Employee Engagement and Integrating Organizational Cybersecurity: A Conceptual Framework for Malaysian FinTech

Sugesanan Renganathan[1], Rohani BT Mohd[2]*

[1]Business Faculty, UNITAR International University, Selangor, Malaysia

[2]Business Faculty, UNITAR International University, Selangor, Malaysia

***Corresponding Author**

DOI: https://doi.org/10.47772/IJRISS.2026.101000399

Received: 18 October 2026; Accepted: 23 October 2026; Published: 03 November 2026

ABSTRACT

The rapid expansion of financial technology (FinTech) has increased the importance of effective cybersecurity risk management (CRM). Although Malaysia has introduced regulatory instruments, including the Cyber Security Act 2024 and Bank Negara Malaysia's Risk Management in Technology policy, effective cybersecurity also depends on how organizational controls are implemented in practice. This conceptual paper develops a framework linking technology adoption, regulatory implementation and secure remote-work practices to CRM, with employee engagement proposed as a mediating mechanism. The framework integrates the Technology-Organization-Environment (TOE) framework with the Job Demands-Resources (JD-R) model. TOE explains how technological and environmental conditions shape organizational cybersecurity arrangements, while JD-R helps explain how work resources and demands may influence employee engagement and security-related conduct. Seven propositions are developed to guide future empirical testing; the paper itself does not validate those propositions with new data. The contribution is an integrative one: organizational conditions and an employee-level mechanism are brought into a single, testable model scoped to Malaysian FinTech, while distinguishing regulated financial institutions from other FinTech firms. The paper also identifies construct-definition, perceptual measurement and level-of-analysis issues that future multi-source and longitudinal research must address.

Keywords: Cybersecurity risk management; employee engagement; FinTech; Technology-Organization-Environment framework; Job Demands-Resources model

INTRODUCTION

Malaysia’s financial technology (FinTech) sector has expanded alongside national efforts to accelerate digitalization. The Malaysia Digital Economy Blueprint identifies digital financial services and FinTech development as components of the country’s wider digital-economy ambitions (Economic Planning Unit, 2021). Estimates published in 2025 placed the Malaysian FinTech ecosystem at approximately 360 firms across areas such as digital payments, lending, wealth management and digital assets (Fintech News Malaysia, 2025a). The country’s digital-banking services have also expanded, while real-time payment infrastructure supports increasingly connected financial transactions (Fintech News Malaysia, 2025b; Bank Negara Malaysia [BNM], 2024). These developments create opportunities for financial inclusion and service innovation, but they also increase the importance of protecting interconnected systems, sensitive data and digital transactions.

For this paper, "Malaysian FinTech" refers to organizations that provide technology-enabled financial products or services in Malaysia, spanning digital payments, lending, wealth management, digital assets and related activities (Fintech News Malaysia, 2025a). The sector is not homogeneous in regulatory exposure. Licensed digital banks and other institutions supervised by Bank Negara Malaysia (BNM) face technology-risk expectations under the Risk Management in Technology (RMiT) policy (BNM, 2025). Capital-market intermediaries may fall under the Securities Commission Malaysia's Guidelines on Technology Risk

Management (Securities Commission Malaysia [SC], 2024). Designated National Critical Information Infrastructure (NCII) entities have obligations under the Cyber Security Act 2024 (National Cyber Security Agency [NACSA], 2024). Other FinTech firms may operate with lighter or different formal obligations even when they handle sensitive customer data and interconnected payment rails. Clarifying these boundaries matters because regulatory implementation, as used in the framework, means the organizational translation of applicable requirements rather than the mere existence of national statutes. Future empirical work should therefore treat regulatory status as a sampling and boundary condition, not as a uniform backdrop for all Malaysian FinTech firms.

Digital financial services are exposed to evolving cyber threats, including fraud, phishing, ransomware and attacks on interconnected systems. CyberSecurity Malaysia reported 1,657 incidents to its Cyber999 Incident Response Centre in the first quarter of 2025, compared with 1,550 in the preceding quarter; fraud was the most frequently reported category (CyberSecurity Malaysia, 2025). Although national incident figures do not represent FinTech incidents alone, they provide relevant context for the wider threat environment in which Malaysian financial-technology firms operate. At the international level, research has also identified a broad range of FinTech-related threats and corresponding defensive strategies (Javaheri et al., 2024). Cybersecurity therefore needs to be considered not only as a technical issue but also as an organizational risk-management responsibility.

Malaysia has established regulatory requirements relevant to cybersecurity and technology risk. The Cyber Security Act 2024 sets obligations for designated National Critical Information Infrastructure (NCII) entities, while BNM's Risk Management in Technology policy establishes technology-risk and resilience expectations for institutions within its regulatory remit (National Cyber Security Agency [NACSA], 2024; BNM, 2025). The Securities Commission Malaysia also issued Guidelines on Technology Risk Management (Securities Commission Malaysia [SC], 2024). These instruments provide important governance requirements, but their scope and applicability differ across types of organizations. Moreover, the existence of rules does not by itself establish that controls are understood, implemented, tested and improved consistently. Organizational capability and employee conduct therefore remain relevant to the effectiveness of formal cybersecurity arrangements.

Employees routinely interact with digital systems, customer information, access controls and security alerts. Their decisions can either reinforce or weaken the controls established by an organization. Malaysian studies indicate that employees' threat perceptions, self-efficacy, security awareness and management support are associated with cybersecurity-related behaviour (Sulaiman et al., 2022; Ramalu et al., 2023). However, the findings also caution against assuming that awareness training alone will reliably improve behaviour: Ramalu et al. (2023), for example, reported a positive association between awareness training and risky behaviour in their sample. Such results suggest that cybersecurity outcomes may depend on how training, organizational support, workload and employee motivation interact.

This issue is consistent with research on cybersecurity fatigue. Repeated security demands, poorly designed procedures or excessive training requirements may contribute to fatigue and reduce employees' willingness to engage with security practices (Reeves et al., 2021; Hsu et al., 2024). A meta-analysis by Cram et al. (2019) also indicates that security-policy compliance is shaped by multiple attitudinal, normative and organizational factors rather than by a single intervention. Consequently, the presence of security policies, technologies and training should not be treated as sufficient evidence of effective implementation. The organization must also consider whether employees understand the purpose of controls, have the resources to follow them and remain motivated to support security objectives.

These considerations are particularly relevant to FinTech firms, which may rely on cloud computing, artificial intelligence, blockchain, advanced analytics and application programming interfaces. Such technologies can improve service delivery and support detection or response capabilities, but they may also introduce risks involving access management, data handling, system configuration and third-party connections. The effectiveness of security controls consequently depends on both technological capability and the organizational processes through which the technology is configured, monitored and used. Regulatory requirements likewise need to be translated into clear responsibilities and everyday practices.

Remote and hybrid work add another dimension because employees may access organizational systems from different locations, networks and devices. These arrangements can increase exposure when access controls, device security or reporting procedures are inadequate (Borkovich & Skovira, 2020; Nizamuddin, 2025). Remote work is not, however, inherently beneficial or harmful to cybersecurity: its implications depend on the security arrangements and resources accompanying it. For this reason, the present framework distinguishes the prevalence of remote work from the secure remote-work practices required to manage the associated risks.

Despite research on cybersecurity adoption, employee security behaviour and remote-work risks, the literature synthesized for this paper does not establish a single, integrated explanation of how technology adoption, regulatory implementation and secure remote-work practices may relate to organizational CRM through employee engagement in Malaysian FinTech. Existing research has extended the TOE framework to cybersecurity adoption (Wallace et al., 2020), examined remote-work vulnerabilities (Nizamuddin, 2025) and reviewed trust and security in FinTech adoption (Jafri et al., 2024). These streams address different parts of the problem. What remains underspecified is the joint pathway: organizational and work-context conditions, an employee-level motivational mechanism, and an explicitly defined organizational risk-management outcome.

