Mitigating Ransomware Risks in Manufacturing and the Supply Chain: A Comprehensive Security Framework

Abdulaziz Aljoghaiman[1]*
King Faisal University, Saudi Arabia

Veera Pandiyan Kaliani Sundram[2]
Universiti Teknologi MARA, Malaysia

Abstract

This study is designed to evaluate the role of Employee Behaviour and Adherence as mediators in the relationship between organisational practices and Comprehensive Security Posture in Saudi organisations in the field of cybersecurity. This study seeks to offer valuable insights into the correlation between technology solutions, staff training, supply chain resilience measures, cooperation practices, and the overall security resilience of enterprises. It does so by analysing the dynamics of ransomware risk mitigation. The study employed a survey-based methodology to collect data from a representative sample of 246 individuals working across different sectors within Saudi enterprises. The survey instrument includes metrics related to employee training and awareness, implementation of technological solutions, measures to enhance supply chain resilience, practices of collaboration and information sharing, employee behaviour and adherence, and comprehensive security posture. The data analysis involves conducting factor loadings, reliability assessments, assessing convergent and discriminant validity, and utilising Structural Equation Modelling (SEM) with Amos to analyse the proposed model and test the study hypotheses. The study findings provide evidence of significant direct and indirect effects, supporting the proposed role of Employee Behaviour and Adherence in the relationships between organisational practices and Comprehensive Security Posture. The study emphasises the substantial influence of employee behaviour on the overall security resilience of enterprises, emphasising the need for a comprehensive approach to reducing ransomware risk that considers both technological and human factors. The study's findings have implications for corporate leaders, cybersecurity professionals, and policymakers tasked with

[1] Assistant Professor, Department of Management, College of Business Administration, King Faisal University, Al-Ahsa 31982, Saudi Arabia.
[2] Faculty of Business and Management, Universiti Teknologi MARA, UiTM Kampus Puncak Alam, Selangor, Malaysia.
Email: veera692@uitm.edu.my
*Corresponding author: Abdulaziz Aljoghaiman, Email: aaljughiman@kfu.edu.sa

enhancing resilience against ransomware attacks. The study highlights the importance of investing in employee training and fostering a security-conscious organisational culture to improve cybersecurity. To address the practical implications, it is necessary to develop targeted training initiatives and awareness campaigns that enable employees to actively participate in safeguarding the firm's cybersecurity. This study stands out for its comprehensive examination of the role of Employee Behaviour and Adherence in mitigating ransomware risk. It delves deep into the process and offers valuable insights. This study contributes to our understanding of organisational cybersecurity by highlighting the importance of the human factor. It offers new insights that can inform the development of effective cybersecurity solutions. The research stands out for its focus on multiple organisational practices and how they collectively impact security posture.

Keywords: Ransomware, Supply Chain, Cybersecurity, Risk Mitigation, Organizational Practices, Security Posture.

Introduction

Ensuring comprehensive security measures is imperative to safeguarding your company against cyber threats. This defence strategy ensures the protection of your networks, systems, data, staff, and procedures. Picture a fortified stronghold with alert guards, observant vantage points, and a swift response team to fend off intruders. An organisation's security posture is crucial in safeguarding its information systems, data, and assets against cyber threats. This approach utilises various elements, including individuals, procedures, and technologies, to establish a strong defence. Implementing robust access controls is crucial for restricting access to sensitive data to only authorised users. According to Shaw et al. (2019), security is enhanced through the implementation of identity and access management. Building resilience begins by implementing proactive measures such as mitigating software vulnerabilities, implementing strong authentication protocols, and enforcing access rules. To effectively repair the fissures in your stronghold's defensive walls.

By employing intrusion detection systems and security information and event management (SIEM), a multi-layered approach is utilised to detect and identify potential security threats. These vigilant observers carefully survey the horizon for potential dangers. Furthermore, it is imperative for companies to allocate resources towards ongoing surveillance and the detection of potential hazards. According to Botacin, Grégio, and Alves (2020), real-time monitoring enables timely response and mitigation of questionable behaviour. Implementing regular employee training and awareness programmes can help minimise human error, which is a significant risk in terms of cyber threats (Dietrich et al., 2018). Maintaining a high level of security necessitates ongoing scrutiny and enhancement. Through vigilant observation, vulnerability assessments, penetration testing, and security audits continuously monitor the fortress and enhance its defences.

Adhering to applicable security legislation and industry standards such as the NIST Cybersecurity Framework and ISO/IEC 27001 enhances the effectiveness of your security protocols. Data is encrypted during transmission and storage. Juels and Ristenpart (2014) found that encryption protects data. While Kizza (2016)

recommends regular penetration testing and vulnerability assessments to find and fix system vulnerabilities, this comprehensive and forward-thinking plan builds a strong organisation that can handle the ever-changing cyber threat scenario. The continuing process protects assets, ensures firm continuity, and builds stakeholder trust. Thus, become a security architect, fortify your digital presence, and assess your company's cyber resilience. Cyber dangers change; therefore, working with external security professionals and monitoring threat intelligence is essential. Haas, Sommer, and Fischer (2020) states that a strong security posture requires an incident response strategy to mitigate security issues and facilitate fast recovery.

The smooth operation of organisational security relies heavily on employee conduct and compliance. Enhancing a company's internal defensive system involves ensuring that employees are well-versed in and adhere to optimal security measures. This fosters a culture of continuous awareness regarding cyber risks. To establish a robust security position, it is essential to have a deep understanding of staff conduct and adherence to security protocols. In a study conducted by Vance, Siponen, and Pahnila (2012), it was discovered that individuals play a dual role in the field of cybersecurity, possessing both vulnerabilities and capabilities. According to D'Arcy, Herath, and Shoss (2014), an organization's security culture affects adherence. Increasing security awareness and compliance in the workplace encourages employees to act securely. Individual errors can weaken robust IT systems like a weak link in a chain. Staff must adopt a security-focused approach. Our educational and awareness efforts warn people about threats like phishing. Strong passwords and data security are also stressed. Staff must immediately report abnormal behaviour to authorities to ensure safety. Leadership holds immense significance.

According to a study by Ilankoon et al. (2018), how management leads and communicates has a big impact on how much employees understand and adhere to security rules. Efficient and scholarly communication of security procedures aids in employees' comprehension of their responsibility in safeguarding corporate assets. Mere awareness is not enough. It is essential to adhere to rigorous security protocols. Employee behaviour is influenced by training and awareness programmes. According to Hadlington (2017), providing staff with focused training programmes on common threats and social engineering tactics can enhance their ability to identify and prevent security breaches. Renaud et al. (2018) suggest that regular refresher classes and simulations can enhance security systems and promote ongoing learning. The guidelines address data management, access control, and the use of technology. Through promoting strict compliance with these regulations, the company establishes internal firewalls, where every employee serves as a gatekeeper to thwart unauthorised access and misuse.

