Science World Journal Vol. 20(No 4) 2025 https://dx.doi.org/10.4314/swj.v20i4.55
www.scienceworldjournal.org
ISSN: 1597-6343 (Online), ISSN: 2756-391X (Print)
Published by Faculty of Science, Kaduna State University

Full Length Research Article

EVALUATING CYBERSECURITY RESILIENCE IN FINANCIAL INSTITUTIONS: A STUDY ON RISK MITIGATION, INCIDENT RESPONSE, AND COMPLIANCE

*Onwubiko E.I., Chaku E.S., Kulugh E.V., Amufua O.I.G.

Centre for Cyberspace Studies, Nasarawa State University, Keffi, Nasarawa State, Nigeria

*Corresponding Author Email Address: emmadesaint@yahoo.co.uk

ABSTRACT

The increasing digitization of financial services has heightened the vulnerability of financial institutions to cyber threats, making cyber security resilience a strategic organizational capability. This study evaluates resilience to cyber threats in financial institutions by examining the roles of risk mitigation practices, incident response capability, and regulatory compliance frameworks. The study was conducted using a quantitative, cross-sectional design, with data collected from 148 respondents involved in cyber security governance, risk management, and regulatory compliance through a structured Likert-scale questionnaire. Descriptive analysis revealed that regulatory compliance recorded the highest mean score (M = 4.05, SD = 0.58), followed by risk mitigation (M = 3.82, SD = 0.61), with incident response capability showing comparatively lower scores (M = 3.47, SD = 0.74 which indicated variability in preparedness across institutions. Reliability analysis demonstrated strong internal consistency (Cronbach's α ranging from 0.81 to 0.88). Pearson correlation analysis indicated statistically significant positive relationships between all predictors and cyber security resilience, with incident response capability exhibiting the strongest correlation ($r = 0.74$, $p < 0.01$). Multiple regression analysis confirmed that risk mitigation ($\beta = 0.31$, $p < 0.001$), incident response capability ($\beta = 0.43$, $p < 0.001$), and regulatory compliance ($\beta = 0.19$, $p = 0.002$) collectively explained 62% of the variance in cyber security resilience ($R^2 = 0.62$). Findings highlighted that while risk mitigation and compliance formed essential foundations, incident response capability is the most critical determinant of overall resilience. The study underscores the need for integrated, resilience-oriented cyber security strategies that emphasize preparedness, adaptive response, and operational continuity. The results offered actionable insights for financial institutions and regulators to enhance cyber resilience in an increasingly complex threat landscape.

Keywords*: Cyber security resilience, Financial institutions, Risk mitigation, Incident response, Regulatory compliance, Operational continuity*

INTRODUCTION

The increasing digitization of financial services has significantly expanded the attack surface of financial institutions, making cyber security resilience a critical organizational capability rather than a purely technical concern. Financial institutions operate complex, interconnected information systems that process high-value transactions and sensitive customer data, rendering them prime targets for cyberattacks such as ransomware, phishing, insider threats, and advanced persistent threats. Peer-reviewed studies consistently identify the financial sector as one of the most frequently targeted industries due to its systemic importance and potential for financial gain (Kopp *et al*., 2021; Eling & Schnell, 2022). Consequently, the ability of financial institutions to anticipate, withstand, respond to, and recover from cyber incidents has emerged as a central determinant of operational stability and public trust.

This resilience construct is theoretically grounded in risk management, systems theory, and organizational resilience frameworks. From a risk management perspective, cyber security resilience extends beyond preventive controls to include adaptive capabilities that enable institutions to maintain critical functions during and after cyber disruptions (ISO 31000; NIST, 2024). Systems theory further emphasizes that failures in one component of a financial system can propagate across interconnected networks, amplifying the impact of cyber incidents. This interconnectedness necessitates a holistic approach to cyber security that integrates risk mitigation strategies, incident response capabilities, and regulatory compliance mechanisms into a unified governance framework (Linkov et al., 2020) Unlike traditional cyber security models that prioritize perimeter defence, resilience-oriented models recognize cyber incidents as inevitable and focus on minimizing operational and financial impact.

Recent empirical research highlights that while many financial institutions invest heavily in technical security controls, deficiencies persist in incident response coordination, organizational preparedness, and regulatory alignment (Torkura *et al*., 2021; Eling *et al*., 2023). Incident response effectiveness is influenced not only by technical detection mechanisms but also by governance structures, decision-making speed, employee awareness, and cross-functional collaboration. Furthermore, regulatory compliance driven by frameworks such as the International Organization for Standardization/International Electrotechnical Commission ISO/IEC 27001, the Payment Card Industry Data Security Standard (PCI DSS), and the General Data Protection Regulation (GDPR), and national financial regulations plays a dual role by both enforcing minimum security standards and shaping institutional risk management behaviour. However, compliance alone does not guarantee resilience, as organizations may adopt a checkbox approach that overlooks adaptive and recovery-oriented capabilities.