Evidence from Malaysia and the wider ASEAN region reinforces the need for such an account, while also showing that claims must be stated cautiously. Wan Abdullah and Hisamudin (2024) examined FinTech adoption in the Klang Valley, with attention to security, innovation and perceived benefits. Rattanapong et al. (2025) examined factors associated with cybersecurity investment in ASEAN organizations, while Ali et al. (2025) reviewed regional cybersecurity trends and challenges. Javaheri et al. (2024) synthesized FinTech threats and defenses. These studies contribute to understanding adoption, investment and threat management, but their foci differ from the combination proposed here. The novelty of this paper is therefore integrative rather than the invention of a wholly new theoretical mechanism. The paper's claim is that bringing TOE-informed organizational antecedents, JD-R-informed secure remote-work resources and employee engagement into one CRM-focused model for Malaysian FinTech produces a clearer, testable specification than treating these streams separately. That claim remains provisional until the propositions are examined empirically.

Accordingly, this paper develops a conceptual framework integrating the TOE framework and the Job Demands-Resources (JD-R) model. Technology adoption and the organizational implementation of regulatory requirements are treated as organizational antecedents informed by TOE. Secure remote-work practices are considered through JD-R as work-context resources that may support employee engagement and security-related conduct. Employee engagement is proposed as a mediator between these antecedents and CRM, while direct relationships are also proposed. Because the direction of the remote-work relationship is conditional on security arrangements, the framework refers to secure remote-work practices rather than assuming that remote work itself necessarily improves cybersecurity.

RQ1: How is organizational adoption of cybersecurity technology related to cybersecurity risk management in Malaysian FinTech?

RQ2: How is the implementation of cybersecurity-related regulatory requirements related to cybersecurity risk management in Malaysian FinTech?

RQ3: How are secure remote-work practices related to employee engagement and cybersecurity risk management?

RQ4: How is employee engagement related to cybersecurity risk management?

RQ5: Does employee engagement mediate the relationships between technology adoption, regulatory implementation and secure remote-work practices and cybersecurity risk management?

The paper proceeds as follows. The literature review defines CRM and synthesizes research on technology adoption, regulatory implementation, remote work and employee engagement. The theoretical section explains the complementary roles of TOE and JD-R. The subsequent sections develop the propositions and present the

conceptual framework, followed by theoretical and practical implications, directions for future research and a conclusion.

LITERATURE REVIEW

The review focuses on the five constructs included in the proposed framework. It first clarifies CRM as an organizational capability and then examines technology adoption, regulatory implementation, secure remote-work practices and employee engagement. The purpose is not to catalogue every related study, but to identify mechanisms, boundary conditions and limitations that motivate the proposed relationships.

Literature Review Approach

This paper uses a structured narrative review rather than a full systematic literature review with a registered protocol. The aim was to substantiate the constructs, research gaps and theoretical links sufficiently for a conceptual framework, and to make the search reproducible enough for readers to audit. Sources were identified through iterative searches in Google Scholar, Scopus and publisher platforms, supplemented by official Malaysian regulatory and institutional publications (BNM, NACSA, SC, CyberSecurity Malaysia and the Economic Planning Unit). Core keyword combinations covered cybersecurity risk management / capability; FinTech cybersecurity; technology adoption and TOE; regulatory implementation and technology-risk governance; remote / hybrid work and cyber risk; and employee engagement, security compliance and security fatigue. Preference was given to peer-reviewed journal articles and recognized working papers; recent systematic reviews were used as anchor sources for threat landscapes and remote-work vulnerabilities (for example, Javaheri et al., 2024; Nizamuddin, 2025; Cele & Kwenda, 2025; Jafri et al., 2024). Malaysian and ASEAN evidence was prioritized where available; when direct evidence was scarce, studies from other sectors or countries were retained only as theoretical or analogical support and are labelled as such in the proposition arguments. Inclusion required conceptual relevance to at least one framework construct or to the Malaysian FinTech setting; purely technical vulnerability papers without organizational or behavioural implications were excluded. This approach does not replace a protocol-based systematic review, but it makes the gap and originality claims inspectable and open to later update.

Cybersecurity Risk Management as an Organizational Capability

Cybersecurity risk management (CRM) has been conceptualized in different ways, including estimated financial losses, organizational preparedness, resilience, compliance and the effectiveness of technical controls. For example, Bouveret (2018) considers aggregate cyber losses, while Khan and Malaika (2021) discuss cybersecurity within central-bank and financial-sector risk management. Reviews of FinTech cybersecurity have focused on threats and mitigation measures (Ali et al., 2024; Javaheri et al., 2024). These approaches are related but not interchangeable: incident losses are outcomes of risk exposure, whereas organizational risk-management capability concerns the processes and resources used to anticipate, prevent, detect, respond to and recover from incidents.

The NIST Cybersecurity Framework 2.0 provides a useful organizing reference through its functions of Govern, Identify, Protect, Detect, Respond and Recover (National Institute of Standards and Technology [NIST], 2024). These functions emphasize that cybersecurity involves a coordinated set of governance and operational capabilities rather than a single control or the absence of reported incidents. ENISA (2022) similarly reviews risk-management standards and the methods used to implement them. Together, these sources support treating CRM as a multidimensional organizational capability.

In this paper, CRM is defined as the perceived organizational capability to govern cyber risk and to prepare for, prevent, detect, respond to and recover from cyber threats. Indicative measures-updated policies, regular training, a tested incident-response plan and integration of cybersecurity into organizational strategy-provide a starting point, but they do not fully represent all six NIST functions. Because survey-based CRM is largely perceptual, it raises common-method and level-of-analysis concerns when the same respondents also report engagement and antecedents. Future measurement should therefore consider governance, risk identification,

protection, detection, response and recovery; distinguish capability from compliance or incident frequency; and, where feasible, triangulate perceptions with organizational records or multiple informants.

The Financial Sector and the Malaysian Setting

In financial services, cyber risk is no longer handled as a purely technical matter. Crisanto et al. (2023) describe a second generation of regulatory approaches to bank cybersecurity that moves toward an assume breach view. These approaches cover strategy, governance, incident response, testing, third party risk, culture and workforce, though only a few jurisdictions have set workforce requirements so far. Khan and Malaika (2021), writing on central bank risk management, stress integrated risk management, a dedicated risk management unit, board and staff training and regular assessment of cyber resilience. Doerr et al. (2022) note that central banks have spent more on cyber since 2020, yet the ways they collect cyber incident data are still uneven. Customers feel the threats too. Cele and Kwenda (2025) reviewed 58 studies and found that malware, identity theft and phishing keep people away from digital banking.

The Malaysian studies keep coming back to people. Krishnan et al. (2023) studied 384 employees of a Malaysian bank and stressed security culture, training and awareness for protecting data. Ramalu et al. (2023) and Sulaiman et al. (2022), discussed earlier, point the same way. These studies agree that employee behavior affects cybersecurity in some form. Where they differ is on whether training is enough. Notice what they measure, though. Each one looks at individual behavior or awareness, not at how well the organization manages risk. Accordingly, in the studies reviewed here, the link between employee engagement and CRM in Malaysian FinTech has not been tested.

Technology Adoption

Most work on how organizations adopt technology leans on the TOE framework. Tornatzky and Fleischer (1990) introduced it to explain how technological, organizational and environmental contexts create constraints and opportunities for adoption, and Baker (2012) describes it as a foundational framework for adoption studies. Things change, though, when the technology is a security tool. Wallace et al. (2020) found that the traditional TOE framework misses some of the problems specific to cybersecurity, so they extended it with cyber catalysts and practice standards. Hasani et al. (2023) combined TOE with other adoption theories in a study of UK small and medium enterprises. They found eight factors that affect cybersecurity adoption and showed that adoption has a positive impact on organizational performance.

