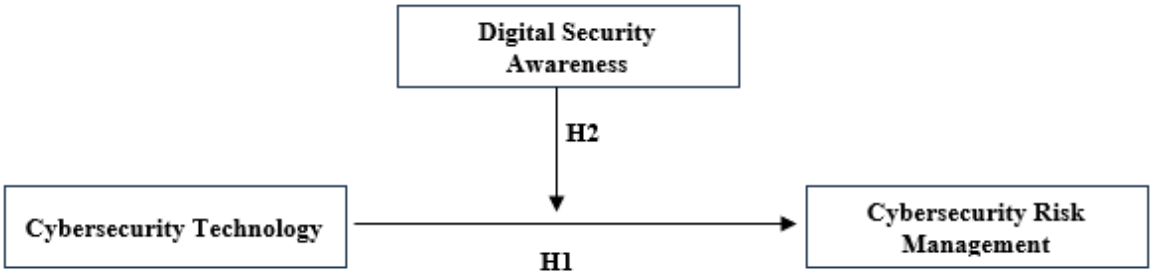

Figure 1. Research Model

B. METHODOLOGY

The research is conducted in Denpasar, Bali, on the digital business firms, including SMEs and startups. Denpasar was chosen as the research location because it is among the most rapidly growing digital markets in Bali where technology adoption is rapidly increasing but at the same time also faces challenges in the form of limited infrastructure, economic assistance, and digital divides. The city itself is unique as well, with the integration of legacy business conventions and new bases of digital modernity, creating a fertile context for understanding the role of cybersecurity technology adoption in the development of more effective risk management practices.

The study applies a purposive sampling approach. The respondents are managers or owners of digital business companies—startups and SMEs—who have adopted or are considering adopting cybersecurity technologies in their companies. To verify the validity of the data, additional criteria are established: (1) the firm must be operating in digital-savvy industries such as e-commerce, FinTech, or logistics; (2) respondents must have at least rudimentary knowledge about cybersecurity practices; and (3) the firm must be willing to collaborate and provide adequate responses. Based on PLS-SEM rule of thumb, the sample size is determined by multiplying the indicators with 5 to 10. With approximately 15 indicators, the minimum required sample size following the 5–10 times rule of thumb is between 75 and 150 respondents. To ensure robustness and adequate representation, this study targets around 200 respondents, which exceeds the minimum threshold. (Hair, 2022).

A standardized questionnaire is employed as the research instrument. The questionnaire seeks to measure this research's most significant variables: Cybersecurity Technology (X), i.e., the level of usage and adoption of security technologies such as firewalls, encryption, and intrusion detection systems; Cybersecurity Risk Management (Y), which measures the company's ability to identify, evade, and react properly to cyber attacks; and Digital Security Awareness (Z), i.e., the employees' and managers' level of knowledge regarding cybersecurity risks, compliance with procedures, and proactive security behavior. The measurement items are crafted on a five-point Likert scale, ranging from 1 = Strongly Disagree to 5 = Strongly Agree. Sensitive crafting is undertaken for each item to address both the technological and human aspects of cybersecurity, as well as the potential moderating role of digital security awareness in achieving risk management results.

The analysis of data is done utilizing Partial Least Squares Structural Equation Modeling (PLS-SEM) using the aid of SmartPLS version 4.0 software. PLS-SEM is selected because it is feasible for measuring complex models that include latent constructs, as well as the measurement of relatively small to medium-sized samples (Magno et al., 2024). Analysis process is in two stages: (1) the Measurement Model, which tests for reliability and validity of the constructs through convergent and discriminant validity tests, and (2) the Structural Model, which tests for the hypothesized causal relationships among cybersecurity technology, cybersecurity risk management, and digital security awareness as a moderator. This analytical viewpoint is most likely to offer extensive insights on how cybersecurity technology has a direct impact on organizational risk management and how digital security awareness strengthens these ties to create stronger digital business ecosystems.