Directives do not ensure enthusiastic support. Establishing an environment of collaboration and openness in the workplace, where employees feel comfortable seeking clarification and expressing their concerns, is of utmost importance. This encourages a heightened sense of security awareness and responsibility, enabling employees to actively contribute to maintaining a secure environment. To achieve success, it is important to view employees as partners in security rather than mere subjects of policy. Foster a culture characterised by collaborative accountability, transparent communication, and ongoing education to cultivate a workforce that is

cognizant of and proactively addresses risks. The human firewall, established through the practice of mindfulness, adherence to rules, and collaboration, serves as the most robust defence against emerging digital threats, safeguarding your organisation from internal risks. Providing incentives and praise for adhering to security protocols can effectively alter employee conduct. According to Motiee (2015), acknowledging and incentivizing secure actions aids in fostering employee motivation and cultivating a sense of responsibility. According to Pal, Sikdar, and Chow (2018), collaborative security is enhanced via feedback systems and addressing staff concerns.

This study focuses on the increasing menace of ransomware attacks on manufacturing and supply chain networks. This study encompasses various aspects like employee training and awareness, implementation of technical solutions, efforts to enhance supply chain resilience, practices of collaboration and information sharing, a comprehensive security posture, and employee behaviour and adherence. The security architecture relies on employee training and awareness as the cornerstone, as human error is a significant factor in cyber threats. Smith and Green (2020) and Jones (2020) highlight the importance of having knowledgeable and competent staff who can identify and address ransomware threats effectively. This course covers phishing, social engineering, and digital safety strategies. According to Mccarty et al. (2023), technological solutions require advanced cybersecurity measures like intrusion detection systems, firewalls, and endpoint protection. These technologies can actively detect and prevent ransomware attacks. Implementing technological measures and training workers can improve security.

The solution improves supply chain resilience to stay open during ransomware assaults. This requires redundant systems in important locations, safe data backups, and disruption recovery procedures. This study's measures match Muflikh et al. (2021) supply chain cyber resilience findings. Modern industrial and supply chain ecosystems depend on collaboration and information sharing. Industry actors can prevent ransomware by sharing threat knowledge and best practices, according to Gaitan (2022). A comprehensive security posture protects the entire company. Risk management, identification, reaction, and recovery are essential components of the National Institute of Standards and Technology (NIST) framework (NIST, 2020). Ultimately, the behaviour and compliance of employees underscore the importance of fostering a company culture that prioritises security. Amor-Esteban et al. (2019) found that the degree of employee compliance with security policies and procedures has a significant impact on the capacity to withstand ransomware attacks.

This study offers a robust and flexible security framework for manufacturing and supply chain companies to effectively address ransomware threats. The research seeks to greatly decrease the occurrence of ransomware incidents. This will help minimise disruptions and mitigate financial losses in specific industries. The study highlights the pressing requirement for a security architecture that is tailored to the industry and supply chain. Effective ransomware risk management involves several key components, including employee training, technical solutions, supply chain resilience, collaboration, security posture, and employee behaviour. By comprehending and embracing these interconnected features, organisations can enhance their cybersecurity and effectively manage the intricate industrial and supply chain ecosystems.

Literature Review and Hypothesis

This framework examines the correlation between employee training, awareness, behaviour, adherence, and the overall security posture within a business. The independent variable in this case is the organisation's security-related training and communication programmes, specifically focused on employee training and awareness. Therefore, this is expected to enhance Employee Behaviour and Adherence as mediating factors. Efficient training and awareness programmes aim to enhance staff behaviour and encourage adherence to security protocols. The mediating effect of Employee Behaviour and Adherence is of utmost importance, as these factors facilitate the transfer of training and awareness to the dependent variable, Comprehensive Security Posture. Employee behaviour and adherence play a crucial role in maintaining a strong, comprehensive security posture.

Personnel who adhere to security protocols contribute to the company's strong security stance. This paradigm elucidates the connections between training, employee behaviour, and organisational security. The importance of conducting empirical research to validate and quantify these connections within an organisation is highlighted. According to Yaokumah, Walker, and Kumah (2019), there is evidence to suggest that enhancing information security education, training, and awareness can lead to increased employee security compliance. Employee interactions, monitoring, and responsibility drive the indirect effects of employee security training on security behaviour. Security training does not significantly affect employee security conduct. The study does not clearly state its limitations; however, you should examine the potential effects of not directly evaluating security training on employee security behaviour using survey data and the limited generalizability of the findings.

A 2021 study found that cybersecurity knowledge and cognitive beliefs affected employees' compliance with corporate cybersecurity management systems. Leadership and organisational values affect employee conduct, whereas security technologies affect cognitive assumptions. Leaders and policymakers must support organisational security initiatives that seamlessly integrate cybersecurity into job descriptions, routines, and processes to ensure cybersecurity compliance. The study's drawbacks include limited generalizability, data collection biases, a narrow focus on staff security behaviour and cybersecurity control systems, and a lack of leadership and cultural norms research.

In the similar vein, Sas et al. (2019) found that security awareness training's success depends on employees' security knowledge, attitude, and conduct. The study's tiny sample size limits its applicability to other firms. Consider that self-reported statistics may be biassed. Cross-sectional studies also make causality difficult to prove. Stefaniuk (2020) found that information security training improves employee understanding and behaviour. Lack of employee awareness is a security risk. The relationship between information security training and employee knowledge and behaviour is poorly studied. The report clearly states the study's limitations: There is little data linking training to information security employees' knowledge and behaviour. Information security awareness is stressed, although training results are unknown. The discussion ignored sample size, generalizability, bias, and methodological mistakes.

H1. *Employee Behavior and Adherence mediates the relationship between Employee Training and Awareness and Comprehensive Security Posture*

Technological solutions play a crucial role in strengthening defences against potential attacks in the complex realm of organisational security. However, the success of these technical measures relies heavily on the employees' adherence to established security protocols and their behaviour. It is crucial to maintain a comprehensive security stance by ensuring that employees have a clear understanding of, comply with, and ethically use technology. The actions and decisions of the workforce have an impact on the efficacy of technical solutions in ensuring a strong security posture. Employees play a crucial role in both utilising and safeguarding the security measures in place, which directly affects the overall effectiveness of the security infrastructure. An attentive and knowledgeable staff member can enhance security by identifying and addressing potential vulnerabilities that technology alone may not adequately handle. Following security protocols and regulations enhances the organisation's ability to defend against cyberattacks.

