Advanced International Journal of Business, Entrepreneurship and SME's
AIJBES
EISSN: 2682-8545
Volume: 8 Issue: 29 (September 2026) PP. 435-456

ADVANCED INTERNATIONAL JOURNAL OF BUSINESS, ENTREPRENEURSHIP AND SMES (AIJBES)
www.gaexcellence.com/aijbes

GLOBAL ACADEMIC EXCELLENCE

ORGANIZATIONAL DETERMINANTS OF CYBER RISK OCCURRENCE IN MALAYSIAN LOCAL AUTHORITIES

Halil Paino[1], Marlina Rahmat[2], Mohd Soffi Puteh[3], Mohd Zulfikri Abd Rashid[4*]

[1]Faculty of Accountancy, Universiti Teknologi MARA Puncak Alam Selangor
halil@uitm.edu.my https://orcid.org/0000-0002-6026-6607
[2]Shah Alam City Council, Selangor Malaysia
marlina@mbsa.gov.my https://orcid.org/0009-0007-8447-4383
[3]Faculty of Accountancy, Universiti Teknologi MARA, Perak Branch, Tapah Campus, 35400, Tapah Road, Perak, Malaysia
sopiuitm@uitm.edu.my https://orcid.org/0000-0003-4358-5080
[4]Faculty of Accountancy, Universiti Teknologi MARA, Perak Branch, Tapah Campus, 35400, Tapah Road, Perak, Malaysia
mohdzulfikri@uitm.edu.my https://orcid.org/0009-0003-3790-891X
*Corresponding Author

Article Info:

Article history:
Received date: 05.07.2026
Revised date: 10.08.2026
Accepted date: 27.08.2026
Published date: 14.09.2026

To cite this document:

Paino, H., Rahmat, M., Puteh, M. S., & Rashid, M. Z. A. (2026). Organizational Determinants of Cyber Risk Occurrence in Malaysian Local Authorities. *Advanced International Journal of Business Entrepreneurship and SMEs, 8* (29), 435-456.

Abstract:

The increasing dependence on digital infrastructure has intensified the need for effective cyber risk management, particularly within public sector organizations such as local authorities. Within the context of Majlis Bandaraya Shah Alam (MBSA), the extent to which organizational factors, including cybersecurity policies, cybersecurity training, and leadership commitment, influence Cyber Risk Occurrence (CRO) requires empirical investigation. Although these factors have been recognised as important elements of cybersecurity governance, limited context-specific evidence is available regarding their relative contribution to CRO within Malaysian local authorities. Therefore, this study examines how organizational factors, namely cybersecurity policies, cybersecurity training, and leadership commitment, influence Cyber Risk Occurrence (CRO) within MBSA. A quantitative research design was adopted using a structured online questionnaire. Stratified random sampling was employed to ensure proportional representation of senior management (Officer A) and operational staff (Officer B). A total of 242 respondents participated in the study. Pearson correlation analysis revealed that Cybersecurity Policies (CP), Cybersecurity Training (CT), and Leadership Commitment (LC) were significantly associated with Cyber Risk Occurrence (CRO). However, multiple regression analysis identified cybersecurity training as the only

Advanced International Journal of Business, Entrepreneurship and SME's
AIJBES
EISSN: 2682-8545
Volume: 8 Issue: 29 (September 2026) PP. 435-456

significant predictor of CRO after controlling for the other organizational factors. The findings highlight the critical role of continuous employee training in strengthening organizational resilience against cyber threats. This study contributes to the cybersecurity literature by integrating Risk Management Theory, Human Capital Theory, and Transformational Leadership Theory to explain cyber risk occurrence in Malaysian local authorities. The findings also provide practical insights for policymakers, practitioners, and public sector organizations in strengthening cybersecurity governance, enhancing employee capabilities, and improving organizational cyber resilience.

DOI: 10.35631/AIJBES.829024

Keyword:

Cyber Risk Management, Cyber Risk Occurrence, Cybersecurity Policies, Cybersecurity Training, Leadership Commitment, Majlis Bandaraya Shah Alam (MBSA).

Introduction

Nowadays, the increasing dependence on digital infrastructure has heightened the need for effective cyber risk management, particularly within public sector organizations such as local authorities. Cyber incidents, including data breaches, ransomware attacks, and unauthorized access, pose significant threats to operational continuity, data integrity, and public trust. Several international cybersecurity incidents, including the Singapore Cybersecurity Strategy (2021), the Baltimore Ransomware Attack (2019), and the Colonial Pipeline Cyberattack (2021), have demonstrated the importance of effective cybersecurity governance and incident response mechanisms (Insurica, 2025). These incidents highlight the need for public institutions to strengthen their cybersecurity governance frameworks to safeguard critical information assets and ensure the continuity of public services. Consequently, understanding the organizational determinants of cyber risk occurrence has become increasingly important.

Despite the growing awareness of cybersecurity risks, Malaysian local authorities face increasing challenges in managing cyber threats as their dependence on digital systems and online public services continues to expand. Effective cybersecurity management requires not only technological controls but also appropriate organizational measures, including well-established cybersecurity policies, continuous employee training, and strong leadership commitment. Understanding how these organizational factors contribute to Cyber Risk Occurrence (CRO) is therefore important for strengthening cybersecurity governance and organizational resilience.

Advanced International Journal of Business, Entrepreneurship and SME's
AIJBES
EISSN: 2682-8545
Volume: 8 Issue: 29 (September 2026) PP. 435-456

The increasing frequency and sophistication of cyber threats, ranging from unauthorized system access to malware attacks, emphasize the importance of effective cybersecurity risk management within public sector organizations, including local authorities. Internationally recognized standards, such as ISO/IEC 27001, provide a useful reference for information security governance and risk management. However, the present study does not assess MBSA's compliance with or alignment to ISO/IEC 27001. Instead, ISO/IEC 27001 is referred to as contextual background for understanding the broader importance of structured information security governance.

Although previous studies have examined cybersecurity practices in various organizational settings, empirical evidence on the organizational determinants of Cyber Risk Occurrence (CRO) within Malaysian local authorities remains limited (Herath & Rao, 2009; Puhakainen & Siponen, 2010). Existing studies have primarily examined cybersecurity practices in relation to technological controls, security compliance, and employee security behaviour. Comparatively less attention has been given to examining organizational factors such as cybersecurity policies, cybersecurity training, and leadership commitment together within the Malaysian local government context. More specifically, limited empirical studies have examined the relative and unique contributions of these three organizational factors to CRO. Consequently, this study addresses this gap by providing context-specific empirical evidence on how cybersecurity policies, cybersecurity training, and leadership commitment influence CRO within Malaysian local authorities.