C. RESULTS AND DISCUSSION

Descriptive Analysis

Table 1. Descriptive Statistics Table

Characteristics	Category	Frequency	Percentage (%)
Gender	Male	121	60.5
	Female	79	39.5
Age	18–25 years	41	20.5
	26–35 years	78	39
	36–45 years	51	25.5
	> 45 years	30	15
Education	High School	49	24.5
	Diploma/Associate Degree	61	30.5
	Bachelor’s Degree	69	34.5
	Master’s Degree	21	10.5

Table 1 describes the demographic characteristics of the 200 respondents. The majority are male (60.5%), while female respondents account for 39.5%. In terms of age, most respondents fall within the productive age groups, with 39% aged 26–35 years and 25.5% aged 36–45 years, which indicates that the study participants are in a stage where professional and business activities are highly active. Regarding educational background, the largest group holds a Bachelor’s degree (34.5%), followed by Diploma/Associate degree holders (30.5%). This suggests that most respondents have relatively high educational attainment, which is beneficial for understanding digital business dynamics and cybersecurity issues. Overall, the profile reflects a sample dominated by educated and productive-age individuals, appropriate for examining technology adoption and risk management in the digital business sector.

Reliability and Validity Test

Table 2. Cosntruct Reliability and Validity

	Cronbach's alpha	Composite reliability (rho_a)	Composite reliability (rho_c)	Average variance extracted (AVE)
Cybersecurity Technology	0.790	0.894	0.848	0.552
Cybersecurity Risk Management	0.790	0.925	0.848	0.571
Digital Security Awareness	0.815	0.941	0.892	0.670

Table 2 indicates that each of the three constructs—Cybersecurity Technology, Cybersecurity Risk Management, and Digital Security Awareness—achieves satisfactory reliability. Cronbach's alpha values (0.790–0.815) are above the minimum value of 0.70, which suggests that items under each construct have good internal consistency. Likewise, composite reliability scores (rho_a and rho_c) for all the constructs are more than 0.80, which is yet another measure of measurement reliability. These results affirm that the constructs are being measured fairly and as accurately as possible with regards to their corresponding indicators.

Validity-wise, the Average Variance Extracted (AVE) estimates are 0.552 for Cybersecurity Technology, 0.571 for Cybersecurity Risk Management, and 0.67 for Digital Security Awareness. Due to the reason that all AVE scores are greater than the cut-off of 0.50, the constructs achieve adequate convergent validity, in that indicators measure a considerable amount of the variance of their latent variables. Together, the findings validate that the measurement model is reliable and valid with a firm foundation for structural relationships testing of the research model.

Hypothesis Test

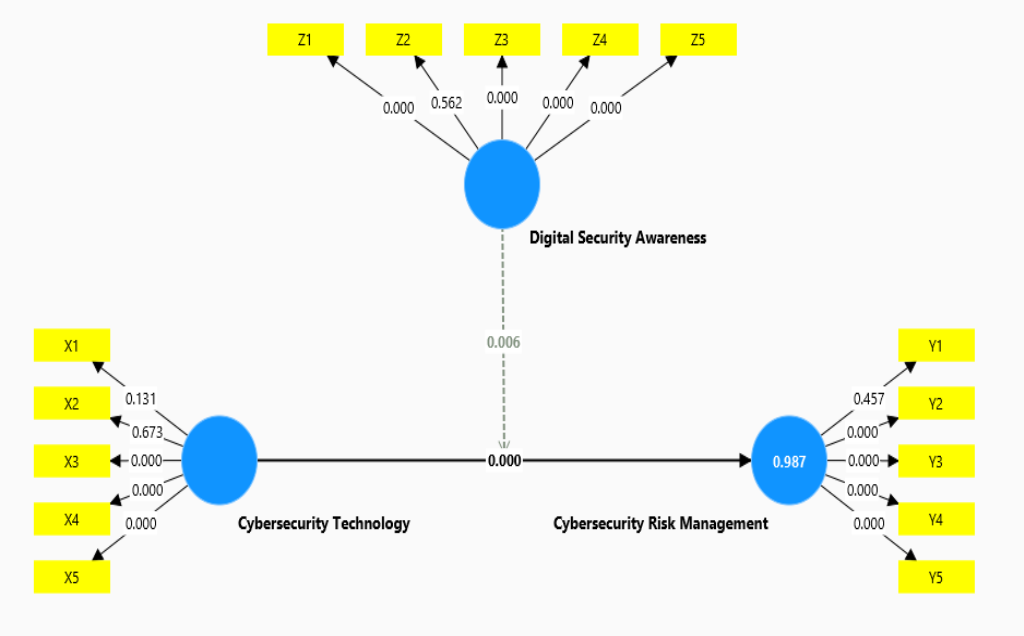

Figure 2. Structural Equation Model Testing

Table 3. Regression Weight Structural Equational Model

	Original sample (O)	Sample mean (M)	Standard deviation (STDEV)	T statistics (|O/STDEV|)	P values
Cybersecurity Technology -> Cybersecurity Risk Management	0.677	0.653	0.061	9.051	0.000
Digital Security Awareness x Cybersecurity Technology -> Cybersecurity Risk Management	0.023	0.022	0.008	2.754	0.006