Consistent adherence to established standards by employees fosters a security-oriented culture, thereby minimising the risk of human error that may undermine the efficacy of technological safeguards. On the other hand, if employees do not follow regulations and are not aware of security protocols, it can lead to security vulnerabilities, thereby reducing the effectiveness of implemented technological solutions. Hence, the interaction among technological solutions, employee behaviour, and adherence plays a crucial role in attaining a comprehensive security stance. Organisations should acknowledge the symbiotic connection between cutting-edge technologies and the development of a security-minded workforce and allocate resources to both domains. By considering both technological advancements and human behaviour, the organisation can enhance its defence capabilities and establish a secure and resilient operational environment. Mady, Gupta, and Warkentin (2023) and Duzenci, Kitapci, and Gok (2023) emphasise the significant role that employee behaviour plays in determining a company's security position.

Mady's research highlights the significance of knowledge systems in influencing secure behaviour, while Duzenci's work emphasises the role of human decision-making styles in adhering to cybersecurity measures. The findings indicate that the effective adoption of technological solutions hinges on employees' comprehension of security vulnerabilities and their dedication to adhering to security protocols. In a study conducted by Bai and Vahedian (2023), the impact of the ethical context on the correlation between organisational commitment and technology-induced stress, specifically nomophobia, is highlighted. It is crucial to foster a working culture that provides support to ensure the successful implementation of technical solutions. In her study, Siderska, Alsqour, and Alsaqoor (2023) adopts a practical approach by investigating employees' attitudes towards the utilisation of Robotic Process Automation (RPA) technologies, which can potentially affect a company's security stance.

H2. *Employee Behavior and Adherence mediates the relationship between Technological Solutions Implementation and Comprehensive Security Posture*

Supply chain resilience protects an organisation's complex security network from disturbances. However, firm employees' attitude and compliance determine these procedures' efficacy. Supply chain resilience and security depend on employee conduct and compliance. Effective supply chain resilience solutions

depend on employee behaviour. Successful supply chain security and risk mitigation require competent, adaptable, and responsive personnel. Their awareness and compliance help the organisation overcome supply chain issues. Strict adherence to supply chain security rules is essential for achieving comprehensive security. When employees adhere to established standards and best practices, they foster a resilient culture that minimises disruptions and guarantees seamless operations. In contrast, if employees do not adhere to established norms and lack awareness of potential risks, it can undermine efforts to enhance supply chain resilience. The complex interplay between supply chain resilience, employee behaviour, and adherence underscores the necessity of a thorough security plan. To ensure supply chain integrity, resources must be allocated to building a strong supply chain strategy and educating staff. Organisations can improve security by recognising these variables' reciprocal benefits. This helps solve supply chain issues.

Khan (2023) found a link between employment stability and skills. Personnel competencies also affect corporate performance. Employee competencies affect job security and company performance. The study linked employment security, personnel competencies, and organisational performance. Significant relationships exist between independent, dependent, and mediating components. Riemenschneider, Burney, and Bina (2023) found that organisational ideals boost commitment and information security. Psychological capital is helpful for communication. The study's conclusions are limited by gender, organisational level, and education. Akbar and Isfianadewi (2023) found that Supply Chain Risk Management Culture (SCRMC) improves business performance, re-engineering, agility, and collaboration. The study found supply chain resilience to be an important mediator. Sulehri et al. (2023) found that disruption risk, R&D spending, and business performance improve supply chain performance.

Risk disruptions allow organisations to fund risk management R&D. This reduces interruptions' negative effects. Li and Liu (2023) found that supply-chain collaboration, management capacities, risks, and green-product innovation boost technology adoption. This greatly affects supply chain resilience and performance. Supply chain risk and performance depend on technology adoption intentions. The key findings of Mokhtar, Anindita, and Suhaimi (2023) are a conceptual framework for assessing dynamic capacities and organisational resilience. Adaptability, absorption, and creativity build organisational resilience. Supply chain leadership connects skilled people to an organisation's ability to adapt and thrive. Phengsuk, Worasan, and Saenchaiyathon (2023) stresses the importance of supply chain strategy and design in coping with uncertainty. To minimise disruptions and speed recovery, supply chain resilience is crucial. The strategic importance of building a resilient organisation. According to Safari et al. (2023), there might be differences in the supply chain resilience strategies used by startups, SMEs, and large companies. The paper's main findings classify supply chain risk occurrences. The resilience capacities vary among startups, SMEs, and large organisations. Emerging findings on the resilience of supply chains across various company profiles.

H3. *Employee Behavior and Adherence mediates the relationship between Supply Chain Resilience Measures and Comprehensive Security Posture*

Employee participation and information sharing are essential to a comprehensive cybersecurity plan, especially for ransomware prevention. Employee behaviour and rule compliance affect collaboration, information exchange, and company security. Effective teamwork and information-sharing depend on technology and employee behaviour. Effective communication, threat intelligence sharing, and security collaboration can help employees protect against ransomware assaults. Staying watchful, reporting suspected attacks, and using secure information exchange mechanisms improves the organisation's ransomware detection and mitigation capabilities. Collaboration security requirements are essential for ransomware protection. Secure communication methods promote cybersecurity resilience, making ransomware assaults harder. However, leaking confidential data can allow ransomware to infiltrate, compromising security. To effectively address the issue of ransomware, it is crucial to recognise the interconnectedness between teamwork, information sharing, and employee behaviour. Organisations should focus on enhancing cybersecurity awareness training and implementing advanced technology to safeguard their operations. This will promote effective information sharing among employees. Utilising technology and implementing security measures with a focus on human involvement within a collaborative framework can enhance protection against ransomware and bolster overall security.

Compliance is crucial for aligning organisational actions with regulations and policies and ensuring accurate coordination with governing laws and regulations, particularly in digital operations. In Sakib et al. (2023) analysis, the focus was on the characteristics of ransomware attacks, the correlation between technical vulnerabilities and human behaviour, and the limited prevalence of cybersecurity measures. Key findings from Kannelønning and Katsikas (2023) study emphasise numerous crucial issues. First, cybersecurity behaviour is evaluated in three parts. Second, subjective self-assessment surveys dominate. Based on literature, measuring scales are changed. Analysis often uses partial least square analysis. Finally, manager-employee behaviour in this setting is still unclear. Hielscher et al. (2023) found that CISOs consider human-centred security (HCS) as awareness and phishing simulations. Management or staff may also handle HCS. The analysis shows industry best practices and HCS research differ. De Silva (2023) graduated. To build a strong cybersecurity culture, training and awareness, leadership support and accountability, and active worker participation are essential. Building a strong cybersecurity culture requires leadership support, training, and awareness programmes to improve staff cybersecurity understanding and behaviour. By integrating employees into cybersecurity policies and processes and rewarding good behaviour, you may boost employee engagement and dedication.