The effect on people is less clear cut. Molino et al. (2020) found that opportunities for information and training relate positively to technology acceptance, which in turn relates positively to work engagement. On the other hand, Pothuganti et al. (2025) found that technostress from workplace technology is associated with lower engagement and wellbeing among private bank employees. At the level of the firm, Catal et al. (2025) surveyed 44 managers and found that putting money into digital transformation while giving cybersecurity too little effort and resources may raise both the likelihood and the severity of breaches. In this paper, TA means something specific: the extent to which the organization accepts, uses and integrates cybersecurity technologies in its daily operations, with support from management and the readiness to take on new tools.

Regulatory Framework

In TOE terms, regulation is part of the environment that firms operate in. The regulatory framework refers to the laws, standards and supervisory expectations that govern how firms manage cybersecurity. In Malaysia that includes RMiT and the Cyber Security Act 2024 (BNM, 2025; NACSA, 2024). Yong et al. (2022) review the earlier Malaysian framework and show that both the Securities Commission's guidelines and RMiT set requirements for the governance of cyber risk, including the roles of directors and top management. Laws alone, however, say little about what happens inside a given firm. That is why this paper looks at RF as it shows up inside the firm: a clear governance framework that promotes compliance, compliance as a priority of top management, and regular assessment and monitoring of whether the rules are followed.

The relationship between regulation and cybersecurity outcomes is not necessarily uniform. Some evidence says it can. Malaivongs et al. (2022) find that cybersecurity performance is higher for firms in highly regulated industries than in less regulated ones. But rules are not uniformly applied, and there is still unevenness in cyber incident data collection even among central banks (Doerr et al., 2022). Formal requirements therefore need to be translated into effective organizational practices.

Remote Work

Remote work is work done outside the traditional office environment via digital means. This could be full time telework, hybrid arrangements or home working. Remote work affects where and how people access company systems and data. We can look at the literature from a demands and resources angle. Shared or insecure home networks, personal devices, weaker oversight, policy noncompliance, rushed transitions during the pandemic, and shadow IT are all demands. Clear policy, management support, adequate training, and technical tools such as VPNs and zero trust architectures are resources. Nizamuddin's (2025) review of 20 studies categorized remote work vulnerabilities into human, technical and organizational clusters. The biggest risk factor was human behavior. Solutions proposed were training, secure devices and networks, policy alignment, zero trust architecture and continuous monitoring.

This is also true of engagement. Galanti et al. (2021) surveyed 209 employees working from home. Family work conflict and social isolation were negatively related to engagement. Self leadership and autonomy were positively related to engagement. This relationship is relevant to cybersecurity research because The people who feel isolated or overwhelmed are the same people we rely on to comply with remote access policies. The same people we look to for spotting suspicious messages. So when we talk about RW in this paper, we are talking about more than just the arrangement. We are talking about how common remote access to company systems is. Awareness of the cyber risks of remote work. How secure their remote setups are. And whether they report suspicious activity when working remotely.

Employee Engagement

Engagement is mostly defined by the concepts of vigor, dedication and absorption in most studies of organizations. Security researchers apply a narrower notion of engagement that relates to the extent to which employees care about, comply with and sometimes go beyond security expectations. We adopt this more restricted notion of engagement. Cram et al. (2019), in their meta-analysis of 95 papers, found that attitude, personal norms, ethics and normative beliefs are among the strongest predictors of compliance, while punishment and rewards are among the weakest. Cram and D'Arcy (2023) add that the way employees judge the legitimacy of cybersecurity carries the effect of management support through to compliance. So employees need to see security initiatives as fair and reasonable.

Culture and fatigue fill in the rest of the picture. Goo et al. (2014) found that a security climate built on top management attention, policy, enforcement and awareness programs raises compliance intention. Delso-Vicente et al. (2025) found that top management support and organizational culture stand out, and that intrinsic and extrinsic motivators work best together. The darker side is fatigue. Cram et al. (2021) have highlighted that fatigue and low compliance may follow from security related demands. Hsu et al. (2024) have also shown that job and personal resources can ease that fatigue because they raise engagement. In this paper, EE is therefore defined as the degree to which employees are involved in and motivated to support the organization's cybersecurity activities. Engaged staff know the policies and why they matter. They feel trained and confident enough to spot threats. They are motivated to help and they follow the policies. In short, they can act as a human firewall.

Research Gaps

Three connected gaps motivate the framework. First, research on cybersecurity technology adoption and regulatory requirements does not consistently explain how these organizational conditions relate to CRM through an employee-level mechanism. Second, employee engagement and security-related behaviour are often examined as individual outcomes, while organizational CRM is conceptualized at a different level; the

relationship between these levels requires clearer theoretical specification and measurement design. Third, evidence from Malaysian FinTech remains fragmented across studies of adoption, employee behaviour, cybersecurity threats and regional investment, and much of the path-level evidence available for the propositions still comes from other sectors or countries. The present paper addresses these gaps by proposing an integrated, testable framework rather than by claiming that the individual constructs are new.

THEORETICAL FOUNDATION

The Technology-Organization-Environment Framework

The Technology-Organization-Environment (TOE) framework explains organizational innovation and technology adoption through technological, organizational and environmental contexts (Tornatzky & Fleischer, 1990; Baker, 2012). In cybersecurity, technological conditions include the availability and suitability of security tools; organizational conditions include resources, leadership and readiness; and environmental conditions include regulation and external expectations. Wallace et al. (2020) argue that cybersecurity adoption requires attention to factors beyond those captured by a conventional application of TOE. In the proposed framework, technology adoption and the organizational implementation of regulatory requirements are the two antecedents most directly informed by TOE.

The theoretical extension proposed here requires care. TOE was developed primarily to explain organizational adoption decisions, not to serve as a general explanation of all cybersecurity outcomes. This paper therefore uses TOE to explain why technological and environmental conditions may shape the organizational arrangements through which cybersecurity is managed. The proposed paths from those conditions to CRM are extensions to be tested, not relationships that TOE alone establishes.

The Job Demands-Resources Model

The JD-R model proposes that job resources can support motivation and engagement, while job demands may consume energy and contribute to strain (Bakker & Demerouti, 2017). Research applying JD-R to information security suggests that security demands can contribute to fatigue and that job and personal resources may reduce its effects (Hsu et al., 2024). Remote work is therefore best understood as a work arrangement whose consequences depend on accompanying demands and resources. Secure devices, reliable access controls, clear procedures, appropriate training and responsive support may enable employees to work remotely without unnecessary security burdens; inadequate resources may instead increase exposure and strain.

Why Employee Engagement Sits in the Middle

Employee engagement is proposed as a mediating mechanism because organizational arrangements influence outcomes partly through employees' interpretation and use of those arrangements. The JD-R perspective suggests that resources can support motivation, but engagement should not be treated as synonymous with cybersecurity compliance. Engagement concerns employees' energy, dedication and involvement; compliance refers to adherence to specific security requirements. The framework proposes that engaged employees may be more willing to understand, support and enact security practices, while recognizing that engagement alone cannot substitute for effective controls, adequate resources or organizational accountability.

Prior studies provide indirect support for this mechanism. Kraushaar and Bohnet-Joschko (2025) report a relationship between work engagement and information-security compliance in a healthcare setting, while Hsu et al. (2024) examine engagement in relation to security fatigue. Research on employee involvement in technology-enabled operational change also suggests that employee responses can help explain the relationship between organizational initiatives and outcomes (Tortorella et al., 2021). These findings come from different settings and do not establish the proposed mediation in Malaysian FinTech; rather, they provide a rationale for testing it.