The importance of this study is underscored by the increasing financial and systemic consequences of cyber incidents in the banking and financial services sector. Cyber disruptions can lead to direct financial losses, reputational damage, regulatory penalties, and broader economic instability. As financial systems form the backbone of national economies, weaknesses in cyber security resilience pose risks that extend beyond individual institutions. Understanding how risk mitigation strategies, incident response mechanisms, and compliance practices interact to influence overall cyber security resilience is therefore essential for both organizational leaders and regulators.

The primary goal of this research is to evaluate the level of cyber security resilience in financial institutions by examining the effectiveness of risk mitigation practices, incident response capabilities, and regulatory compliance frameworks. Specifically, the study investigates how these factors contribute to an institution's ability to prevent cyber incidents, respond effectively when incidents occur, and maintain operational continuity. The research is guided by the hypothesis that financial institutions with integrated risk management processes, well-coordinated incident response structures, and proactive compliance approaches exhibit higher levels of cyber security resilience than those relying primarily on technical controls or regulatory adherence alone.

This study was undertaken to address the gap between theoretical cyber security resilience models and their practical implementation within financial institutions. By empirically assessing the interplay between technical, organizational, and regulatory dimensions of cyber security, the research aims to contribute to the growing body of literature on cyber resilience and provide actionable insights for improving cyber security governance in the financial sector. Ultimately, the findings are intended to support the development of more resilient financial systems capable of withstanding an increasingly complex cyber threat landscape.

MATERIALS AND METHODS

Research Design

This study adopted a quantitative, cross-sectional research design to evaluate resilience outcomes in financial institutions, with specific emphasis on risk mitigation practices, incident response capabilities, and regulatory compliance mechanisms. The design was selected to enable systematic measurement of cyber security resilience constructs at a single point in time and to facilitate statistical analysis of relationships among key variables. A structured survey-based approach was employed, complemented by document-based assessments of institutional cyber security practices where applicable.

Study Setting and Sampling Technique

The study focused on financial institutions operating within regulated financial environments and subject to established cyber security and data protection requirements. A **purposive sampling technique** was employed to select participating institutions and respondents with direct involvement in cyber security governance, risk management, information security operations, and regulatory compliance. This approach ensured that data were collected from individuals with sufficient technical and managerial expertise to provide informed assessments of cyber security resilience practices.

The rationale for using purposive sampling lies in the specialized nature of cyber security functions within financial institutions, where relevant knowledge is typically concentrated among specific roles rather than distributed across the general workforce. However, the use of purposive sampling introduces potential limitations, including **selection bias and reduced generalizability** of findings beyond the sampled institutions. These limitations were mitigated by targeting diverse functional roles and ensuring representation across multiple cyber security domains, although the results should still be interpreted within the contextual boundaries of the sampled institutions.

Data Collection Instruments

Data were collected using a structured questionnaire designed to measure three primary dimensions of cyber security resilience: risk mitigation, incident response, and regulatory compliance. The questionnaire items were developed based on established cyber security frameworks and standards, including the NIST Cyber security Framework, ISO/IEC 27001, and prior peer-reviewed empirical studies on cyber resilience in the financial sector. Where applicable, validated measurement scales from existing literature were adapted to fit the financial institution context.

The questionnaire consisted of closed-ended questions using a Likert-scale format to capture respondents' perceptions of cyber security practices, preparedness, and effectiveness. The instrument also included items assessing governance structures, policy enforcement, employee awareness, and post-incident recovery capabilities. To ensure content validity, the questionnaire was reviewed against relevant standards and previously published instruments, and ambiguous items were refined prior to data collection.

Data Collection Procedure

Data collection was conducted electronically to facilitate secure and efficient distribution of the questionnaire. Participants were provided with an explanation of the study's purpose and assured of confidentiality and anonymity. Participation was voluntary, and informed consent was obtained prior to data submission. Respondents completed the questionnaire based on their institutional cyber security practices and operational experiences.

To support reproducibility, the data collection protocol followed standardized procedures for survey administration, including consistent instructions, uniform question sequencing, and controlled access to the survey platform. Protocols for questionnaire design and electronic survey administration align with established methods reported in prior cyber security and information systems research and are therefore not described in full detail here.