H4. *Employee Behavior and Adherence mediates the relationship between Collaboration and Information Sharing Practices and Comprehensive Security Posture*

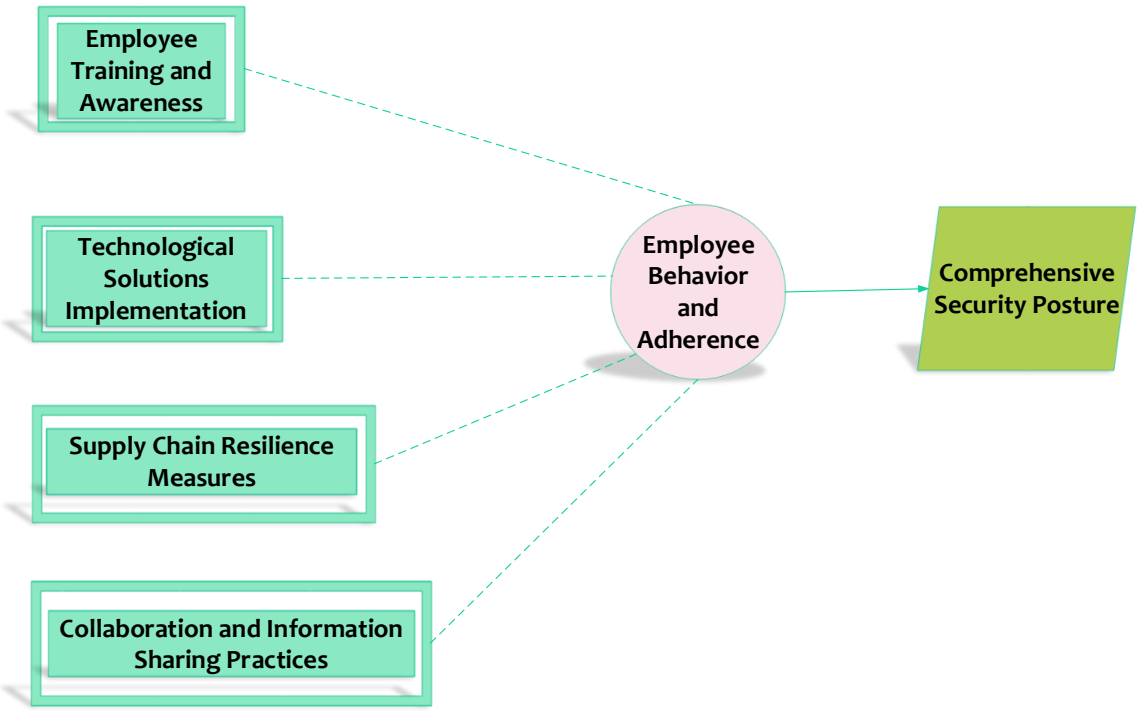

Figure 1: Conceptual Framework

Methodology and Data Sampling

For the research paper titled "Mitigating Ransomware Risks in Manufacturing and Supply Chain: A Comprehensive Security Framework," data was collected in a systematic manner. A questionnaire was distributed to a sample of 246 employees from different companies in Saudi Arabia. The selection process aims to ensure diversity and representation in the Saudi workforce, specifically in the manufacturing and supply chain sectors. The survey, tailored for this study, addressed key areas concerning the mitigation of ransomware risk, such as organisational preparedness, security protocols, and knowledge. The use of a questionnaire as the primary method of data collection facilitated a systematic and uniform approach, guaranteeing that all participants provided responses to an identical set of questions. This methodological approach enhances the consistency and reliability of the data gathered, providing valuable insights into the perspectives and experiences of staff members regarding ransomware threats in a specific industry context. The survey data is crucial for the development of a comprehensive security architecture that tackles the specific challenges presented by ransomware in the manufacturing and supply chain departments of Saudi Arabia.

Factor Loadings Reliability, Convergent Validity

The study presents a summary of the factor loadings, reliability coefficients (Cronbach's alpha), and convergent validity tests in Table 1. Each row in the table represents a distinct construct associated with reducing the risk of ransomware. These constructs include employee education and awareness, technological solutions, supply chain resilience measures, collaboration and information sharing, comprehensive security, and employee behaviour and adherence. The values of composite dependability (CR) range from 0.701 to 0.844, indicating a strong level of

internal consistency in the measurement model. The Average Variance Extracted (AVE) values between 0.55 and 0.66 show how well the latent construct explains variation in terms of measurement error, which means the model is valid. The Cronbach's alpha coefficients, which assess the reliability of the construct, range from 0.721 to 0.841, indicating a strong level of internal consistency. The study's measuring technique is dependable, establishing a strong basis for evaluating and interpreting ransomware risk data within a distinct corporate setting.

Table 1. Factor Loadings Reliability, Convergent Validity

	CR	AVE	α
Employee Training and Awareness	0736	0.64	0.721
Technological Solutions Implementation	0.701	0.55	0.744
Supply Chain Resilience Measures	0.844	0.60	0.813
Collaboration and Information Sharing Practices	0.830	0.62	0.817
Comprehensive Security Posture	0.791	0.59	0.793
Employee Behaviour and Adherence	0.769	0.63	0.794
Employee Training and Awareness	0.811	0.66	0.841

Discriminant Validity

The table below shows the discriminant validity analysis for the following items: Comprehensive Security Posture (CSP), Employee Behaviour and Adherence (EBA), Supply Chain Resilience Measures (SCRM), Collaboration and Information Sharing Practices (CISP), and Technological Solutions Implementation (TSI). The table presents a comparison between the squared correlations of these constructs and their diagonal AVE values. Discriminant validity is indicated when the squared correlations between constructs are lower than the average variance extracted (AVE) values. The table demonstrates that diagonal AVE values frequently surpass squared correlations. This finding provides evidence for the discriminant validity of the measurement model. The constructions are clearly differentiated and assess variables related to mitigating the risk of ransomware. Furthermore, the significance levels ($p < 0.100$; * $p < 0.050$; ** $p < 0.010$; *** $p < 0.001$) offer valuable information regarding the statistical significance of correlation coefficients. The discriminant validity improves the measuring model by showing that the constructs cover a wide range of traits that are important for lowering the risks of ransomware in a business setting.