The integrated framework thus assigns complementary, rather than interchangeable, roles to the theories. TOE informs the organizational conditions associated with technology adoption and regulatory implementation. JD-

R explains how work resources and demands may shape employee engagement in the security context. What is claimed as novel is not a new psychological mechanism inside JD-R or a replacement for TOE, but the specification of how these lenses jointly generate direct and engagement-mediated paths to CRM in Malaysian FinTech, with secure remote-work practices treated as resources rather than as remote work per se. Because CRM is an organizational-level construct, empirical testing should either obtain organization-level evidence or explicitly define the outcome as employees' perceptions of organizational CRM capability.

PROPOSITION DEVELOPMENT

The following propositions are theoretically motivated expectations, not established findings. Supporting studies are often drawn from other sectors or countries and sometimes examine related but non-identical constructs; they therefore provide analogical rather than conclusive support for Malaysian FinTech. The positive direction of each proposition is a hypothesis for future testing rather than a conclusion already demonstrated by the literature.

Technology Adoption and Employee Engagement

Technology and engagement is a mixed picture. For example, Molino et al. (2020) find (for 598 employees in an Italian firm) that opportunities for information and training relate positively to technology acceptance, which in turn relates positively to work engagement. In contrast, Pothuganti et al. (2025) find (for 388 private bank employees in India) that technostress is linked with lower engagement and wellbeing. Luo and Chen (2025) show that engagement from the adoption of intelligent machines is not just about the technology. It is about a mix of factors in the right ecosystem. For example, leadership empowerment. Kausar (2020) shows employee motivation is more about senior management support and participation in decision making. Tortorella et al. (2021) also show that the adoption of Industry 4.0 means you still need to get employees involved. Ter Hoeven et al. (2016) warn that technology at work can increase engagement through ease of access and efficiency, but it can decrease it through interruptions and unpredictability.

Negative findings typically concern everyday workplace technology that raises demands (technostress, interruptions and so on). Technology adoption here is narrower: cybersecurity technology that is supported by management and integrated into work. From a TOE perspective, that support is an organizational condition that can give staff resources and clarity to participate in security. From a JD-R perspective, those conditions function as job resources, which are the side of the model more often linked with engagement (Kausar, 2020; Molino et al., 2020). If the organization supports and encourages the use of such technologies, employees are more likely to have the resources and clarity to engage, instead of tiring out.

> **P1:** Organizational adoption of cybersecurity technology is positively associated with employee engagement.

Regulatory Framework and Employee Engagement

Rules can pull engagement either way. They set the ethical, procedural and operational boundaries of how employees work, so trust and fairness may lift engagement while rules that feel unfair may hold it back. Work on how firms are set up and run mostly points to positive links. Nienaber and Martins (2020) find that organizational strategy and implementation, organizational commitment and team commitment significantly predict engagement, and Saks (2006) finds that perceived procedural justice predicts organization engagement. Still, the picture has some nuance. Bakker and Demerouti (2017) note that job resources start motivation and also buffer the effect of job demands. Following this, frameworks that leave room for employees to act may raise engagement, while overly restrictive and bureaucratic ones may lower it. Borst et al. (2019), in a survey of 9,465 Dutch public servants, found that red tape changes how strongly job resources feed into work engagement.

Think of two employees. One works under rules that nobody explains. The other works where security is a stated top management priority, where the governance framework is clear and where compliance is checked regularly. The second person knows what is expected and why it matters. That is the sense of RF in this paper,

which views it from inside the firm. Rules framed this way give purpose, clarity and support, which is the side of the evidence that links structure to higher engagement (Nienaber & Martins, 2020; Saks, 2006). Few studies look at this link in the digital economy, and FinTech gets even less attention.

P2: The organizational implementation of cybersecurity-related regulatory requirements is positively associated with employee engagement.

Remote Work and Employee Engagement

How remote work is set up and run shapes much of its effect on engagement. Fatima et al. (2024) note that poorly managed remote work can lead to disengagement and lower motivation, and they flag weak communication as one cause. Galanti et al. (2021) show that autonomy is positively related to engagement when working from home. Other studies are more cautious. Gillet et al. (2021) describe remote working as a double edged sword: it buffered the negative effect of work centrality on family satisfaction, but it also limited its positive effect on work engagement. Wontorczyk and Rożnowski (2022) surveyed 544 remote, hybrid and onsite workers and found no significant difference in engagement between the groups, although relationships and social media use were the most important factors among remote workers. Leadership matters as well. Boccoli et al. (2024) show that transformational leadership and a supervisor's digital communication skills help keep remote staff engaged. Adisa et al. (2023), by contrast, found that work intensification, online presenteeism and insecurity held engagement back during pandemic remote work.

Where negative findings appear, they often come from the rushed shift to home working during the pandemic, when support for staff was thin (Adisa et al., 2023). Secure remote-work practices, as defined above, cover how common remote access is together with awareness of remote risks, a secure setup and reporting of suspicious activity. In JD-R terms these are resources, and resources such as autonomy and support are linked to higher engagement (Boccoli et al., 2024; Galanti et al., 2021). Engagement therefore depends largely on how remote work is supported, not on remote location alone.

P3: Secure remote-work practices are positively associated with employee engagement.

Employee Engagement and Cybersecurity Risk Management

Engagement is often named as something that makes a firm more resilient, yet few studies have put EE and CRM side by side. Engaged employees are more effective at building and endorsing a positive security culture. Tran et al. (2024) studied 330 public servants in Vietnam and found that cybersecurity awareness lifts motivation to protect information and protective behavior, and that organizational compliance builds that awareness. Cram and D'Arcy (2023), in a three wave survey of 529 employees, report that legitimacy judgements carry the effect of management support through to compliance. Staff who buy into the purpose of the controls, as engaged staff usually do, are less likely to see them as red tape. Goo et al. (2014) found much the same in a study of 581 participants, where a security climate built on top management attention, policy, enforcement and awareness programs raised employees' conformity with security policy.

The closest evidence links engagement to security outcomes directly. Kraushaar and Bohnet-Joschko (2025) found that work engagement had a significant positive effect on information security compliance. Hsu et al. (2024) found that job and personal resources cut fatigue and opportunistic security behavior by raising engagement. There is a caution here, though. Ramalu et al. (2023) found that awareness training was linked to more risky behavior, while security awareness and top management support were linked to less. Training on its own, then, does not guarantee better practice. So the focus here is on engagement, not just on attending training. A firm whose staff know the policies, feel trained and motivated, and follow the rules is expected to manage cyber risk better.

P4: Employee engagement is positively associated with perceived organizational cybersecurity risk-management capability.

Technology Adoption and Cybersecurity Risk Management

Not all effects have to go through people. For example, artificial intelligence, blockchain and big data technologies can enhance organizations' ability to predict, detect and respond to cyber threats. Saeed et al. (2023) pointed out that these technologies drive digital transformation, but they also bring new cyber risks. Therefore, they propose that cybersecurity readiness should be built step by step. In addition, Hasani et al. (2023) found that the adoption of cybersecurity technologies has a positive effect on organizational performance. However, technology adoption may also introduce additional risks. Catal et al. (2025) found that firms that invest in digital transformation but give cybersecurity too little effort and resources may face more likely and more severe breaches. Nifakos et al. (2021), reviewing 70 articles on healthcare cybersecurity, show that attacks have moved from exploiting IT infrastructure toward exploiting human vulnerability.

Much of the mixed evidence concerns digital technology in general, which can widen the attack surface. Technology adoption here is the use of cybersecurity technology, with management support and readiness to integrate it. In TOE terms, that readiness is the kind of organizational condition linked with better outcomes (Hasani et al., 2023), while neglecting security during broader digital investment raises breach risk (Catal et al., 2025). The same tools are what a firm relies on to detect and contain threats, so a direct positive association with CRM is also proposed.

> **P5:** Organizational adoption of cybersecurity technology is positively associated with perceived organizational cybersecurity risk-management capability.