Therefore, this study examines the influence of Cybersecurity Policies (CP), Cybersecurity Training (CT), and Leadership Commitment (LC) on Cyber Risk Occurrence (CRO) at Majlis Bandaraya Shah Alam (MBSA). Specifically, the study aims to examine the influence of cybersecurity policies on cyber risk occurrence, determine the influence of cybersecurity training on cyber risk occurrence, and analyse the influence of leadership commitment on cyber risk occurrence. To address these objectives, the study is underpinned by Risk Management Theory and supported by Institutional Theory, Human Capital Theory, and Transformational Leadership Theory (Herath & Rao, 2009; Puhakainen & Siponen, 2010; Traynor, 2025). A quantitative research approach was employed using a structured questionnaire distributed to MBSA employees, while stratified random sampling was adopted to ensure appropriate representation of respondents. The findings are expected to contribute to the growing literature on organizational determinants of cyber risk occurrence and provide practical insights for policymakers and public sector administrators in strengthening cybersecurity governance, improving organizational resilience, and supporting secure digital public service delivery.

Literature Review

This section reviews the literature related to the organizational determinants of cyber risk occurrence, with particular emphasis on cybersecurity policies, cybersecurity training, and leadership commitment within public sector organizations. These organizational factors have been widely recognised as important elements in strengthening cybersecurity governance and reducing organizational exposure to cyber threats. Previous studies suggest that effective cybersecurity management requires not only technological safeguards but also strong governance structures, competent employees, and committed leadership.

Advanced International Journal of Business, Entrepreneurship and SME's
AIJBES
EISSN: 2682-8545
Volume: 8 Issue: 29 (September 2026) PP. 435-456

Cybersecurity policies provide the formal rules, procedures, and guidelines that govern how organizations identify, manage, and respond to cyber threats. Well-defined and enforceable policies promote consistency in cybersecurity practices and support organizational compliance with security requirements. Gupta and Remella (2025) emphasised that an effective risk management framework should include comprehensive cybersecurity policies that clearly define organizational responsibilities and risk management procedures. Similarly, Chong et al. (2022) highlighted the importance of policy development in protecting digital infrastructure, particularly within public sector and urban environments.

Cybersecurity training is another important organizational determinant of cyber risk occurrence. Previous studies consistently reported that continuous training programmes improve employees' cybersecurity awareness, reduce human error, and strengthen organizational resilience against cyber threats (Goswami et al., 2023; Aliane & Zakariya, 2023). However, the effectiveness of training programmes depends on adequate organizational support and leadership commitment. Puhakainen and Siponen (2010) further demonstrated that structured cybersecurity education contributes significantly to improving security compliance and reducing cybersecurity incidents within public organizations.

Leadership commitment also plays an essential role in promoting a strong cybersecurity culture. Senior management influences cybersecurity governance by establishing strategic priorities, allocating resources, and encouraging employee compliance with organizational security policies. According to Sarumi and Abdul-Raheem (2022), active leadership involvement strengthens cybersecurity strategy implementation and organizational preparedness. Likewise, Herath and Rao (2009) argued that leadership commitment enhances policy compliance and fosters a security-conscious organizational culture.

Collectively, the existing literature indicates that cybersecurity policies, cybersecurity training, and leadership commitment are important organizational determinants that influence cyber risk occurrence. These organizational factors provide the foundation for effective cybersecurity governance and support the development of resilient public sector organizations. Accordingly, this study examines the relationships between these organizational determinants and cyber risk occurrence within Majlis Bandaraya Shah Alam (MBSA).

Theoretical Framework

Risk Management Theory serves as the principal theoretical foundation of this study because it provides a systematic framework for identifying, assessing, and mitigating risks that may affect organizational objectives. Within the cybersecurity context, the theory emphasises proactive risk identification, continuous risk assessment, and the implementation of appropriate controls to minimise the likelihood and impact of cyber incidents (ISO, 2018). Unlike purely technical approaches, Risk Management Theory integrates governance, organizational processes, and human behaviour, making it particularly suitable for examining the organizational determinants of cyber risk occurrence in Malaysian local authorities.

According to ISO/IEC 27001 (ISO, 2018), effective cyber risk management is a continuous process comprising risk identification, risk analysis, risk evaluation, and risk treatment. These processes enable organizations to develop appropriate governance mechanisms that strengthen cybersecurity resilience and improve organizational preparedness against emerging cyber threats. For public sector organizations such as Majlis Bandaraya Shah Alam (MBSA),

Advanced International Journal of Business, Entrepreneurship and SME's
AIJBES
EISSN: 2682-8545
Volume: 8 Issue: 29 (September 2026) PP. 435-456

effective risk management is especially important because of the need to protect public information assets, maintain service continuity, and fulfil governance and accountability responsibilities.

Although Risk Management Theory provides the primary theoretical perspective, this study is further supported by Institutional Theory, Human Capital Theory, and Transformational Leadership Theory. Institutional Theory explains how formal organizational structures, policies, and governance mechanisms promote regulatory compliance and organizational legitimacy (Gupta & Remella, 2025). Human Capital Theory emphasises that employee knowledge, competencies, and continuous learning are valuable organizational resources that reduce operational risks and strengthen cybersecurity capabilities (Becker, 1993). Meanwhile, Transformational Leadership Theory highlights the role of senior management in shaping organizational culture, allocating resources, and encouraging employees to adopt secure cybersecurity practices (Bass & Avolio, 1994). Together, these supporting theories complement Risk Management Theory by explaining how organizational governance, employee capability, and leadership commitment collectively influence cyber risk occurrence.

From the perspective of Risk Management Theory, cybersecurity policies function as preventive governance mechanisms that define organizational responsibilities, establish acceptable security practices, and standardise incident response procedures. Organizations with comprehensive cybersecurity policies generally demonstrate stronger governance and improved cyber resilience (Herath & Rao, 2009; Gupta & Remella, 2025). Similarly, cybersecurity training strengthens employees' ability to recognise and respond to cyber threats such as phishing, malware, and social engineering attacks, thereby reducing human-related vulnerabilities (Puhakainen & Siponen, 2010; Goswami et al., 2023). Leadership commitment further supports effective cybersecurity governance by establishing strategic priorities, allocating appropriate resources, and promoting a culture of continuous cybersecurity improvement (Sarumi & Abdul-Raheem, 2022).

In Sum, Risk Management Theory provides a comprehensive framework for examining how cybersecurity policies, cybersecurity training, and leadership commitment interact as organizational determinants of cyber risk occurrence. By integrating governance mechanisms, employee competencies, and leadership practices, the theory offers a holistic explanation of organizational efforts to strengthen cybersecurity resilience within Malaysian local authorities.

Cybersecurity Policies and Cyber Risk Occurrence

Cybersecurity policies represent one of the key organizational determinants examined in this study. They consist of formal rules, guidelines, and procedures that govern how organizations identify, manage, and respond to cybersecurity risks. Well-developed cybersecurity policies ensure that roles, responsibilities, and security practices are clearly defined, thereby promoting consistency in organizational risk management. Institutional Theory explains that organizations establish formal structures and policies to achieve regulatory compliance, organizational legitimacy, and effective governance (Gupta & Remella, 2025; Chong et al., 2022). Accordingly, comprehensive cybersecurity policies provide a structured framework for managing cyber threats while ensuring that security measures are implemented consistently across the organization.