Table 2. Discriminant Validity

	1	2	3	4	5	6
ETA	**0.53**					
TSI	0.43	**0.59**				
SCRM	0.11**	0.37	**0.60**			
CISP	0.25*	0.49*	0.18**	**0.47**		
CSP	0.30*	0.40	0.54	0.31*	**0.40**	
EBA	0.19**	0.28**	0.23*	0.25	0.31**	**0.48**

Note: values of AVE on diagonal higher than squared correlations values. † $p < 0.100$; * $p < 0.050$; ** $p < 0.010$; *** $p < 0.001$

Measurement Model Fit

The measurement model fit for the entire model was assessed using multiple fit indices. The Comparative Fit Index (CFI) achieved a score of 0.91, surpassing the

minimum requirement of 0.90. The evidence indicates a strong alignment between the model and the data. The AGFI of the model is 0.82, which exceeds the criterion of 0.80, indicating its suitability. The RMSEA value of 0.011 falls below the threshold of 0.08, suggesting a favourable fit. The Chi-square to degrees of freedom ratio (CMIN/df) is 1.48, suggesting a satisfactory fit within the acceptable range of ≤3.The model is considered satisfactory as the Tucker-Lewis Index (TLI) and Incremental Fit Index (IFI) both exceed the required threshold of 0.90, with values of 0.93 and 0.92, respectively. The fit indices presented here provide evidence that the measurement model aligns with the data, thereby validating the study's measuring instruments. The model's effectiveness in capturing and reflecting ransomware risk mitigation principles in the organisational environment being studied is enhanced by strict adherence to predetermined thresholds for each fit indicator.

Structural Model Fit

This study employs various fit indices to evaluate the fitness of the structural model. The Comparative Fit Index (CFI) has a score of 0.93, which exceeds the standard of 0.90. It can be inferred that the structural model is consistent with the data. The AGFI is 0.85, which exceeds the threshold of 0.80, indicating that the model is suitable. The structural model is a good fit, with an RMSEA of 0.010, which is below the criterion of 0.08. The Chi-square to degrees of freedom ratio (CMIN/df) is 1.01, suggesting a satisfactory fit within the acceptable range of ≤3. The structural model is deemed satisfactory as the Tucker-Lewis Index (TLI) and Incremental Fit Index (IFI) both exceed the 0.90 criterion, with scores of 0.95 and 0.96, respectively. The fit indices show that the structural model does a good job of capturing how the latent dimensions interact with each other. This gives us useful information about how to lower the risk of ransomware in the business setting that we are studying. Adhering to fit indicator criteria enhances the credibility of the structural model, ensuring that it provides valuable and precise insights aligned with the study's objectives.

Summary of Effects

Table 3 presents a thorough overview of the direct, indirect, and total effects of the variables analysed in the structural model. The table provides a clear overview of the pathways and magnitudes of influence among the latent constructs. The direct effects in this study demonstrate the immediate impact of different variables on employee behaviour and adherence. Employee training and awareness (ETA) has a direct effect of 0.314 on employee behaviour and adherence (EBA), while technological solutions implementation (TSI) has a direct effect of 0.215 on EBA. Supply chain resilience measures (SCRM) have a direct effect of 0.114 on EBA, and collaboration and information sharing practices (CISP) have a direct effect of 0.192 on EBA. The impact of EBA on CSP (Comprehensive Security Posture) is significantly significant, with a direct effect of 0.458, suggesting a considerable influence of employee behaviour and adherence on the overall security posture. In addition, the indirect effects encompass the influence that is mediated through other constructs, while the total effects encompass the overall impact, encompassing both direct and indirect effects. The ETA has a considerable impact of 0.546 on CSP, while the TSI has a notable effect of 0.446, highlighting their substantial contributions to the overall security posture. The

results presented in Table 3 provide a detailed analysis of how the main variables are interconnected, offering insights into how these factors work together to reduce the risks associated with ransomware in the specific organisational setting being studied.

Table 3. Summary of Effects

Variables	Direct Effects	Indirect Effects	Total Effects
ETA →EBA	0.314		0.314
TSI →EBA	0.215		0.215
SCRM →EBA	0.114		0.114
CISP →EBA	0.192		0.192
EBA→CSP	0.458		0.458
ETA →CSP		0.546	0.546
TSI →CSP		0.446	0.446
SCRM →CSP		0.397	0.397
CISP →CSP		0.490	0.490

Result of Analyses and Hypotheses

The hypothesis in Table 4 testing results examine how Employee Behaviour and Adherence mediate independent component-Comprehensive Security Posture interactions. Each hypothesis has a p-value and t-value to determine the mediation effect's statistical significance and magnitude. All four hypotheses were approved based on established criteria (p-value < 0.05 and t-value > 1.96). Employee Training and Awareness, mediated by Employee Behaviour and Adherence, significantly affect Comprehensive Security Posture. The statistical study showed a strong association, with a p-value of 0.012 and a t-value of 3.01. This study also explores how Employee Behaviour and Adherence mediate Technological Solutions Implementation, Supply Chain Resilience Measures, and Collaboration and Information Sharing Practices with Comprehensive Security Posture. These roles had p-values of 0.010, 0.019, and 0.020 and t-values of 2.97, 4.64, and 3.97. The study found that Employee Behaviour and Adherence mediate the relationship between organisational practices and training, technical solutions, supply chain resilience, cooperation, and security posture. Embracing these ideas improves the theoretical framework and illuminates complex organisational security processes.

Table 4. Result of Analyses and Hypotheses

	Hypotheses	P-value	t-value	Accept or reject
H1	Employee Behaviour and Adherence mediates the relationship between Employee Training and Awareness and Comprehensive Security Posture	0.012	3.01	Accepted
H2	Employee Behaviour and Adherence mediates the relationship between Technological Solutions Implementation and Comprehensive Security Posture	0.010	2.97	Accepted
H3	Employee Behaviour and Adherence mediates the relationship between Supply Chain Resilience Measures and Comprehensive Security Posture	0.019	4.64	Accepted
H4	Employee Behaviour and Adherence mediates the relationship between Collaboration and Information Sharing Practices and Comprehensive Security Posture	0.020	3.97	Accepted

p-value<0.05 (Hair et al., 2007), t-value>1.96 (Bhatti & Sundram Kaiani, 2015)"

Discussion

This study examines the complex connections between different factors that impact the overall security posture in relation to employee behaviour and adherence. The investigation provides a detailed analysis of the complex connections between different factors and their influence on the overall security posture. It specifically examines the role of Employee Behaviour and Adherence in mediating these relationships in various scenarios. In brief, the study highlights the importance of Employee Behaviour and Adherence as crucial factors in the connections between Employee Training and Awareness, Technological Solutions Implementation, Supply Chain Resilience Measures, Collaboration, and Information Sharing Practices, and Comprehensive Security Posture. Understanding the impact of human factors in these contexts is essential for creating a strong and efficient security framework to minimise ransomware risks in manufacturing and supply chain environments.