From Figure 2 and Table 3, the structural model results indicate that Cybersecurity Technology has a strong and positive impact on Cybersecurity Risk Management ($\beta = 0.677$, $T = 9.051$, $p < 0.001$). It implies that companies adopting and using advanced cyber technologies are in a position to better detect, prevent, and mitigate cyber attacks. The high path coefficient also indicates that adoption of technology is at the center of improving general risk management practices.

Apart from that, the moderating role of Digital Security Awareness × Cybersecurity Technology → Cybersecurity Risk Management is also positive and significant statistically ($\beta = 0.023$, $T = 2.754$, $p = 0.006$). Although the coefficient is quite small in relation to the direct effect, it shows that Digital Security Awareness moderates and enhances the effectiveness of cybersecurity technologies toward managing risks. That is, with higher levels of employee and manager awareness, technology's role in risk management is solidified, demonstrating the interdependence required between technology equipment and human factors in achieving effective cybersecurity outcomes.

Discussion

The findings of this study provide solid empirical support to the proposed hypotheses and highlight the critical interaction between technology adoption and human awareness in cybersecurity risk management. Firstly, the findings confirm H1, which reveals that Cybersecurity Technology significantly and positively affects Cybersecurity Risk Management ($\beta = 0.677$, $p < 0.001$). This result affirms the reality that firms that strategically invest in leading-edge security technologies such as firewalls, encryption mechanisms, and intrusion detection systems are in a better position to prevent, detect, and respond to cyber threats. The large path coefficient further highlights that technology plays a direct role in enabling organizational resilience by reducing vulnerabilities and defending sensitive information. This is in line with the Technology Acceptance Model (TAM), where it is stated that adoption is based on perceived ease of use and perceived usefulness. When employees see these systems as useful and easy to use, frequent use follows, and organizational risk management performance improves.

The second significant finding relates to H2, where the moderating effect of Digital Security Awareness in Cybersecurity Technology and Cybersecurity Risk Management was examined. The results indicate that Digital Security Awareness significantly improves this relationship ($\beta = 0.023$, $t = 2.754$, $p < 0.01$). Although the coefficient is smaller than the direct effect of technology, its statistical significance verifies that human factors are not only complementary but also a necessity in ensuring the success of cybersecurity measures. This is in line with the Resource-Based View (RBV) accounting for how sustainable competitive advantage is achieved by companies through combining tangible resources

(cybersecurity technologies) and intangible resources (employee knowledge and awareness). Awareness in this context is human capability that renders technology an active, strategic defense entity instead of a passive tool. Lack of awareness, in turn, can render even the most sophisticated tools powerless to produce their intended impact through negligence, mistake, or intentional misuse by hands of users. Awareness is thus a driving force that increases the value gained from investment in technology.

Theoretically, the study proves the complementarities between TAM and RBV. TAM outlines how employees' faith in the usefulness and usability of technology guide the uptake of the technology and its absorption within organizational daily routines. Meanwhile, RBV situates the combination of technology and awareness as a rare, valuable, and imitable asset that promotes resilience. Overall, the results suggest that organizations cannot rely solely on tech awareness. Instead, they must actively integrate training, awareness initiatives, and a security-conscious culture in an effort to derive optimal return on investments. The empirical hypothesis that awareness acts as a mediator of the technology–risk management relationship is sustained by the evidence that highlights the contention that cybersecurity is as much a matter of behavior and organization as it is technical.