Advanced International Journal of Business, Entrepreneurship and SME's
AIJBES
EISSN: 2682-8545
Volume: 8 Issue: 29 (September 2026) PP. 435-456

Risk Management Theory further suggests that structured governance mechanisms reduce uncertainty and improve the effectiveness of organizational risk controls (ISO, 2018). From this perspective, cybersecurity policies function as preventive controls that support risk identification, incident response, and continuous monitoring of cybersecurity practices. Organizations with comprehensive and well-implemented cybersecurity policies generally experience fewer cybersecurity incidents and demonstrate stronger organizational resilience (Chong et al., 2022). Institutional Theory similarly proposes that formalized policies enhance organizational compliance and encourage consistent security-related behaviour (Gupta & Remella, 2025).

Evidence from previous studies supports the importance of cybersecurity policies in reducing organizational exposure to cyber threats. For example, the NHS WannaCry ransomware attack demonstrated how fragmented policies and inconsistent governance contributed to significant operational disruption across healthcare institutions (NAO, 2018). Likewise, the Equifax data breach highlighted how weaknesses in governance and policy implementation increased organizational vulnerability to cyberattacks (Equifax, 2017). These findings suggest that organizations with comprehensive and integrated cybersecurity policies are better positioned to prevent cyber incidents and strengthen cyber resilience.

Based on the theoretical and empirical evidence, the following hypothesis is proposed:
H1: *Cybersecurity policies significantly reduce cyber risk occurrence at MBSA.*

Cybersecurity Training and Cyber Risk Occurrence

Cybersecurity training is the second organizational determinant examined in this study. It refers to structured educational programmes that equip employees with the knowledge, skills, and awareness required to identify, prevent, and respond to cybersecurity threats. Effective training enhances employees' ability to recognise risks such as phishing, malware, and social engineering attacks, thereby reducing the likelihood of human error, which remains one of the leading causes of cybersecurity incidents.

Human Capital Theory provides the theoretical foundation for this construct by emphasising that employee knowledge, competencies, and continuous learning are valuable organizational resources that strengthen organizational performance and reduce operational risks (Becker, 1993). Within the cybersecurity context, continuous training enables employees to develop the competencies required to recognise emerging threats and respond appropriately to cyber incidents. Consequently, organizations that invest in regular and relevant cybersecurity training are generally better equipped to minimise human-related vulnerabilities and improve overall cyber resilience (Goswami et al., 2023; Aliane & Zakariya, 2023).

From the perspective of Risk Management Theory, cybersecurity training functions as a preventive risk control that enhances employees' awareness and supports the effective implementation of cybersecurity policies (ISO, 2018). Previous studies have consistently reported that structured and continuous training programmes reduce cognitive and behavioural vulnerabilities, improve compliance with cybersecurity procedures, and decrease the occurrence of human-related cyber incidents (Parsons et al., 2017; ENISA, 2022; Goswami et al., 2023; Aliane & Zakariya, 2023). Similarly, Puhakainen and Siponen (2010) found that continuous security awareness programmes significantly improve employee compliance and cybersecurity practices within public sector organizations.

Advanced International Journal of Business, Entrepreneurship and SME's
AIJBES
EISSN: 2682-8545
Volume: 8 Issue: 29 (September 2026) PP. 435-456

Empirical evidence further supports the importance of cybersecurity training. The 2018 City of Atlanta ransomware attack demonstrated how inadequate employee preparedness and limited cybersecurity awareness contributed to widespread service disruption and significant operational losses (U.S. Department of Justice, 2018). These findings suggest that systematic and continuous cybersecurity training plays an important role in reducing cyber risk occurrence by strengthening employee preparedness and organizational resilience.

Based on the theoretical and empirical evidence, the following hypothesis is proposed:
H2: *Cybersecurity training significantly reduces cyber risk occurrence at MBSA*.

Leadership Commitment and Cyber Risk Occurrence

Leadership commitment is the third organizational determinant examined in this study. It refers to the extent to which top management prioritises cybersecurity, allocates adequate resources for cybersecurity initiatives, and promotes a culture of security awareness throughout the organization. Strong leadership commitment ensures that cybersecurity is incorporated into strategic planning and organizational decision-making, thereby strengthening overall cybersecurity governance.

Transformational Leadership Theory provides the theoretical foundation for this construct by emphasising the role of visionary and committed leaders in driving organizational change and influencing employee behaviour (Bass & Avolio, 1994). Leaders play a significant role in establishing cybersecurity priorities, supporting policy implementation, and ensuring that sufficient financial, technological, and human resources are allocated to cybersecurity risk management (Sarumi & Abdul-Raheem, 2022). Through effective leadership, organizations are better positioned to develop a security-conscious culture that encourages compliance with cybersecurity policies and continuous organizational improvement.

From the perspective of Risk Management Theory, leadership commitment strengthens organizational governance by integrating cybersecurity into enterprise-wide risk management processes (ISO, 2018). Strong executive involvement improves accountability, clarifies risk ownership, and supports the consistent implementation of cybersecurity controls (Herath & Rao, 2009). Likewise, organizations with active leadership demonstrate higher levels of cybersecurity maturity and more effective governance practices (Alshaikh, 2020).

Empirical evidence further supports the importance of leadership commitment in reducing cyber risk occurrence. The Equifax data breach in 2017 demonstrated how weak executive oversight and delayed governance decisions contributed to one of the largest data breaches in history (U.S. House Committee on Oversight and Reform, 2018). The incident illustrates that cybersecurity failures often arise from governance and leadership deficiencies rather than technological weaknesses alone. Therefore, organizations with committed leadership are more likely to strengthen cybersecurity governance, improve organizational resilience, and reduce exposure to cyber threats.

Based on the theoretical and empirical evidence, the following hypothesis is proposed:
H3: *Leadership commitment significantly reduces cyber risk occurrence at MBSA*.

Advanced International Journal of Business, Entrepreneurship and SME's
AIJBES
EISSN: 2682-8545
Volume: 8 Issue: 29 (September 2026) PP. 435-456

Conceptual Framework

The conceptual framework illustrates the relationships between the organizational determinants of cyber risk occurrence examined in this study. It proposes that three independent variables; Cybersecurity Policies (CP), Cybersecurity Training (CT), and Leadership Commitment (LC); influence the dependent variable, namely Cyber Risk Occurrence (CRO), within Majlis Bandaraya Shah Alam (MBSA). The framework is primarily underpinned by Risk Management Theory, which emphasises that organizational risks can be effectively managed through systematic governance, risk assessment, and appropriate control mechanisms (ISO, 2018).

Within the framework, cybersecurity policies function as governance mechanisms that establish organizational rules, responsibilities, and security procedures for managing cyber risks. Cybersecurity training enhances employees' knowledge, awareness, and competencies, enabling them to recognise and respond effectively to evolving cyber threats while reducing human-related vulnerabilities. Leadership commitment supports cybersecurity governance by providing strategic direction, allocating adequate resources, and fostering a security-conscious organizational culture. Collectively, these organizational determinants strengthen cybersecurity resilience and are expected to reduce cyber risk occurrence within MBSA.