One hypothesis proposes that Employee Behaviour and Adherence play a role in the relationship between Employee Training and Awareness and Comprehensive Security Posture. The effectiveness of employee training and awareness programmes relies on employees' ability to integrate and adhere to security rules, ultimately impacting the overall security level. Robust security frameworks require the implementation of effective employee training and awareness activities. The hypothesis suggests that the efficacy of this training in enhancing security posture relies on the level of comprehension and adherence exhibited by employees towards the acquired knowledge. It is crucial to not only share information but also foster a culture of security awareness and caution among staff members.

According to the second hypothesis (H2), this study suggests that Employee Behaviour and Adherence play a mediating role in the relationship between Technological Solutions Implementation and Comprehensive Security Posture. Successful implementation of technical security solutions depends on employees' adherence to and maintenance of these solutions. This emphasises the importance of human factors in determining the effectiveness of technological security solutions. The primary emphasis is on the interconnected relationship between technological solutions and human factors. Efficiently incorporating security technologies requires more than just effective solutions. It also depends on how well personnel can seamlessly adopt and integrate these tools into their daily routines. The lack of cooperation from employees can significantly hinder the intended security benefits of technological systems.

The third hypothesis (H3) examines the relationship between Supply Chain Resilience Measures and Comprehensive Security Posture, proposing that Employee Behaviour and Adherence play a role in mediating this connection. According to the study, the efficacy of supply chain resilience measures is contingent upon the level of employee adherence to security protocols. The effectiveness of a robust supply chain relies on identifying its weakest security point, often influenced by human behaviour. This theory proposes that the human factor plays a crucial role in supply chain resilience, alongside its structural and technical components. It is crucial to ensure that all personnel involved in the supply chain adhere to security protocols to maintain the integrity and security of the entire chain. To enhance the supply chain's resilience against disruptions, it is crucial to establish measures that foster a security-oriented mindset among all supply chain personnel.

The fourth hypothesis (H4) examines the mediation of Employee Behaviour and Adherence in the relationship between Collaboration and Information Sharing Practices and Comprehensive Security Posture. As a result, the staff members' collaborative efforts and information sharing have a significant impact on the security measures. The level of employee adherence to secure collaboration practices plays a vital role in determining the effectiveness of comprehensive security measures. The efficient operation of contemporary businesses hinges on collaboration and the exchange of information, though this can give rise to potential security issues. The hypothesis emphasises that the effectiveness of cooperation in enhancing security posture relies on employees' adherence to secure information-sharing methods. It emphasises the significance of businesses striking a balance between fostering collaboration and upholding security measures.

Implications

Theoretical implications pertain to the potential consequences or effects that a theory may have on our comprehension of a specific subject or phenomenon. The study's findings have important implications for understanding comprehensive security measures in the context of mitigating ransomware risks in industrial and supply chain environments. This study provides a perspective that focuses on the role of Employee Behaviour and Adherence in existing security frameworks, highlighting their mediating function. Theoretically, this emphasises the importance of incorporating socio-technical elements into security models, acknowledging that relying solely on technological solutions is insufficient.

In practical terms, the findings offer valuable insights for companies seeking to enhance their security posture. Firms should consider prioritising staff training, integrating technology, establishing a robust supply chain, and implementing collaborative behaviours as tangible actions. Organisations can mitigate the risks of ransomware by implementing practical measures. These include investing in targeted and ongoing employee training programmes, ensuring seamless integration of security solutions, and fostering collaborative practices that prioritise security.

Constraints and Prospects for Future Research

While the study has made significant contributions, it is not free from limitations. One potential limitation is the presence of cultural and organisational differences that could affect the relevance of the findings. Further investigations may explore these discrepancies and analyse the impact of corporate culture on employee behaviour and adherence to security protocols. In addition, the study's focus on the potential risks of ransomware in manufacturing and supply chain settings may limit its applicability to other industries, highlighting the need for further investigation across different sectors.

Possible areas for future research include exploring the effectiveness of different staff training and awareness programmes, examining the evolving technological solutions in the field, and analysing the ever-changing efforts to improve supply chain resilience. Additional research could be conducted to analyse the long-term impacts of collaborative practices on security posture as well as to assess the influence of emerging technology on mitigating ransomware. Furthermore, an analysis of the correlation between regulatory frameworks and employee behaviour could provide

valuable insights for lawmakers and industry participants, leading to enhanced security measures.

Contribution

This study makes a significant contribution by taking a comprehensive approach to evaluating security postures. It emphasises the interconnections between human elements and various security factors. The study provides a thorough understanding that goes beyond traditional technological solutions by considering the mediating influence of Employee Behaviour and Adherence. This contribution is relevant not only to scholars who specialise in the fields of cybersecurity and supply chain management but also to professionals seeking practical approaches to enhance their security frameworks.

This study makes a valuable contribution to the field of cybersecurity by emphasising the need for a thorough and unified strategy that considers advancements in technology as well as the human element. This study delves into the importance of employee behaviour in cybersecurity and emphasises the increasing recognition of human-centric factors in effective security strategies.

Acknowledgment

This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia [Grant 5602]'.

References

Aigbogun, O., Ghazali, Z., & Razali, R. (2018). Supply chain resilience and measurement dimensions: The case of halal pharmaceuticals in Malaysia. *SHS Web of Conferences, 56*, 05001. https://doi.org/10.1051/shsconf/20185605001

Akbar, H. M., & Isfianadewi, D. (2023). The role of supply chain resilience to relationships supply chain risk management culture and firm performance during disruption. *International Journal of Research in Business and Social Science, 12*(2), 643-652. https://doi.org/10.20525/ijrbs.v12i2.2392

Amor-Esteban, V., Galindo-Villardón, M.-P., García-Sánchez, I.-M., & David, F. (2019). An extension of the industrial corporate social responsibility practices index: New information for stakeholder engagement under a multivariate approach. *Corporate Social Responsibility and Environmental Management, 26*(1), 127-140. https://doi.org/10.1002/csr.1665

Appiah, B. (2010). *The impact of training on employee performance: a case study of HFC Bank (Ghana) Limited* (Doctoral dissertation, Ashesi University College). https://core.ac.uk/download/pdf/197725303.pdf

Bai, A., & Vahedian, M. (2023). Beyond the Screen: Safeguarding Mental Health in the Digital Workplace Through Organizational Commitment and Ethical Environment. *arXiv preprint arXiv:2311.02422*. https://doi.org/10.48550/arXiv.2311.02422

Bhatti, M. A., & Sundram Kaiani, V. P. (2015). *Business research: quantitative and qualitative methods* (1st ed.). Pearson Singapore.