From the managerial implications standpoint, the results provide several meaningful insights. First, managers need to realize that mere investment in cybersecurity technologies is not sufficient. To realize maximum returns on such investments, companies must invest effort in organizing digital security awareness programs, which include well-planned training sessions, phishing simulation, and regular checks for compliance. Second, organizations must integrate cybersecurity awareness into corporate culture, which becomes everybody's responsibility across all the levels of the firm. This not only reduces the risk of human error but also turns workers into proactive guardians rather than vulnerabilities in the security chain. Third, SME and startup managers, particularly in early-stage digital environments such as Denpasar, Bali, must balance investments in technology with low-budget high-value awareness campaigns, thereby sustaining resilience despite tight purse strings. Last but not least, strategically, technology and awareness integration represents a risk-adjusted defense that not only reduces threats but also reinforces customer confidence, builds up reputation, and offers a competitive advantage in the online market.

D. CONCLUSION

This study confirms that Cybersecurity Technology has a significant positive impact on Cybersecurity Risk Management, and Digital Security Awareness significantly strengthens this impact. The findings stress that it is not sufficient to have advanced security tools alone; they work in direct proportion to workers' awareness, knowledge, and active behavior. This confirms the convergence between Technology Acceptance Model (TAM) and Resource-Based View (RBV), proving that cyber threat resilience originates from the interaction between technological resources and human awareness as a non-material capability. Implications for managers, especially in startups and SMEs, are clear: investments in security technology must be accompanied by programs of awareness, training, and organizational support to enable digital resilience on a sustained basis.

But such a study has its limitations in scope and design. The convergence of digital business firms in Denpasar has a tendency to limit the generalizability of findings, and cross-sectional research design and reliance on self-reported data may not accurately reflect long-term dynamics or actual practices. In the future, the study can be replicated in other locations and industries, can utilize longitudinal designs, and include other intervening variables such as leadership, organizational culture, or regulatory compliance. By doing so, researchers can provide a clearer picture of how organizations develop sustainable cybersecurity resilience in the current highly digitized society.

E. REFERENCES

Ahavi, K. S. (2023). *Rollins Scholarship Online Cyber Risk Management from a Resource Advantage Perspective*.

Aljarrah, E., Elrehail, H., & Aababneh, B. (2016). E-voting in Jordan: Assessing readiness and

developing a system. *Computers in Human Behavior*, *63*, 860–867. https://doi.org/https://doi.org/10.1016/j.chb.2016.05.076

Assoratgoon, W., & Kantabutra, S. (2023). Toward a sustainability organizational culture model. *Journal of Cleaner Production*, *400*, 136666. https://doi.org/https://doi.org/10.1016/j.jclepro.2023.136666

Bukartaite, R., & Hooper, D. (2023). Automation, artificial intelligence and future skills needs: an Irish perspective. *European Journal of Training and Development*, *47*(10), 163–185. https://doi.org/10.1108/EJTD-03-2023-0045

Cheng, Z. M., Bonetti, F., de Regt, A., Ribeiro, J. Lo, & Plangger, K. (2024). Principles of responsible digital implementation: Developing operational business resilience to reduce resistance to digital innovations. *Organizational Dynamics*, *53*(2), 101043. https://doi.org/https://doi.org/10.1016/j.orgdyn.2024.101043

Colabianchi, S., Costantino, F., Nonino, F., & Palombi, G. (2025). Transforming threats into opportunities: The role of human factors in enhancing cybersecurity. *Journal of Innovation & Knowledge*, *10*(3), 100695. https://doi.org/https://doi.org/10.1016/j.jik.2025.100695

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. *The Geneva Papers on Risk and Insurance. Issues and Practice*, *47*(3), 698–736. https://doi.org/10.1057/s41288-022-00266-6

Fatima, F., Hyatt, J. C., Rehman, S. U., De La Cruz, E., Nadella, G. S., & Meduri, K. (2024). Resilience and risk management in cybersecurity: A grounded theory study of emotional, psychological, and organizational dynamics. *Journal of Economy and Technology*, *2*, 247–257. https://doi.org/https://doi.org/10.1016/j.ject.2024.08.004

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/https://doi.org/10.1016/j.procs.2021.01.103

Haapamäki, E., & Sihvonen, J. (2019). Cybersecurity in accounting research. *Managerial Auditing Journal*, *34*(7), 808–834. https://doi.org/10.1108/MAJ-09-2018-2004