This study is primarily underpinned by Risk Management Theory, which provides the overall explanation for how organizational measures may influence Cyber Risk Occurrence (CRO). Institutional Theory provides the theoretical basis for examining Cybersecurity Policies (CP), as formal policies and organizational structures guide employees' behaviour and support cybersecurity practices. Human Capital Theory supports the relationship between Cybersecurity Training (CT) and CRO by explaining how investment in employees' knowledge and skills can improve their ability to identify, prevent, and respond to cyber threats. Transformational Leadership Theory supports the examination of Leadership Commitment (LC), as committed leaders can influence organizational priorities, allocate appropriate resources, and promote a cybersecurity-conscious culture. Therefore, the four theories provide complementary explanations for the relationships between the organizational factors and CRO rather than representing separate theories explaining the same relationship.

The conceptual framework is based on the proposed relationships between Cybersecurity Policies (CP), Cybersecurity Training (CT), Leadership Commitment (LC), and Cyber Risk Occurrence (CRO). Based on the theoretical perspectives discussed above, the framework examines how these organizational factors are associated with CRO within Malaysian local authorities. The proposed conceptual framework is presented in Figure 1.

Advanced International Journal of Business, Entrepreneurship and SME's
AIJBES
EISSN: 2682-8545
Volume: 8 Issue: 29 (September 2026) PP. 435-456

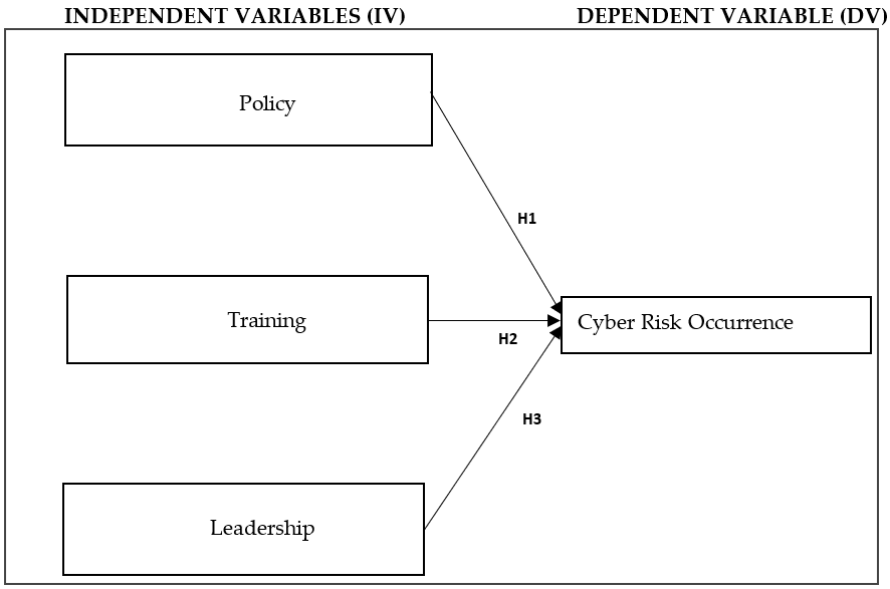

Figure 1: Conceptual Framework

Methodology

Research Design

This study employed a quantitative cross-sectional research design to examine the influence of organizational determinants—Cybersecurity Policies (CP), Cybersecurity Training (CT), and Leadership Commitment (LC)—on Cyber Risk Occurrence (CRO) at Majlis Bandaraya Shah Alam (MBSA). A minimal-interference approach was adopted to ensure that data collection did not disrupt normal organizational operations, allowing respondents to provide perceptions based on their actual workplace experiences.

The unit of analysis comprised MBSA employees from two organizational levels: Officer A (senior management and decision-makers) and Officer B (operational staff). Including both groups enabled the study to capture perspectives from strategic and operational levels of cybersecurity management. Data were collected using a structured questionnaire distributed through an online survey. Stratified random sampling was employed to ensure proportional representation of both employee groups and minimise sampling bias. The collected data were analysed using descriptive statistics, Pearson correlation analysis, and multiple regression analysis.

Population

The target population consisted of 242 employees of Majlis Bandaraya Shah Alam (MBSA) who were directly or indirectly involved in cybersecurity-related activities. The population was divided into two strata based on organizational roles. Officer A comprised 32 senior managers and administrators responsible for cybersecurity governance, strategic planning, and policy development. Officer B consisted of 210 operational employees responsible for implementing cybersecurity practices and supporting daily organizational operations.

Advanced International Journal of Business, Entrepreneurship and SME's
AIJBES
EISSN: 2682-8545
Volume: 8 Issue: 29 (September 2026) PP. 435-456

The inclusion of both managerial and operational employees provided a comprehensive understanding of cybersecurity governance across different organizational levels and enabled the study to examine how cybersecurity practices were perceived and implemented within MBSA.

Sampling Technique

This study employed stratified random sampling to ensure proportional representation of Officer A and Officer B within the sample. The population was first divided into the two strata, after which respondents were selected proportionately according to the size of each group. This sampling technique reduces sampling bias while ensuring that both managerial and operational perspectives are adequately represented.

Based on the total population of 242 employees, the minimum required sample size was determined using the Krejcie and Morgan (1970) sample size table, resulting in a minimum sample of 149 respondents. However, the data collection resulted in 242 valid responses, and all valid responses were included in the final analysis. The formula used to determine the required sample size is presented as follows:

$$s = \frac{x^2.N.P(1-P)}{d^2(N-1) + X^2.P(1-P)}$$

Where:

S: Total required sample size
N: Population size (242)
χ^2: Chi-square value (3.841 for 95% confidence level)
P: Proportion (0.5 for maximum variability)
d^2: Margin of error (0.05 for 5%)

Meanwhile, the total sample size is calculated to be 149 respondents. Next, proportions for Officer A and Officer B are calculated as below:

a) Proportion for Officer A: 32/242 ≈ 0.13
b) Proportion for Officer B: 210/242 ≈ 0.87

Next, the total sample size (S = 149) is multiplied by the respective proportions:

a) Sample Size for Officer A: 32/242 × 149 ≈ 20
b) Sample Size for Officer B: 210/242 × 149 ≈ 129

Thus, a total of 20 respondents was chosen from the Officer A group, which represents upper-echelon decision-makers and administrators. A larger fraction of the sample, 129 respondents, are drawn from the Officer B group that represents operational and support staff. This proportional allocation of respondents ensures that both Officer A and Officer B are represented according to their size in the overall population.

Data Collection Procedures

Prior to data collection, ethical approval was obtained from the Research Ethics Committee of Universiti Teknologi MARA. Respondents were provided with information regarding the

Advanced International Journal of Business, Entrepreneurship and SME's
AIJBES
EISSN: 2682-8545
Volume: 8 Issue: 29 (September 2026) PP. 435-456
purpose of the study, the nature of their participation, and their rights as research participants. Informed consent was obtained electronically before respondents completed the online questionnaire. All responses were treated confidentially and used solely for academic purposes. Data were collected using a structured questionnaire administered through Google Forms. The online survey enabled the efficient collection of primary data reflecting employees' perceptions of organizational practices, cybersecurity measures, and cyber risk management within Majlis Bandaraya Shah Alam (MBSA).

Data Analysis

The collected data were analysed using IBM SPSS Statistics Version 29. Descriptive statistics, including frequencies, percentages, means, and standard deviations, were used to summarise respondents' demographic characteristics and describe the study variables. These analyses provided an overview of employees' perceptions of Cybersecurity Policies (CP), Cybersecurity Training (CT), Leadership Commitment (LC), and Cyber Risk Occurrence (CRO).