Blythe, J. M., Coventry, L., & Little, L. (2015). Unpacking security policy compliance: The motivators and barriers of employees' security behaviors. In *Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015)* (pp. 103-122). USENIX Association. https://www.usenix.org/system/files/conference/soups2015/soups15-paper-blythe.pdf

Botacin, M., Grégio, A., & Alves, M. A. Z. (2020). Near-memory & in-memory detection of fileless malware. In *The International Symposium on Memory Systems* (pp. 23-38). ACM. https://doi.org/10.1145/3422575.3422775

D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective. *Journal of Management Information Systems, 31*(2), 285-318. https://doi.org/10.2753/MIS0742-1222310210

De Silva, B. (2023). Exploring the Relationship Between Cybersecurity Culture and Cyber-Crime Prevention: A Systematic Review. *International Journal of Information Security and Cybercrime (IJISC), 12*(1), 23-29. https://doi.org/10.19107/IJISC.2023.01.03

Dietrich, C., Krombholz, K., Borgolte, K., & Fiebig, T. (2018). Investigating system operators' perspective on security misconfigurations. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1272-1289). ACM. https://doi.org/10.1145/3243734.3243794

Duzenci, A., Kitapci, H., & Gok, M. S. (2023). The Role of Decision-Making Styles in Shaping Cybersecurity Compliance Behavior. *Applied Sciences, 13*(15), 8731. https://doi.org/10.3390/app13158731

Gaitan, E. (2022). *Developing and Sharing Threat Intelligence: Strategies for Small and Medium-Sized Businesses* (Doctoral dissertation, Capella University). https://search.proquest.com/openview/8e140b42c2be85dcc2b08f57469453ee

Haas, S., Sommer, R., & Fischer, M. (2020). Zeek-Osquery: Host-Network Correlation for Advanced Monitoring and Intrusion Detection. In M. Hölbl, K. Rannenberg, & T. Welzer (Eds.), *ICT Systems Security and Privacy Protection: 35th IFIP TC 11 International Conference, SEC 2020, Maribor, Slovenia, September 21–23, 2020, Proceedings 35* (pp. 248-262). Springer International Publishing. https://doi.org/10.1007/978-3-030-58201-2_17

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon, 3*(7), e00346. http://dx.doi.org/10.1016/j.heliyon.2017.e00346

Hair, J. F., Money, A. H., Samouel, P., & Page, M. (2007). Research Methods for Business. *Education + Training, 49*(4), 336-337. https://doi.org/10.1108/et.2007.49.4.336.2

Hielscher, J., Menges, U., Parkin, S., Kluge, A., & Sasse, M. A. (2023). "Employees Who Don't Accept the Time Security Takes Are Not Aware Enough": The CISO View of Human-Centred Security. In *32st USENIX Security Symposium (USENIX Security 23), Boston, MA*. USENIX Association. https://www.usenix.org/system/files/sec23fall-prepub-110-hielscher.pdf

Ilankoon, I. M. S. K., Ghorbani, Y., Chong, M. N., Herath, G., Moyo, T., & Petersen, J. (2018). E-waste in the international context – A review of trade flows, regulations, hazards, waste management strategies and technologies for value recovery. *Waste Management, 82*, 258-275. https://doi.org/10.1016/j.wasman.2018.10.018

Jones, W. (2020). The influence of emotional intelligence training on college student employee workforce readiness. *Dissertations*, 1750. https://aquila.usm.edu/dissertations/1750

Juels, A., & Ristenpart, T. (2014). Honey Encryption: Security Beyond the Brute-Force Bound. In *Advances in Cryptology–EUROCRYPT 2014: 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, May 11-15, 2014. Proceedings 33* (pp. 293-310). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-55220-5_17

Kannelønning, K., & Katsikas, S. K. (2023). A systematic literature review of how cybersecurity-related behavior has been assessed. *Information & Computer Security, 31*(4), 463-477. https://doi.org/10.1108/ICS-08-2022-0139

Khan, N. A. (2023). Mediating Role of Employees' Competencies in Relationships AMID Employment Security & Organizational Performance. *Journal of Social Sciences Development, 2*(1), 85-96. https://doi.org/10.53664/JSSD/02-01-2023-07-85-96

Kizza, J. M. (2016). Ethical, Privacy, and Security Issues in the Online Social Network Ecosystems. In *Ethics in Computing: A Concise Module* (pp. 227-253). Springer International Publishing. https://doi.org/10.1007/978-3-319-29106-2_11

Li, W., & Liu, Z. (2023). Social, Environmental, and Governance Factors on Supply-Chain Performance with Mediating Technology Adoption. *Sustainability, 15*(14), 10865. https://doi.org/10.3390/su151410865

Mady, A., Gupta, S., & Warkentin, M. (2023). The effects of knowledge mechanisms on employees' information security threat construal. *Information Systems Journal, 33*(4), 790-841. https://doi.org/10.1111/isj.12424

Mccarty, M., Johnson, J., Richardson, B., Rieger, C., Cooley, R., Gentle, J., Rothwell, B., Phillips, T., Novak, B., Culler, M., & Wright, B. (2023). Cybersecurity Resilience Demonstration for Wind Energy Sites in Co-Simulation Environment. *IEEE Access, 11*, 15297-15313. https://doi.org/10.1109/ACCESS.2023.3244778

Mokhtar, A. R., Anindita, M., & Suhaimi, Z. S. (2023). Leveraging Supply Chain Leadership for Dynamic Capabilities and Organisational Resilience. *Advances in Social Sciences Research Journal, 10*(6.2), 54-66. https://doi.org/10.14738/assrj.106.2.14992

Motiee, M. (2015). The Culture, Intercultural and Cross-cultural Dimensions in Communication. *International Journal of Social Sciences (IJSS), 5*(3), 43-50. https://www.sid.ir/en/VEWSSID/J_pdf/5053020150305.pdf

Muflikh, Y. N., Smith, C., Brown, C., & Aziz, A. A. (2021). Analysing price volatility in agricultural value chains using systems thinking: A case study of the Indonesian chilli value chain. *Agricultural Systems, 192*, 103179. https://doi.org/10.1016/j.agsy.2021.103179

Olorunniwo, F. O., & Li, X. (2010). Information sharing and collaboration practices in reverse logistics. *Supply Chain Management: An International Journal, 15*(6), 454-462. https://doi.org/10.1108/13598541011080437

Pal, S., Sikdar, B., & Chow, J. H. (2018). An Online Mechanism for Detection of Gray-Hole Attacks on PMU Data. *IEEE Transactions on Smart Grid, 9*(4), 2498-2507. https://doi.org/10.1109/TSG.2016.2614327