Regulatory Framework and Cybersecurity Risk Management

Regulation can shape risk management directly. Yamada (2024), in a desk review of Japanese laws, states that stringent cybersecurity laws push corporations to adopt risk management strategies alongside cybersecurity frameworks and standards. Malaivongs et al. (2022) find that cybersecurity performance is higher in highly regulated industries than in less regulated ones. Buil-Gil et al. (2021) find that firms that invest in staff training and employ their own cybersecurity staff are less victimized than firms that rely only on basic software protection. Second generation regulations also focus on cyber resilience and give financial institutions specific tools to achieve it (Crisanto et al., 2023).

Regulation seems to help most when it is built into the firm's own governance, made a priority by top management and checked regularly. That is how RF is understood here, and so a positive direct link with CRM is expected through compliance, governance and reporting. One point needs care. RF and CRM are related, but they are not the same thing. RF asks whether the firm is set up to comply. CRM asks whether the firm is equipped to manage cyber risk, through current policies, regular training, a tested incident response plan and security built into strategy. A firm can tick every compliance box and still have an incident response plan that nobody has ever tested.

> **P6:** The organizational implementation of cybersecurity-related regulatory requirements is positively associated with perceived organizational cybersecurity risk-management capability.

Remote Work and Cybersecurity Risk Management

Remote work clearly changes cyber risk. Ozer et al. (2023), in a preprint that analyzes data breach notifications, report that incidents more than doubled after the shift to remote work. Yet the same body of work shows that these risks can be managed. Treacy et al. (2023) spoke with twenty industry experts and found that remote working risks span management, technical and human factors, and that organizations can mitigate them through policy, training and technical controls. Karayel et al. (2025), in a sample of 442 remote employees, found that the security measures companies put in place are significantly associated with their employees' cyber hygiene. Nizamuddin (2025) recommends training, device and network hygiene and policy alignment to reduce threats.

The question is therefore not whether remote work carries risk-it does-but whether the firm has the practices in place to handle it. Secure remote-work practices capture prevalence of remote access together with awareness,

secure setup and reporting. These are resources in JD-R terms. Remote arrangements could also affect CRM directly by changing the attack surface or how well controls work. Where remote work is well managed, a positive link with CRM is expected (Karayel et al., 2025; Treacy et al., 2023).

> **P7:** Secure remote-work practices are positively associated with perceived organizational cybersecurity risk-management capability.

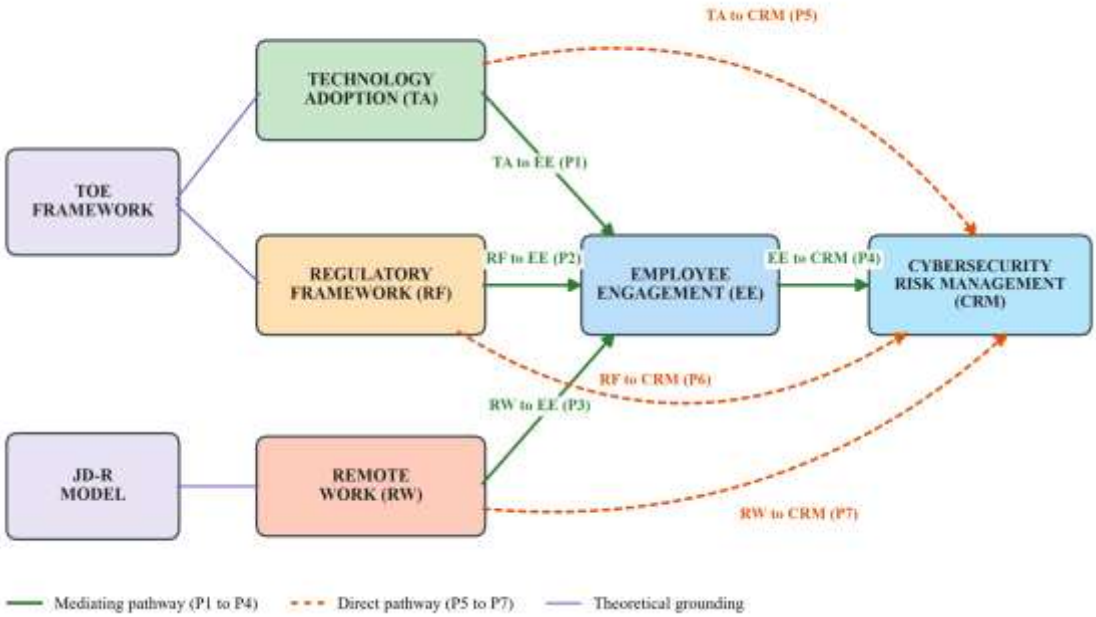
The Mediating Role of Employee Engagement

The proposed model also implies three indirect relationships: technology adoption, regulatory implementation and secure remote-work practices may each be associated with CRM through employee engagement. These indirect effects should be tested explicitly, rather than inferred solely because the relevant direct paths are included. Future empirical work should estimate each indirect effect and its confidence interval, while retaining the direct paths to determine whether mediation is partial, indirect-only or unsupported. The model does not assume in advance that mediation will be statistically significant.

CONCEPTUAL FRAMEWORK

Figure 1 summarizes the proposed relationships. Technology adoption and regulatory implementation are informed primarily by TOE, while secure remote-work practices and the motivational role of employee engagement are informed by JD-R. The model proposes direct paths from each antecedent to CRM and indirect paths through employee engagement. The propositions are conceptual expectations and require empirical validation; no claim is made that the seven paths have already been demonstrated in Malaysian FinTech.

Figure 1: Conceptual framework of cybersecurity risk management in Malaysian FinTech



Source: Adapted from the author's thesis framework, drawing on the TOE framework (Tornatzky & Fleischer, 1990; Wallace et al., 2020) and the JD-R model (Bakker & Demerouti, 2017).

Table 1. Propositions and supporting literature

Proposition	Path	Statement	Key sources
P1	TA → EE	Organizational adoption of cybersecurity technology is positively associated with	Molino et al. (2020); Kausar (2020); Tortorella et al. (2021); Ter Hoeven et al.

		employee engagement.	(2016)
P2	RI → EE	Organizational implementation of cybersecurity-related regulatory requirements is positively associated with employee engagement.	Nienaber and Martins (2020); Saks (2006); Bakker and Demerouti (2017); Borst et al. (2019)
P3	SRWP → EE	Secure remote-work practices are positively associated with employee engagement.	Galanti et al. (2021); Boccoli et al. (2024); Gillet et al. (2021); Adisa et al. (2023)
P4	EE → CRM	Employee engagement is positively associated with perceived organizational cybersecurity risk-management capability.	Kraushaar and Bohnet-Joschko (2025); Hsu et al. (2024); Cram and D'Arcy (2023); Goo et al. (2014)
P5	TA → CRM	Organizational adoption of cybersecurity technology is positively associated with perceived organizational cybersecurity risk-management capability.	Hasani et al. (2023); Saeed et al. (2023); Catal et al. (2025)
P6	RI → CRM	Organizational implementation of cybersecurity-related regulatory requirements is positively associated with perceived organizational cybersecurity risk-management capability.	Yamada (2024); Malaivongs et al. (2022); Buil-Gil et al. (2021)
P7	SRWP → CRM	Secure remote-work practices are positively associated with perceived organizational cybersecurity risk-management capability.	Karayel et al. (2025); Treacy et al. (2023); Nizamuddin (2025)