Inferential statistical analyses were subsequently performed to examine the relationships between the independent and dependent variables. Pearson correlation analysis was used to determine the strength and direction of the relationships among the study variables, while multiple regression analysis was conducted to identify the predictors of cyber risk occurrence. The reliability of the research instrument was assessed using Cronbach's alpha coefficient. Normality was evaluated using the Kolmogorov–Smirnov and Shapiro–Wilk tests, supported by Q-Q plots. Multicollinearity was assessed using Variance Inflation Factor (VIF) values to ensure the independence of the predictor variables.

Research Instrument

The research instrument consisted of a structured questionnaire developed based on established literature in cybersecurity governance, risk management, and organizational behaviour. The questionnaire was designed to collect quantitative data on the organizational determinants of cyber risk occurrence at Majlis Bandaraya Shah Alam (MBSA) and was aligned with the study objectives and theoretical framework.

The questionnaire comprised five sections. Section 1 collected respondents' demographic information, including gender, age, academic qualification, job role, department, years of service, and level of involvement in cybersecurity-related tasks. Sections 2, 3, and 4 measured respondents' perceptions of Cybersecurity Policies (CP), Cybersecurity Training (CT), and Leadership Commitment (LC), respectively. These constructs were measured using five-point Likert scales, with response categories ranging from "Strongly Disagree" to "Strongly Agree" or from "Very Ineffective" to "Very Effective," depending on the construct being measured.
Section 5 measured Cyber Risk Occurrence (CRO), referring to respondents' perceptions of cybersecurity-related risk experiences within the organization. The construct included the frequency and types of cybersecurity incidents, their perceived impact, and the organization's incident response and recovery practices. Therefore, CRO in this study represents a perception-based measure of cyber risk experiences and related organizational consequences rather than solely the actual number of cybersecurity incidents recorded by MBSA.

Advanced International Journal of Business, Entrepreneurship and SME's
AIJBES
EISSN: 2682-8545
Volume: 8 Issue: 29 (September 2026) PP. 435-456

Validity and Reliability

Content validity was established by adapting questionnaire items from validated instruments used in previous cybersecurity and organizational studies (Herath & Rao, 2009; Puhakainen & Siponen, 2010; Aliane & Zakariya, 2023). Face validity was further strengthened through expert review to ensure the clarity, relevance, and appropriateness of the questionnaire items. Construct validity was supported through the use of established measurement scales that are widely adopted in cybersecurity and organizational research.

The reliability of the instrument was evaluated using Cronbach's alpha coefficient, where a value of 0.70 or above is generally considered acceptable for social science research (Hair et al., 2019). The use of standardized five-point Likert scales further enhanced response consistency across participants. Previous studies employing similar instruments have also reported satisfactory reliability, supporting the suitability of the questionnaire for measuring the organizational determinants of cyber risk occurrence (Herath & Rao, 2009; Puhakainen & Siponen, 2010).

Result And Analysis

Preliminary Data Analysis

Preliminary data analysis was conducted to examine data quality before hypothesis testing, including response rate, straight-lining behaviour, missing values, and data normality. Of the questionnaires distributed, 242 valid responses were obtained, representing a response rate of 80.6%, which is considered excellent for large-scale online surveys (Masson, 2025).

Data screening using IBM SPSS Statistics Version 29 indicated that no questionnaires were removed due to straight-lining behaviour, as all response items recorded standard deviation and variance values greater than zero (Hair et al., 2017). Furthermore, all study variables demonstrated acceptable skewness and kurtosis values within the range of −1 to +1, indicating an approximately normal distribution (Kline, 2011; Jackson, 2012).

The normality assumption was further assessed using histograms, Q-Q plots, and P-P plots. The graphical results showed that the data points were distributed closely around the reference line without substantial deviations, indicating the absence of serious outliers and supporting the assumption of normality (Das & Imon, 2016). These findings confirm that the data were suitable for subsequent parametric analyses, including Pearson correlation and multiple regression.

Demographic Profile

The demographic characteristics of the respondents are presented in Table 1. A total of 242 valid responses were obtained, comprising 47.1% male and 52.9% female respondents, indicating a relatively balanced gender distribution. Most respondents were between 31 and 40 years old (42.1%), followed closely by those aged 41 to 50 years (41.3%), suggesting that the majority of respondents were experienced working adults.

Advanced International Journal of Business, Entrepreneurship and SME's
AIJBES
EISSN: 2682-8545
Volume: 8 Issue: 29 (September 2026) PP. 435-456

With regard to educational background, most respondents possessed a Diploma qualification (76.8%), followed by a Bachelor's degree (19.0%), while only a small proportion held postgraduate qualifications. In terms of organizational roles, Officer B represented the largest group (86.8%), whereas Officer A accounted for 13.2%, reflecting the actual staff distribution within MBSA.

The findings also indicate that 75.2% of respondents had more than 10 years of service, suggesting substantial organizational experience. Although 58.3% reported that they were not directly involved in cybersecurity-related tasks, most respondents indicated at least a moderate level of familiarity with cybersecurity concepts, with only 5.4% reporting no familiarity. Overall, the respondents possessed sufficient organizational experience and cybersecurity awareness to provide meaningful responses regarding the organizational determinants of cyber risk occurrence.

Table 1: Demographic Profiles of Respondents (N=242)

Demographic	Frequency	Percentage
Gender		
Male	114	47.1
Female	128	52.9
Age		
Below 30 years old	16	6.6
31 – 40 years old	102	42.1
41 – 50 years old	100	41.3
50 years old and above	24	9.9
Academic Qualification		
STPM	5	2.1
Diploma	186	76.8
Bachelor's Degree	46	19.0
Master's Degree	5	2.1
Doctorate (PhD/EdD)	0	0.0
Role in MBSA		
Officer A	32	13.2
Officer B	210	86.8
Year of Working at MBSA		
1- 5 years	7	2.9
6 – 10 years	53	21.9
More than 10 years	182	75.2

Handle cybersecurity tasks		
Yes	101	41.7
No	141	58.3
Level of familiarity with cybersecurity		
Not at all familiar	13	5.4
A little familiar	40	16.5
Somewhat familiar	95	39.3
Familiar	75	31.0
Very familiar	19	7.9

Descriptive Analysis

This section describes the descriptive analysis of the study variables by presenting the mean (*M*) and standard deviation (*SD*) values. The mean score for cyber risk occurrence was 18.84 with a standard deviation of 3.01. Both subscales, Rate and Patterns (M = 9.34, SD = 1.93) and Impact and Actions (M = 9.50, SD = 2.25), recorded nearly similar means and standard deviations. This suggests that respondents in this study feel that both perspectives are equally important in capturing cyber risk occurrence. Next, Cybersecurity Policies (CP) showed the highest mean and standard deviation among the other independent variables (M = 22.97, SD = 4.52). Besides, Cybersecurity Training (CT) (M = 15.17, SD = 2.83) has the lowest mean and standard deviation, while Leadership Commitment (LC) (M = 17.82, SD = 3.91) was slightly higher than the CT. This suggests the respondents think that leadership commitment, such as allocation of resources and leadership involvement, is slightly more important than CT in capturing cybersecurity incidents.