Phengsuk, T., Worasan, K., & Saenchaiyathon, K. (2023). The Influence of Supply Chain Strategy and Supply Chain Design on Supply Chain Resilience under Uncertain Circumstances: A Review of the Literature. *E3S Web of Conferences, 440*, 06005. https://doi.org/10.1051/e3sconf/202344006005

Renaud, J.-P., Chari, A., Ciferri, C., Liu, W.-t., Rémigy, H.-W., Stark, H., & Wiesmann, C. (2018). Cryo-EM in drug discovery: achievements, limitations and prospects. *Nature Reviews Drug Discovery, 17*(7), 471-492. https://doi.org/10.1038/nrd.2018.77

Riemenschneider, C. K., Burney, L. L., & Bina, S. (2023). The influence of organizational values on employee attitude and information security behavior: the mediating role of psychological capital. *Information & Computer Security, 31*(2), 172-198. https://doi.org/10.1108/ICS-10-2022-0156

Safari, A., Balicevac Al Ismail, V., Parast, M., Gölgeci, I., & Pokharel, S. (2023). Supply chain risk and resilience in startups, SMEs, and large enterprises: a systematic review and directions for research. *The International Journal of Logistics Management*. https://doi.org/10.1108/IJLM-10-2022-0422

Sakib, S., Raiaan, M. A. K., Fahad, N. M., Mukta, M. S. H., Mamun, A. A., & Chowdhury, S. (2023). A Review of the Evaluation of Ransomware: Human Error or Technical Failure? In *2023 International Conference on Information and Communication Technology for Sustainable Development (ICICT4SD)* (pp. 393-397). IEEE. https://doi.org/10.1109/ICICT4SD59951.2023.10303580

Sas, M., Reniers, G., Hardyns, W., & Ponnet, K. (2019). The impact of training sessions on security awareness: measuring the security knowledge, attitude and behaviour of employees. *Chemical Engineering Transactions, 77*, 895-900. https://doi.org/10.3303/CET1977150

Sen, A. C. (2022). Effectiveness of behavioural model with digital nudging in improving cyber security posture. *NeuroQuantology, 20*(11), 9372-9382. https://doi.org/10.48047/NQ.2022.20.11.NQ66934

Shaw, P., Mikusz, M., Trotter, L., Harding, M., & Davies, N. (2019). Towards an understanding of emerging cyber security threats in mapping the IoT. In *Living in the Internet of Things (IoT 2019)* (pp. 1-6). IET. https://doi.org/10.1049/cp.2019.0158

Siderska, J., Alsqour, M. D., & Alsaqoor, S. (2023). Employees' Attitudes Towards Implementing Robotic Process Automation Technology At Service Companies. *Human Technology, 19*(1), 23-40. http://dx.doi.org/10.14254/1795-6889.2023.19-1.3

Smith, N. L., & Green, B. C. (2020). Examining the factors influencing organizational creativity in professional sport organizations. *Sport Management Review, 23*(5), 992-1004. https://doi.org/10.1016/j.smr.2020.02.003

Stefaniuk, T. (2020). Training in shaping employee information security awareness. *Entrepreneurship and Sustainability Issues, 7*(3), 1832. http://doi.org/10.9770/jesi.2020.7.3(26)

Sulehri, N. A., Ullah, N., Maroof, Z., Uzair, A., Murtaza, A., & Irfan, M. (2023). Employee associations with R&D investment, firm performance, disruption risk, and supply chain performance during the COVID-19 pandemic: A multiple mediational model. *Frontiers in Environmental Science, 10*, 1050488. https://doi.org/10.3389/fenvs.2022.1050488

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information & Management, 49*(3), 190-198. https://doi.org/10.1016/j.im.2012.04.002

Yaokumah, W., Walker, D. O., & Kumah, P. (2019). SETA and security behavior: Mediating role of employee relations, monitoring, and accountability. *Journal of Global Information Management (JGIM), 27*(2), 102-121. https://doi.org/10.4018/JGIM.2019040106

Appendix 1: Measurement Scales

Employee Training and Awareness	
1. I am aware of any training programmes based on ransomeware risks. 2. I had any form of training based on ransomeware risks since I joined this organization 3. In your opinion, training at your organization is planned and systematic 4. I am motivated by and satisfied with the training program of this organzation 5. In your opinion, training had an impact on the growth of the company	Appiah (2010).
Technological Solutions Implementation	
1. There is proper mechanism for energy efficiency monitoring 2. There is proper mechanism for energy efficiency improving system 3. There is proper mechanism for identification and traceability of final products 4. There is proper mechanism for identification and traceability of raw materials **5.** There is proper mechanism for simulation of processes (digital manufacturing)	
Supply Chain Resilience Measures	
1. There is a proper mechanism of Supply chain communication 2. There may be possibility of Sup. involvement in innovation 3. There may be possibility of Postponement of orders **4.** There is a proper mechanism of Supplier collaboration	Aigbogun, Ghazali, and Razali (2018).
Collaboration and Information Sharing Practices	
1. There is proper mechanism for accuracy of information with my partners 2. There is mutual access to our and our partners' databases 3. There is a proper mechanism through which the amount of cost data we share with our partner 4. There is a proper mechanism through which the use of web-enabled inventory data information that we share 5. There is a proper mechanism through which the warehouse information we both share 6. There is trust between us and our partners 7. There is long-term alliance with our partners 8. There is well-defined collaborative objectives, scope and responsibilities 9. There is a proper mechanism through which the joint forecast and planning arrangements 10. There is a proper mechanism through which the jointly-established performance measures 11. There is sharing of risk and reward with our partners	Olorunniwo and Li (2010).
Comprehensive Security Posture	
1. The behavioural model with digital nudging interventions motivates you to adopt better security practices. 2. The digital nudging interventions helps to become more conscious of security-related behaviours. 3. I follow the security guidelines presented through the behavioural model and digital nudging interventions 4. The prompts provided by the digital nudging interventions were helpful in reminding you to update your passwords. **5.** The reminders in the digital nudging interventions are keeping you vigilant about ransomware attacks	Sen (2022).
Employee Behavior and Adherence	
Self-efficacy 1. We are implementing security measures in our manufacturing and supply chain **Experiential Attitude** 2. Security measures disrupt our existing workflows or business processes **Instrumental Attitude** 3. Security measures help us prevent or mitigate ransomware attacks **Social pressures** 4. Our organization and our supply chain partners will support the security initiatives **Response efficacy** 5. Security measures considered best practices for mitigating ransomware risks **Response cost** 6. The initial and ongoing costs of implementing and maintaining the security measures **Perceived susceptibility** 7. Our manufacturing and supply chain operations are vulnerable to ransomware attacks if we don't implement security measures	(Blythe, Coventry, & Little, 2015).