Table 2. Construct definitions and indicative measurement domains

Construct	Role	Definition	Indicative content
Technology adoption (TA)	Antecedent; TOE-informed	The extent to which the organization adopts and integrates cybersecurity technologies into routine operations, supported by organizational readiness and management commitment.	Use of cybersecurity technologies in routine operations; management support; integration with existing systems; maintenance and updating of tools.
Regulatory implementation (RI)	Antecedent; TOE-informed	The extent to which relevant cybersecurity laws, standards and supervisory expectations are translated into organizational governance and operating practices.	Clear assignment of responsibilities; procedures aligned with applicable requirements; regular assessment and monitoring; management review of compliance implementation.
Secure remote-work practices (SRWP)	Antecedent; JD-R-informed	The organizational and employee practices that support secure access to organizational systems when work is performed remotely or	Secure devices and networks; appropriate authentication and remote access controls; clear procedures; awareness of remote-work risks; reporting

		in hybrid settings.	of suspicious activity.
Employee engagement (EE)	Proposed mediator	Employees' energy, dedication and involvement in supporting work-related objectives, applied here to their willingness to participate constructively in cybersecurity activities.	Perceived importance of security; willingness to participate in security initiatives; motivation to raise concerns; sustained involvement in security-related activities. Avoid using compliance itself as an engagement item.
Cybersecurity risk-management capability (CRM)	Outcome	The perceived organizational capability to govern, identify, protect against, detect, respond to and recover from cybersecurity risks.	Cybersecurity governance and strategy; risk identification and assessment; preventive controls; monitoring and detection; tested incident response; recovery and continuous improvement.

Source: Definitions adapted from the author's thesis; indicative content summarizes the item themes developed for each construct.

The framework is intended for empirical examination using data from FinTech professionals, with sampling that distinguishes BNM- or SC-regulated institutions from other FinTech firms where possible. Individual respondents can report their own engagement and security-related behaviour, but may not have sufficient knowledge to assess organization-wide risk-management capability. Researchers should therefore define CRM as perceived organizational capability when using employee surveys, validate the measurement model, and address common-method bias through design remedies (for example, temporal separation, marker variables or multi-source ratings). Where feasible, perceptions should be triangulated with organizational records (incident-response tests, audit findings, governance artefacts) or with multiple respondents per firm. Constructs must also be kept distinct: secure remote-work practices should not be measured using general engagement or compliance items, and CRM items should not merely repeat regulatory-compliance indicators.

DISCUSSION AND IMPLICATIONS

Theoretical Implications

The first theoretical contribution is the proposed integration of TOE and JD-R around a CRM outcome in Malaysian FinTech. TOE offers an organizational lens on technology adoption and external requirements; JD-R explains how work resources and demands may influence employee engagement. The novelty is not a claim that either theory is new, nor that engagement has never been linked to security behaviour. It is the explicit multilevel specification that joins TOE-informed antecedents, secure remote-work resources and engagement-mediated paths to perceived CRM capability in one testable model for this setting.

The second contribution is the positioning of employee engagement as a potential mechanism linking organizational conditions to CRM. Prior studies provide related evidence on engagement, fatigue and security compliance, but do not by themselves establish that engagement mediates the proposed relationships in Malaysian FinTech. The framework makes this mechanism explicit and identifies indirect effects as empirical questions.

The third contribution is the proposed extension of TOE beyond the initial adoption decision. The framework asks whether adoption of cybersecurity technology and the implementation of regulatory requirements are associated with the capability to manage cyber risk after technology and governance arrangements have been established. This is a proposed extension and should be evaluated against alternative explanations, including organizational size, cybersecurity maturity and management commitment.

The fourth contribution concerns the treatment of remote work. Rather than assuming that remote work itself improves cybersecurity, the framework focuses on secure remote-work practices as potentially supportive

resources. This distinction acknowledges the dual nature of remote work: it can introduce vulnerabilities when controls are weak, but it can be managed through appropriate technology, procedures, training and organizational support.

Practical Implications

For FinTech managers, the framework suggests that cybersecurity investments should be evaluated as a combination of technical capability, governance and employee support. Security technologies need appropriate configuration, maintenance and integration with incident-response processes. Regulatory requirements should be translated into clear responsibilities, proportionate procedures and regular assessment. Employee engagement initiatives may complement these controls by helping staff understand the purpose of security practices and feel able to raise concerns. These are implications derived from the proposed framework; their relative effectiveness remains to be established empirically.

For regulators and supervisory bodies, the framework highlights the importance of considering implementation as well as formal requirements. Guidance may be more effective when organizations can translate it into operational responsibilities, appropriate resources, incident reporting and continuous improvement. The framework does not imply that employee engagement can replace regulatory oversight or technical safeguards; rather, it suggests that workforce factors merit attention alongside governance and technology.

DIRECTIONS FOR FUTURE RESEARCH

Because this manuscript is conceptual, a first priority is empirical testing of the seven propositions and the implied indirect effects. A pilot among professionals in Malaysian FinTech organizations should use validated measures where available, adapted cautiously to the cybersecurity context, and should assess reliability, convergent and discriminant validity, and the distinction between engagement, compliance behaviour and perceived organizational CRM capability. If partial least squares structural equation modelling is selected, the choice should be justified by prediction objectives, measurement characteristics and sample requirements. Indirect effects should be evaluated using bootstrapped confidence intervals.

Second, designs should reduce common-method and level-of-analysis bias. Preferred options include multiple respondents per organization, supervisor or security-officer ratings of CRM capability, and organizational records on incident response, audits and cybersecurity governance. Longitudinal or time-lagged surveys would further strengthen causal inference relative to single-wave perceptual designs.

Third, researchers should examine boundary conditions that may strengthen or weaken the proposed relationships, including organizational size, cybersecurity maturity, leadership support, quality of remote-work infrastructure and regulatory exposure. Comparing BNM- or SC-regulated financial institutions with other FinTech firms would clarify whether the same paths hold across the Malaysian FinTech boundary defined earlier. A later protocol-based systematic review could also update the gap map as the empirical literature grows.

CONCLUSION

This conceptual paper has proposed a framework for examining cybersecurity risk management in Malaysian FinTech through the complementary perspectives of TOE and JD-R. It links technology adoption, regulatory implementation and secure remote-work practices to perceived organizational CRM capability, with employee engagement proposed as a mediating mechanism. The paper does not offer empirical validation of the seven propositions; its contribution is an integrative specification for future testing, scoped to a sector that includes both regulated financial institutions and other FinTech firms.

The central argument is that cybersecurity risk management depends not only on technology and formal requirements but also on how organizational arrangements are implemented and supported by employees. Engagement should be treated as a potential mechanism rather than a substitute for technical safeguards, governance or accountability. Much of the supporting literature still comes from other settings, so conclusions

for Malaysian FinTech remain provisional. The framework's value will depend on clear construct measurement, multi-source or longitudinal designs that address perceptual bias, appropriate treatment of individual and organizational levels, and empirical assessment of the proposed relationships within the boundaries of Malaysian FinTech.

DECLARATIONS

Ethics statement: Not applicable. This conceptual paper did not involve human participants, human data or animals.

Conflict of interest: None.

Data availability statement: Not applicable. No new data were created or analyzed in this study.

Funding: UNITAR International University.

Acknowledgements: UNITAR International University.