Reliability

An acceptable reliability score is at least 0.7 or higher (Mohajan, 2017; Heal & Twycross, 2015). However, reliability with Cronbach's alpha of 0.60 and above is still considered acceptable and ideally reliable (Jackson, 2012; Schmitt, 1996; Cortina, 1993).

All of the instruments utilized in this current study showed sufficient and good reliability, except for Cyber Risk Occurrence. The highest score was cybersecurity policies and leadership commitment (alpha=.75), while the lowest was cyber risk occurrence (alpha=.45). The low reliability of CRO might be due to the mixed nominal and ordinal items in this subscale. Overall, the whole set of questionnaires achieved a sufficient reliability score with the standardized alpha value of 0.78.

Inferential Statistics

In this section, the inferential statistics, such as Pearson correlation analysis and multiple regression, are discussed.

Advanced International Journal of Business, Entrepreneurship and SME's
AIJBES
EISSN: 2682-8545
Volume: 8 Issue: 29 (September 2026) PP. 435-456

Pearson Correlation Analysis

Pearson correlation analysis explores the strength of the relationships between the Cybersecurity Policies (CP), Cybersecurity Training (CT), Leadership Commitment (LC), and Cyber Risk Occurrence (CRO). The value of the correlation coefficient (r) ranges between -1.0 and +1.0; if there is a +1.0 value, it indicates perfect positive correlation, and a -1.0 value indicates perfect negative correlation (Saccenti et al., 2020).

Table 2: Correlation Analysis

	CP	CT	LC	RaP	IaA	CRO
CP	1	.712**	.713**	-.185**	.536**	.281**
CT	.712**	1	.716**	-.194**	.563**	.295**
LC	.713**	.716**	1	-.276**	.552**	.234**
RaP	-.185**	-.194**	-.276**	1	.034	.667**
IaA	.536**	.563**	.552**	.034	1	.767**
CRO	.281**	.295*	.234**	.667**	.767**	1

Note: **p <.01, CP= Cybersecurity Policies, CT= Cybersecurity Training, LC= Leadership Commitment, RaP= Cyber Risk (Rate and Patterns), IaA= Cyber Risk (Impact and Actions), CRO= Cyber Risk Occurrence

Based on Table 2, all independent variables have a significant positive relationship with cyber risk occurrence. All three independent variables showed nearly similar correlation coefficients, and the strongest strength of relationship was the cybersecurity training and cyber risk occurrence ($r = .295$, $p < .01$). This result is consistent with prior studies that reported if employees' cybersecurity awareness and skills are improved through the training, the organization tends to handle the cyber risk more effectively (Goswami et al., 2023; Aliane & Zakariya, 2023). Next, cybersecurity policies ($r = .281$, $p < .01$) showed nearly the similar strength of positive correlation with the cyber risk occurrence, illustrating that this variable is equally important as the cybersecurity training. This finding is supported by past studies that mentioned the importance of well-defined policies for a company to manage cyber threats (Gupta & Remella, 2025; Chong et al., 2022). Lastly, leadership commitment ($r = .234$, $p < .01$) showed the weakest but significant positive association with cyber risk occurrence, suggesting that leadership commitment would perform better if working together with other factors to increase the effectiveness of managing cyber risk occurrence.

Risk management theory supports the results by mentioning that improvements in cybersecurity policies, employee training, and leadership commitment strengthen preventive and control mechanisms against cyber threats. Specifically, as emphasized by human capital theory, the greater correlation between cybersecurity training and cyber risk occurrence highlights the main role that employee competencies play in reducing operational vulnerabilities (Becker, 1993). Meanwhile, the positive relationships involving policies and leadership commitment highlight the importance of institutional governance and managerial control in promoting cybersecurity compliance and risk awareness. These findings demonstrate that cyber risk management within MBSA is influenced by organizational structures and behavioral factors.

Advanced International Journal of Business, Entrepreneurship and SME's
AIJBES
EISSN: 2682-8545
Volume: 8 Issue: 29 (September 2026) PP. 435-456

Multiple Regression Analysis

Multiple regression analysis examines whether independent variables (cybersecurity policies, cybersecurity training, and leadership commitment) influence the dependent variable (cyber risk occurrence). However, prior to multiple regression, there are some assumptions, such as multicollinearity, outliers, normality, homoscedasticity of residuals, and autocorrelation, that should be reported to ensure that the data can actually be analyzed using multiple regression. The results showed that all study variables had lower than 5 VIF values, ranging from 2.45 to 2.47; thus, it could be assumed that there is no multicollinearity (Daoud, 2017). For checking outliers, the results showed that the value was less than 4/n; thus, there are no outliers (Cook, 1979). For checking normality, the P-P plot and histogram showed that the data are normally distributed. Next, the dots in the scatterplot were all equally distributed and did not have an obvious pattern; thus, the data could be assumed as achieving homoscedasticity. Last but not least, the autocorrelation was tested by Durbin-Watson, and since the d value is between the ranges of 1.5 to 2.5, it is thus considered acceptable (Kenton, 2025).

Table 3: Result of Multiple Regression Analysis

Variables	Beta	Std. Error	β	t	p
Constant	13.54	1.07		12.70	.00**
Cybersecurity Policies (CP)	.70	.45	.15	1.56	.12
Cybersecurity Training (CT)	1.06	.52	.20	2.05	.04*
Leadership Commitment (LC)	-.06	.37	-.02	-.15	.88

Note: Significant level=** p <.01, * p <.05, F= 8.56, R= .31, R^2= .10, Adjusted R^2= .09

Table 3 shows that the multiple regression model significantly predicted CRO, F (3, 238) = 8.56, $p < .001$, and an adjusted R^2 of .10 implies that those predictor variables (cybersecurity policies, cybersecurity training, and leadership commitment) explained about 10% of the variance, R^2 =. 10. Moreover, the F statistic was 8.56, with a significance value less than .001, indicating that the overall regression model is statistically significant and a good fit for the model.

Based on the findings, only cybersecurity training ($\beta = 1.06$, $p < 0.05$) significantly predicts and influences cyber risk occurrence. If the organizations put in efforts and provide cybersecurity training to their employees, they tend to be more effective in handling cyber risk occurrences, and this is consistent with the past studies that mentioned the effectiveness of cybersecurity training in influencing cyber risk occurrence (Goswami et al., 2023; Aliane & Zakariya, 2023). Besides, cybersecurity training is the most influential organizational factor in predicting cyber risk occurrence within MBSA. This result is supported by human capital theory, which mentioned that employee knowledge and competencies are critical resources for mitigating operational risks (Becker, 1993).

In contrast, cybersecurity policies and leadership commitment did not predict cyber risk occurrence in this study. This suggests that policies and leadership support alone may be insufficient to reduce cyber risks unless they include training programs as well. From the perspective of risk management theory, this finding implies that risk controls become effective only when supported by adequate human competencies and operational implementation.