Hair, J. (2022). Partial Least Squares Structural Equation Modeling (PLS-SEM) in second language and education research: Guidelines using an applied example. *Research Methods in Applied Linguistics*, *1*(3), 100027. https://doi.org/https://doi.org/10.1016/j.rmal.2022.100027

Hakimi, M., Amiri, G. A., Jalalzai, S., Darmel, F. A., & Ezam, Z. (2024). Exploring the Integration of AI and Cloud Computing: Navigating Opportunities and Overcoming Challenges. *TIERS Information Technology Journal*, *5*(1), 57–69. https://doi.org/10.38043/tiers.v5i1.5496

Jiang, S., Li, H., & Gan, D. (2025). Technology acceptance model for online education: identifying interdisciplinary topics and their evolution based on BERTopic model. *Social Sciences & Humanities Open*, *12*, 101831. https://doi.org/https://doi.org/10.1016/j.ssaho.2025.101831

Kayode Saheed, Y., Idris Abiodun, A., Misra, S., Kristiansen Holone, M., & Colomo-Palacios, R. (2022). A machine learning-based intrusion detection for detecting internet of things network attacks. *Alexandria Engineering Journal*, *61*(12), 9395–9409. https://doi.org/https://doi.org/10.1016/j.aej.2022.02.063

Loske, A., Widjaja, T., Benlian, A., & Buxmann, P. (2014). Perceived it security risks in cloud adoption: The role of perceptual incongruence between users and providers. *ECIS 2014 Proceedings - 22nd European Conference on Information Systems*, 0–16.

Magno, F., Cassia, F., & Ringle, C. M. (2024). A brief review of partial least squares structural equation modeling (PLS-SEM) use in quality management studies. *The TQM Journal*, *36*(5), 1242–1251. https://doi.org/10.1108/TQM-06-2022-0197

Mailani, D., Hulu, M. Z. T., Simamora, M. R., & Kesuma, S. A. (2024). Resource-Based View Theory to Achieve a Sustainable Competitive Advantage of the Firm : Systematic Literature Review. *International Journal of Entrepreneurship and Sustainability Studies*, *4*(1), 1–15.

Murad, H. A., & Qudah, M. (2025). The attitudes of communicators toward cybersecurity concerning security, safety in national institutions. *Frontiers in Communication*, *10*(July), 1–22. https://doi.org/10.3389/fcomm.2025.1552520

Pankajakshan, J., & Maheshwari Bangur, R. (2024). Employee Awareness and Attitudes Towards Cybersecurity Technologies. *Journal of Advances and Scholarly Researches in Allied Education*, *21*(5), 113–120. www.ignited.in

Parambil, M. M. A., Rustamov, J., Ahmed, S. G., Rustamov, Z., Awad, A. I., Zaki, N., & Alnajjar, F. (2024). Integrating AI-based and conventional cybersecurity measures into online higher education settings: Challenges, opportunities, and prospects. *Computers and Education: Artificial Intelligence*, *7*, 100327. https://doi.org/https://doi.org/10.1016/j.caeai.2024.100327

Russ, M. (Ed.). (2017). *Human Capital and Assets in the Networked World*. Emerald Publishing Limited. https://doi.org/10.1108/9781787148277

Slapničar, S., Vuko, T., Čular, M., & Drašček, M. (2022). Effectiveness of cybersecurity audit. *International Journal of Accounting Information Systems*, *44*, 100548. https://doi.org/https://doi.org/10.1016/j.accinf.2021.100548

Tambwe, O. T., Aigbavboa, C. O., & Akinradewo, O. (2023). Benefits of construction data risks management in the construction industry. *Journal of Engineering, Design and Technology*, *23*(2), 458–476. https://doi.org/10.1108/JEDT-11-2022-0577

Ussher-eke, D. (2025). *Building a cyber-resilient workforce through HR and IT Collaboration*. *27*(June), 706–716.

Wandira, R., & Fauzi, A. (2022). TAM Approach: Effect of Security on Customer Behavioral Intentions to Use Mobile Banking. *Daengku: Journal of Humanities and Social Sciences Innovation*, *2*(2), 192–200. https://doi.org/10.35877/454ri.daengku872

Yeo, L. H., & Banfield, J. (2022). Human Factors in Electronic Health Records Cybersecurity Breach: An Exploratory Analysis. *Perspectives in Health Information Managemen*, *19*(Spring), 1i.