REFERENCES

1. Adisa, T. A., Ogbonnaya, C., & Adekoya, O. D. (2023). Remote working and employee engagement: A qualitative study of British workers during the pandemic. Information Technology & People, 36(5), 1835-1850. https://doi.org/10.1108/itp-12-2020-0850
2. Ali, A. S., Zaaba, Z. F., Singh, M. M., Anuar, N. B., & Shariff, M. R. B. M. (2025). Advancing cybersecurity in ASEAN: Current trends, emerging challenges, and opportunities for enhanced resilience. International Journal of Information Security, 24(5), Article 200. https://doi.org/10.1007/s10207-025-01111-2
3. Ali, G., Mijwil, M. M., Buruga, B. A., & Abotaleb, M. (2024). A comprehensive review on cybersecurity issues and their mitigation measures in FinTech. Iraqi Journal for Computer Science and Mathematics, 5(3). https://doi.org/10.52866/ijcsm.2024.05.03.004
4. Baker, J. (2012). The technology-organization-environment framework. In Y. K. Dwivedi, M. R. Wade, & S. L. Schneberger (Eds.), Information systems theory: Explaining and predicting our digital society (Vol. 1, pp. 231-245). Springer. https://doi.org/10.1007/978-1-4419-6108-2_12
5. Bakker, A. B., & Demerouti, E. (2017). Job demands-resources theory: Taking stock and looking forward. Journal of Occupational Health Psychology, 22(3), 273-285. https://doi.org/10.1037/ocp0000056
6. Bank Negara Malaysia. (2024). Payment statistics [Data set]. https://www.bnm.gov.my/payment-statistics
7. Bank Negara Malaysia. (2025, November 28). Risk management in technology (RMiT) [Policy document; effective 28 November 2025, updated 25 September 2026]. https://www.bnm.gov.my/-/pd-rmit-nov25
8. Boccoli, G., Gastaldi, L., & Corso, M. (2024). Transformational leadership and work engagement in remote work settings: The moderating role of the supervisor's digital communication skills. Leadership & Organization Development Journal, 45(7), 1240-1257. https://doi.org/10.1108/lodj-09-2023-0490
9. Borkovich, D. J., & Skovira, R. J. (2020). Working from home: Cybersecurity in the age of COVID-19. Issues in Information Systems, 21(4), 234-246. https://doi.org/10.48009/4_iis_2020_234-246
10. Borst, R. T., Kruyen, P. M., & Lako, C. J. (2019). Exploring the job demands-resources model of work engagement in government: Bringing in a psychological perspective. Review of Public Personnel Administration, 39(3), 372-397. https://doi.org/10.1177/0734371x17729870
11. Bouveret, A. (2018). Cyber risk for the financial sector: A framework for quantitative assessment (IMF Working Paper No. 18/143). International Monetary Fund. https://doi.org/10.5089/9781484360750.001
12. Buil-Gil, D., Lord, N., & Barrett, E. (2021). The dynamics of business, cybersecurity and cyber-victimization: Foregrounding the internal guardian in prevention. Victims & Offenders, 16(3), 286-315. https://doi.org/10.1080/15564886.2020.1814468

13. Catal, C., Kar, G., & Zarali, M. (2025). Strategic technological innovation investment: Enhancing resilience in the age of digital transformation. Journal of Innovative Digital Transformation, 2(1), 50-72. https://doi.org/10.1108/jidt-05-2024-0010
14. Cele, N. N., & Kwenda, S. (2025). Do cybersecurity threats and risks have an impact on the adoption of digital banking? A systematic literature review. Journal of Financial Crime, 32(1), 31-48. https://doi.org/10.1108/jfc-10-2023-0263
15. Cram, W. A., & D'Arcy, J. (2023). 'What a waste of time': An examination of cybersecurity legitimacy. Information Systems Journal, 33(6), 1396-1422. https://doi.org/10.1111/isj.12460
16. Cram, W. A., D'Arcy, J., & Proudfoot, J. G. (2019). Seeing the forest and the trees: A meta-analysis of the antecedents to information security policy compliance. MIS Quarterly, 43(2), 525-553. https://doi.org/10.25300/misq/2019/15117
17. Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2021). When enough is enough: Investigating the antecedents and consequences of information security fatigue. Information Systems Journal, 31(4), 521-549. https://doi.org/10.1111/isj.12319
18. Crisanto, J. C., Pelegrini, J. U., & Prenio, J. (2023). Banks' cyber security: A second generation of regulatory approaches (FSI Insights No. 50). Bank for International Settlements. https://www.bis.org/fsi/publ/insights50.pdf
19. CyberSecurity Malaysia. (2025). Cyber incident quarterly summary report: Q1 2025 (Report No. SR-030.062025). MyCERT. https://www.mycert.org.my/portal/advisory?id=SR-030.062025
20. Delso-Vicente, A.-T., Diaz-Marcos, L., Aguado-Tevar, O., & de Blanes-Sebastián, M. G. (2025). Factors influencing employee compliance with information security policies: A systematic literature review of behavioral and technological aspects in cybersecurity. Future Business Journal, 11(1), Article 28. https://doi.org/10.1186/s43093-025-00452-7
21. Doerr, S., Gambacorta, L., Leach, T., Legros, B., & Whyte, D. (2022). Cyber risk in central banking (BIS Working Papers No. 1039). Bank for International Settlements. https://www.bis.org/publ/work1039.pdf
22. Economic Planning Unit. (2021). Malaysia digital economy blueprint. Prime Minister's Department. https://ekonomi.gov.my/sites/default/files/2021-02/Malaysia-digital-economy-blueprint.pdf
23. European Union Agency for Cybersecurity. (2022). Risk management standards: Analysis of standardisation requirements in support of cybersecurity policy. https://www.enisa.europa.eu/publications/risk-management-standards
24. Fatima, H., Javaid, Z. K., Arshad, Z., Ashraf, M., & Batool, H. (2024). A systematic review on the impact of remote work on employee engagement. Bulletin of Business and Economics, 13(2), 117-126. https://doi.org/10.61506/01.00306
25. Fintech News Malaysia. (2025a). Malaysia fintech report 2025. https://fintechnews.my/wp-content/uploads/2025/11/MY-Fintech-Report-2025.pdf
26. Fintech News Malaysia. (2025b, December 3). Digital banks in Malaysia hold RM3.1 billion in deposits, serve nearly 2 million users. https://fintechnews.my/55663/digital-banking-news-malaysia/malaysia-digital-banks/
27. Galanti, T., Guidetti, G., Mazzei, E., Zappalà, S., & Toscano, F. (2021). Work from home during the COVID-19 outbreak: The impact on employees' remote work productivity, engagement, and stress. Journal of Occupational and Environmental Medicine, 63(7), e426-e432. https://doi.org/10.1097/jom.0000000000002236
28. 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
29. Gillet, N., Huyghebaert-Zouaghi, T., Austin, S., Fernet, C., & Morin, A. J. S. (2021). Remote working: A double-edged sword for workers' personal and professional well-being. Journal of Management & Organization, 27(6), 1060-1082. https://doi.org/10.1017/jmo.2021.71
30. Goo, J., Yim, M.-S., & Kim, D. J. (2014). A path to successful management of employee security compliance: An empirical study of information security climate. IEEE Transactions on Professional Communication, 57(4), 286-308. https://doi.org/10.1109/tpc.2014.2374011