Advanced International Journal of Business, Entrepreneurship and SME's
AIJBES
EISSN: 2682-8545
Volume: 8 Issue: 29 (September 2026) PP. 435-456

Furthermore, the relatively low explanatory power of the model (Adjusted R^2 = .09) indicates that cyber risk occurrence could be influenced by additional factors, such as technological infrastructure, third-party risks, and external threat environments. Nevertheless, the significant role of training highlights its importance as a main factor in strengthening organizational cyber resilience within MBSA.

Table 4 presents the summary of the hypothesis testing results. The findings indicated that two alternative hypotheses are rejected. These results are in contrast with the past research, which mentioned that cybersecurity policies are necessary to reduce cyber risks (Gupta & Remella, 2025; Chong et al., 2022), and the prior studies, which highlighted the importance of leadership commitment in cyber risk management (Sarumi & Abdul-Raheem, 2022; Herath & Rao, 2009). The present study recorded significant findings that cybersecurity training significantly contributes to cyber risk occurrence.

Table 4: Hypothesis Testing

Hypothesis	Independent Variable	Beta (β)	p-value	Supported
H1: Cybersecurity policies significantly reduce cyber risk occurrence at MBSA	Cybersecurity Policies (CP)	.15	.12	No
H2: Cybersecurity training significantly reduces cyber risk occurrence at MBSA.	Cybersecurity Training (CT)	.20	<0.05	Yes
H3: Leadership commitment significantly reduces cyber risk occurrence at MBSA.	Leadership Commitment (LC)	-.02	.88	No

Conclusion

This study examined the influence of Cybersecurity Policies (CP), Cybersecurity Training (CT), and Leadership Commitment (LC) on Cyber Risk Occurrence (CRO) within Majlis Bandaraya Shah Alam (MBSA). The findings contribute to the understanding of the organizational determinants of cyber risk occurrence in Malaysian local authorities.

The Pearson correlation analysis indicated that cybersecurity policies, cybersecurity training, and leadership commitment were significantly associated with cyber risk occurrence. However, the multiple regression analysis revealed that only cybersecurity training significantly predicted cyber risk occurrence after controlling for the other organizational factors. This finding suggests that while cybersecurity policies and leadership commitment are important components of cybersecurity governance, employee training is the strongest organizational determinant influencing cyber risk occurrence within MBSA.

The findings support Human Capital Theory by demonstrating that continuous investment in employee knowledge, skills, and cybersecurity awareness strengthens organizational capability to identify, prevent, and respond to cyber threats. The study also reinforces Risk Management Theory by highlighting the importance of organizational governance mechanisms in supporting cybersecurity resilience. Although cybersecurity policies and leadership commitment were not significant predictors in the regression model, they remain important organizational

mechanisms that facilitate effective cybersecurity governance and provide the foundation for successful cybersecurity training initiatives.

From a practical perspective, the findings suggest that MBSA should give greater attention to continuous cybersecurity training for employees. The training programmes should not focus only on general cybersecurity awareness but also include practical activities, such as phishing simulations, role-specific cybersecurity training, and incident response exercises. Regular refresher training should also be conducted to address emerging cyber threats. In addition, the effectiveness of the training programmes should be periodically evaluated to ensure that employees are able to apply their cybersecurity knowledge and skills in their respective work roles.

Acknowledgements:	The authors would like to express their sincere appreciation to Majlis Bandaraya Shah Alam (MBSA) for granting permission to conduct this study and for the cooperation provided throughout the data collection process. The authors also wish to thank Universiti Teknologi MARA (UiTM) for its academic support and the respondents who generously participated in this research. Their valuable contributions have greatly supported the successful completion of this study.
Funding Statement:	No Funding
Conflict of Interest Statement:	The authors declare that there is no conflict of interest regarding the publication of this paper. All authors have contributed substantially to this research and have read and approved the final version of the manuscript for submission to the Advanced International Journal of Business, Entrepreneurship and SMEs (AIJBES).
Ethics Statement:	This study was conducted in accordance with standard academic integrity and publication ethics guidelines. Prior to data collection, all participants were provided with information regarding the purpose of the study, and informed consent was obtained electronically. Participation was voluntary, and respondents were assured that their responses would remain confidential and anonymous. All data collected were used solely for academic research purposes.
Author Contribution Statement:	The author solely contributed to the conceptualization, research design, literature review, methodology, data collection, data analysis, interpretation of findings, manuscript preparation, revision, and final approval of this manuscript.

Advanced International Journal of Business, Entrepreneurship and SME's
AIJBES
EISSN: 2682-8545
Volume: 8 Issue: 29 (September 2026) PP. 435-456

References

Aliane, N., & Zakariya, A. (2023). Enhancing cyber security resilience in the industrial sector: A comprehensive framework for third-party risk management. *International Journal of Cyber Criminology, 17*(2), 262–283. https://doi.org/10.5281/zenodo.4766716.

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee compliance behavior. *Computers & Security, 98*, 101734. https://doi.org/10.1016/j.cose.2020.101734

Alshaikh, M., Maynard, S. B., Ahmad, A., & Chang, S. (2021). *Policy communication & employee compliance*. Section: *Information security policy effectiveness*, pp. 1–9. https://doi.org/10.1016/j.cose.2021.102202

Avast Business (2025). *City of Atlanta Ransomware Attack*. Gen Digital Inc. https://www.avast.com/en-my/business/resources/atlanta-ransomware#pc.

Bass, B. M., & Avolio, B. J. (1994). *Improving organizational effectiveness through transformational leadership*. Sage Publications.

Becker, G. S. (1993). *Human capital: A theoretical and empirical analysis with special reference to education* (3rd ed.). The University of Chicago Press.

Chong, W. F., Feng, R., Hu, H., & Zhang, L. (2025). Cyber risk assessment for capital management. *Journal of Risk and Insurance, 92*(2), 424–471. https://doi.org/10.1111/jori.12504

Cook, R. D. (1979). Influential observations in linear regression. *Journal of the American Statistical Association*, *74*(365), 169-174. https://doi.org/10.1080/01621459.1979.10481634

Cortina, J. M. (1993). What is coefficient alpha? An examination of theory and applications. *Journal of Applied Psychology*, *78*(1), 98. https://doi.org/10.1037/0021-9010.78.1.98

Cyber Security Agency of Singapore. (2021). *Singapore cybersecurity strategy*, pp. 18–25. https://www.csa.gov.sg/Strategy/singapore-cybersecurity-strategy

Cyber Security Agency of Singapore. (2021). *The Singapore Cybersecurity Strategy 2021 (Policy document)*. Government of Singapore. https://www.csa.gov.sg/resources/publications/the-singapore-cybersecurity-strategy-2021/

Daoud, J. I. (2017, December). Multicollinearity and regression analysis. *Journal of Physics: Conference Series,* 949(*1*). https://doi.org/10.1088/1742-6596/949/1/012009

Das, K. R., & Imon, A. H. M. R. (2016). A brief review of tests for normality. *American Journal of Theoretical and Applied Statistics, 5*(1), 5-12. https://doi.org/10.11648/j.ajtas.20160501.12

Equifax Inc. (2017). *Equifax announces cybersecurity incident involving consumer information*, pp. 4–7. https://www.equifax.com/personal/education/identity-theft/articles/-/learn/equifax-data-breach/

European Union Agency for Cybersecurity (ENISA),2022. Cybersecurity training, skills development, phishing and credential misuse in public sector organisations. Pages 22–35.