31. 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(5), Article 97. https://doi.org/10.1007/s43546-023-00477-6
32. Hsu, J. S., Hung, Y. W., Hsieh, P., & Chiu, C. (2024). Examining formation and alleviation of information security fatigue by using job demands-resources theory. Information Systems Journal, 34(6), 2132-2172. https://doi.org/10.1111/isj.12524
33. Jafri, J. A., Mohd Amin, S. I., Abdul Rahman, A., & Mohd Nor, S. (2024). A systematic literature review of the role of trust and security on Fintech adoption in banking. Heliyon, 10(1), e22980. https://doi.org/10.1016/j.heliyon.2023.e22980
34. Javaheri, D., Fahmideh, M., Chizari, H., Lalbakhsh, P., & Hur, J. (2024). Cybersecurity threats in FinTech: A systematic review. Expert Systems with Applications, 241, 122697. https://doi.org/10.1016/j.eswa.2023.122697
35. Karayel, T., Aktas, B., & Akbiyik, A. (2025). Human factors in remote work: Examining cyber hygiene practices. Information & Computer Security, 33(1), 96-116. https://doi.org/10.1108/ics-11-2023-0215
36. Kausar, S. (2020). Impact of senior management support, employees' involvement, and open corporate culture on the motivation of employees: An empirical study. Sukkur IBA Journal of Management and Business, 6(2), 99-113. https://doi.org/10.30537/sijmb.v6i2.439
37. Khan, A., & Malaika, M. (2021). Central bank risk management, fintech, and cybersecurity (IMF Working Paper No. 21/105). International Monetary Fund. https://doi.org/10.5089/9781513582344.001
38. Kraushaar, J., & Bohnet-Joschko, S. (2025). The role of the organization in promoting information security-related behavior among resident physicians in hospitals in Germany: Cross-sectional questionnaire study. Journal of Medical Internet Research, 27, e46257. https://doi.org/10.2196/46257
39. Krishnan, S. G., Al-Nahari, A., Ismail, N. A., & Yao, D. N. L. (2023). Enhancing cybersecurity awareness among banking employees in Malaysia: Strategies, implications, and research insights. International Journal of Academic Research in Business and Social Sciences, 13(8). https://doi.org/10.6007/ijarbss/v13-i8/17413
40. Luo, F., & Chen, L. (2025). How to enhance employee engagement in the AI era: An fsQCA-based study. Work, 80(3), 1167-1180. https://doi.org/10.1177/10519815241290285
41. Malaivongs, S., Kiattisin, S., & Chatjuthamard, P. (2022). Cyber trust index: A framework for rating and improving cybersecurity performance. Applied Sciences, 12(21), 11174. https://doi.org/10.3390/app122111174
42. Molino, M., Cortese, C. G., & Ghislieri, C. (2020). The promotion of technology acceptance and work engagement in Industry 4.0: From personal resources to information and training. International Journal of Environmental Research and Public Health, 17(7), 2438. https://doi.org/10.3390/ijerph17072438
43. National Cyber Security Agency. (2024). Cyber Security Act 2024 (Act 854). https://www.nacsa.gov.my/act854.php
44. National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST Cybersecurity White Paper No. 29). https://doi.org/10.6028/NIST.CSWP.29
45. Nienaber, H., & Martins, N. (2020). Exploratory study: Determine which dimensions enhance the levels of employee engagement to improve organisational effectiveness. The TQM Journal, 32(3), 475-495. https://doi.org/10.1108/tqm-05-2019-0151
46. Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of human factors on cyber security within healthcare organisations: A systematic review. Sensors, 21(15), 5119. https://doi.org/10.3390/s21155119
47. Nizamuddin, M. (2025). Investigating the cybersecurity risks of remote work: A systematic literature review of organizational vulnerabilities and mitigation strategies. International Journal of Information Security, 24(4), Article 187. https://doi.org/10.1007/s10207-025-01095-z
48. Ozer, M., Kose, Y., Bastug, M. F., & Kucukkaya, G. (2023). The shifting landscape of cybersecurity: The impact of remote work and COVID-19 on data breach trends [Preprint]. Research Square. https://doi.org/10.21203/rs.3.rs-3630534/v1
49. Pothuganti, S. K., P Ramachandra, G., & V, R. D. (2025). The impact of technostress on employee engagement and wellbeing. Human Systems Management, 44(5), 819-835. https://doi.org/10.1177/01672533251331503

50. Ramalu, S. S., Abidin, N. B. Z., Nadarajah, G., & Anuar, A. B. (2023). The determinants of risky cybersecurity behaviour: A case study among employees in water sector in Malaysia. Journal of Law and Sustainable Development, 11(12), e2706. https://doi.org/10.55908/sdgs.v11i12.2706
51. Rattanapong, P., Sukma, N., & Darakorn Na Ayuthaya, S. (2025). Determinants of cybersecurity investment in ASEAN organizations: An integrated structural equation modeling approach. Frontiers in Communications and Networks, 6, Article 1594554. https://doi.org/10.3389/frcmn.2025.1594554
52. Reeves, A., Delfabbro, P., & Calic, D. (2021). Encouraging employee engagement with cybersecurity: How to tackle cyber fatigue. Sage Open, 11(1), Article 21582440211000049. https://doi.org/10.1177/21582440211000049
53. Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. Sensors, 23(15), 6666. https://doi.org/10.3390/s23156666
54. Saks, A. M. (2006). Antecedents and consequences of employee engagement. Journal of Managerial Psychology, 21(7), 600-619. https://doi.org/10.1108/02683940610690169
55. Securities Commission Malaysia. (2024). Guidelines on technology risk management (SC-GL/2-2023 (R1-2024)). https://www.sc.com.my/regulation/guidelines/technology-risk
56. Sulaiman, N. S., Fauzi, M. A., Hussain, S., & Wider, W. (2022). Cybersecurity behavior among government employees: The role of protection motivation theory and responsibility in mitigating cyberattacks. Information, 13(9), 413. https://doi.org/10.3390/info13090413
57. Ter Hoeven, C. L., van Zoonen, W., & Fonner, K. L. (2016). The practical paradox of technology: The influence of communication technology use on employee burnout and engagement. Communication Monographs, 83(2), 239-263. https://doi.org/10.1080/03637751.2015.1133920
58. Tornatzky, L. G., & Fleischer, M. (1990). The processes of technological innovation. Lexington Books.
59. Tortorella, G., Miorando, R., Caiado, R., Nascimento, D., & Portioli Staudacher, A. (2021). The mediating effect of employees' involvement on the relationship between Industry 4.0 and operational performance improvement. Total Quality Management & Business Excellence, 32(1-2), 119-133. https://doi.org/10.1080/14783363.2018.1532789
60. Tran, D. V., Nguyen, P. V., Vrontis, D., Nguyen, S. T. N., & Dinh, P. U. (2024). Unraveling influential factors shaping employee cybersecurity behaviors: An empirical investigation of public servants in Vietnam. Journal of Asia Business Studies, 18(6), 1445-1464. https://doi.org/10.1108/jabs-01-2024-0058
61. Treacy, S., Sabu, A., Bond, T., O'Sullivan, J., Sullivan, J., & Sylvester, P. (2023). Organizational cybersecurity post the pandemic: An exploration of remote working risks and mitigation strategies. International Conference on Cyber Warfare and Security, 18(1), 394-401. https://doi.org/10.34190/iccws.18.1.973
62. Wallace, S., Green, K. Y., Johnson, C. M., Cooper, J. T., & Gilstrap, C. M. (2020). An extended TOE framework for cybersecurity adoption decisions. Communications of the Association for Information Systems, 47, 338-363. https://doi.org/10.17705/1cais.04716
63. Wan Abdullah, W. R., & Binti Hisamudin, I. N. A. (2024). Adoption of Fintech in Malaysia: An analysis of security, innovation, and perceived benefits. International Journal of Research and Innovation in Social Science, VIII(X), 2643-2658. https://doi.org/10.47772/ijriss.2024.8100221
64. Wontorczyk, A., & Rożnowski, B. (2022). Remote, hybrid, and on-site work during the SARS-CoV-2 pandemic and the consequences for stress and work engagement. International Journal of Environmental Research and Public Health, 19(4), 2400. https://doi.org/10.3390/ijerph19042400
65. Yamada, R. (2024). Impact of cybersecurity regulations on corporate compliance practices in Japan. International Journal of Law and Policy, 9(2), 28-38. https://doi.org/10.47604/ijlp.2705
66. Yaokumah, W., Brown, S., & Dawson, A. A. (2016). Towards modelling the impact of security policy on compliance. Journal of Information Technology Research, 9(2), 1-16. https://doi.org/10.4018/jitr.2016040101
67. Yong, F. Y. Y., Mohamad, A. M., & Sharon, G. (2022). Regulatory response to cybersecurity risks management in Malaysia: Case of worms and malware. Research in Management of Technology and Business, 3(2), 85-97. https://periodical.uthm.edu.my/index.php/rmtb/article/view/9622