European Union Agency for Cybersecurity. (2026). *Cybersecurity certification framework*. ENISA. https://www.enisa.europa.eu/topics/product-security-and-certification/cybersecurity-certification-framework

Fabritius, P. (2019). Baltimore ransomware attack costs city over $18 million. *Government Technology*.

https://www.govtech.com/security/Baltimore-Ransomware-Attack-Costs-City-Over-18M.html

Fabritius, W. (2019). July 25). *Ransomware attack shows Baltimore's lack of organizational resilience.* https://www.route-fifty.com/digital-government/2019/07/ransomware-baltimore-organizational-resilience/158314/

Goswami, S. S., Sarkar, S., Gupta, K. K., & Mondal, S. (2023). The role of cyber security in advancing sustainable digitalization: Opportunities and challenges. *Journal of Decision Analytics and Intelligent Computing, 3*(1), 270–285. https://doi.org/10.31181/jdaic10018122023g

Goswami, S., Dey, S., & Mukherjee, S. (2023). Human factors in cybersecurity risk management: A systematic review. *Computers & Security, 124*, 102973, pp. 6–12. https://doi.org/10.1016/j.cose.2022.102973

Gupta, A., & Remella, S. (2025). Building resilience in hybrid cloud systems: Security frameworks for mission-critical applications — A systematic literature review. *International Journal of Computer Science and Mobile Computing, 14*(9), 52–62. https://doi.org/10.47760/ijcsmc.2025.v14i09.008

Hair, J. F., Hult, G. T. M., Ringle, C. M., Sarstedt, M., & Thiele, K. O. (2017). Mirror, mirror on the wall: A comparative evaluation of composite-based structural equation modeling methods. *Journal of the Academy of Marketing Science*, *45*(5), 616-632. https://doi.org/10.1007/s11747-017-0517-x

Heal, R., & Twycross, A. (2015). Validity and reliability in quantitative research. *Evidence-Based Nursing*, 66-67. https://doi.org/10.1136/eb-2015-102129

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2),154–165. https://doi.org/10.1016/j.dss.2009.02.005

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106–125. https://doi.org/10.1057/ejis.2009.6

https://www.enisa.europa.eu/publications/cybersecurity-skills-development

https://www.iso.org/standard/27001

InfoMSP. (2025, May 30). *Definition of cyber risk management*. InfoMSP. https://www.infomsp.com/whatis/definition/cyber-risk-management/

Insurica (2025, April 25). *Cyber case study: Colonial Pipeline ransomware attack*. Insurica. https://insurica.com/blog/colonial-pipeline-ransomware-attack/

International Organization for Standardization. (2018). *ISO/IEC 27005:2018 — Information technology — Security techniques — Information security risk management*. ISO, Clauses 6–8. https://www.iso.org/standard/75281.html

International Organization for Standardization. (2022). *ISO/IEC 27001:2022 — Information security management systems — Requirements*. https://www.iso.org/standard/27001

ISO/IEC (2022), *Information Security Management governance*. ISO/IEC 27001:2022 – Clause 5 (Leadership), Clause 6 (Planning), Annex A.5 (Information Security Policies)

Jackson, S. L. (2012). *Research methods and statistics: A critical thinking approach* (4th ed.). Wadsworth Publishing.

Kenton, W. (2025, October). *Durbin Watson Test explained: Understanding autocorrelation in regression analysis*. Investopedia. https://www.investopedia.com/terms/d/durbin-watson-statistic.asp

Kline, R. B. (2011). *Principles and practice of structural equation modeling (5th ed.*). The Guilford Press.

Masson, V. L. (2025, June 26). *The magic number: How to optimize and improve your survey response rate*. Kantar.

Mohajan, H. K. (2017). Two criteria for good measurements in research: Validity and reliability. *Economic Series, 17*(4), 59-82.

National Audit Office – NAO (2018), National Health Service – WannaCry ransomware attack, Part Two: *Why the attack succeeded*, pp. 18–27. https://www.nao.org.uk/reports/investigation-wannacry-cyber-attack-and-the-nhs/

National Audit Office (NAO), United Kingdom, 2018. National Health Service – WannaCry ransomware attack, Staff awareness, outdated training, organisational preparedness, Pages 18–27. https://www.nao.org.uk/reports/investigation-wannacry-cyber-attack-and-the-nhs/

National Audit Office. (2018). *Investigation: WannaCry cyber attack and the NHS.* https://www.nao.org.uk/reports/investigation-wannacry-cyber-attack-and-the-nhs/

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2017). *Human behaviour, phishing awareness, password practices, cybersecurity training effectiveness.* Pages 165–172. https://doi.org/10.1016/j.cose.2017.01.002

Ponemon Institute. (2020). *Cost of a data breach report 2020 (Research report).* IBM Security & Ponemon Institute. https://www.capita.com/sites/g/files/nginej291/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pd

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly, 34*(4), 757–778. https://doi.org/10.2307/25750704

Puhakainen, P., & Siponen, M. T. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly, 34*(4), 757–778. https://doi.org/10.2307/25750704

Saccenti, E., Hendriks, M. H., & Smilde, A. K. (2020). Corruption of the Pearson correlation coefficient by measurement error and its estimation, bias, and correction under different error models. *Scientific Reports*, *10*(1), 438. https://doi.org/10.1038/s41598-019-57247-4

Sarumi, A. O., & Abdul-Raheem, I. (2022). Leadership commitment and cybersecurity governance in public organizations. *Journal of Information Security and Applications, 67*, 103176, pp. 5–9. https://doi.org/10.1016/j.jisa.2022.103176

Sarumi, J., & Abdul-Raheem, I. (2022). Ethical hacking and cyber security in Nigerian telecommunication industry. *Advances in Multidisciplinary & Scientific Research Journal Publication, 10*(1), 1–36.

Schmitt, N. (1996). Uses and abuses of coefficient alpha. *Psychological Assessment*, *8*(4), 350. https://doi.org/10.1037/1040-3590.8.4.350

Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management, 46*(5), 267–270. https://doi.org/10.1016/j.im.2008.12.007

Traynor, O. (2025, March 24). *NIST Cybersecurity Framework 2.0: An Overview*. https://cybelangel.com/blog/guide_nist_2/

U.S. Department of Justice (DOJ), 2018. *City of Atlanta ransomware attack / Employee preparedness, cybersecurity training gaps, incident escalation*, Pages 4–9. https://www.justice.gov/criminal-ccips/file/1096976/download

U.S. Government Accountability Office – GAO (2021). *SolarWinds supply-chain cyberattack*. GAO-21-105325, pp. 9–18 (Root causes & governance gaps). https://www.gao.gov/products/gao-21-105325

U.S. House Committee on Oversight and Reform. (2018). *The Equifax data breach* (Majority staff report). https://oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf

United Nations Department of Economic and Social Affairs. (2022). *United Nations E-Government Survey 2022: The future of digital government (Report)*. United Nations. https://unpan.un.org/sites/unpan.org/files/Full%20report%20and%20annexes%20%28English%29.pdf