Operationalization of Variables

The dependent variable was operationalized as a multidimensional construct comprising risk mitigation effectiveness, incident response capability, and regulatory compliance maturity. Risk mitigation was assessed through indicators related to preventive controls, vulnerability management, and risk assessment processes. Incident response capability was measured using indicators such as detection speed, response coordination, communication effectiveness, and recovery planning. Regulatory compliance was evaluated based on adherence to cyber security policies, audit readiness, and alignment with applicable regulatory frameworks.

Each construct was measured using composite indices derived from multiple questionnaire items, allowing for robust assessment of latent variables and minimizing measurement error.

Data Analysis Techniques

Collected data were analysed using the Statistical Package for the Social Sciences (SPSS), version 26. Descriptive statistics were used to summarize respondent characteristics and institutional cyber security practices. Both descriptive and inferential statistical techniques were employed, including correlation and regression analyses, were employed to examine relationships between risk mitigation, incident response, compliance, and overall cyber security resilience. Reliability analysis was conducted to assess internal consistency of measurement scales, while validity was evaluated through factor analysis where appropriate.

Analytical procedures followed established quantitative research protocols widely reported in cyber security and information systems literature, enabling replication of the analytical approach using the same instrument and procedures.

Ethical Considerations

Ethical considerations were observed throughout the study. No personally identifiable information was collected, and institutional identities were anonymised to prevent disclosure of sensitive security information. Data were stored securely and used solely for academic research purposes. The study adhered to accepted ethical standards for research involving human participants and organizational data.

RESULTS

This section presents the findings of the study. on cyber security resilience in financial institutions, focusing on risk mitigation, incident response, and regulatory compliance. Results are organized according to descriptive statistics, reliability analysis, and inferential statistical testing aligned with the study objectives.

Descriptive Analysis of Cyber security Resilience Constructs

Descriptive statistics were computed to summarize responses related to risk mitigation practices, incident response capabilities, regulatory compliance, and overall cyber security resilience. The results indicated that respondents generally reported moderate to high implementation of cyber security controls across all measured dimensions. Among the three constructs, regulatory compliance recorded the highest mean score, followed by risk mitigation, while incident response capability exhibited comparatively lower mean values, suggesting potential gaps in response preparedness and coordination.

The variability observed in incident response responses was higher than that of risk mitigation and compliance, indicating inconsistent implementation of incident handling procedures across institutions. Overall resilience scores suggest that while baseline controls are in place, adaptive and recovery-focused capabilities vary significantly as in Table 1.

Table 1: Descriptive Statistics of Cyber security Resilience Constructs

Variable	Mean	Standard Deviation
Risk Mitigation	3.82	0.61
Incident Response Capability	3.47	0.74
Regulatory Compliance	4.05	0.58
Cyber security Resilience	3.78	0.63

Reliability Analysis of Measurement Scales

Internal consistency reliability of the measurement instrument was assessed using Cronbach's alpha. All constructs demonstrated acceptable to strong reliability coefficients, exceeding the recommended threshold of 0.70. This indicates that the questionnaire items consistently measured their respective constructs.

Table 2: Reliability Analysis of Study Constructs

Cyber security Resilience	Cronbach's Alpha
Risk Mitigation	0.84
Incident Response Capability	0.81
Regulatory Compliance	0.86
Cyber security Resilience	0.88

Correlation Analysis

Correlation analysis was performed to examine the strength and direction of the linear relationship between the variables. The **Pearson correlation coefficient (r)** was computed using the following formula:

$$r = \sum(Xi - X)(Yi - Y)$$

$$\sqrt{\sum(X_i - X)^2 \sum(Y_i - Y)^2}$$

Where:

- X_i and Y_i are the observed values of the two variables,
- X and Y are the means of the respective variables,
- r ranges from -1 to +1, indicating negative or positive correlation.

Basic Assumptions:

1. Both variables are measured on at least an interval scale.
2. The relationship between the variables is linear.
3. The data are normally distributed (for significance testing).
4. There are no significant outliers.

Decision Criteria:

- If $|r| \geq 0.70$, the correlation is considered strong;
- $0.50 \leq |r| < 0.70$, moderate;
- $0.30 \leq |r| < 0.50$, weak;
- $|r| < 0.3$, negligible.

Statistical significance of the correlation was evaluated using a **t-test**, with the null hypothesis (H_0) that r = 0 (no correlation). A p-value less than 0.05 ($p < 0.05$) was used to reject the null hypothesis, indicating a statistically significant correlation.

Application to this study:

The **Pearson product-moment correlation analysis** was conducted to examine the relationships between risk mitigation, incident response capability, regulatory compliance, and cyber security resilience. The results revealed statistically significant positive correlations between all independent variables and cyber security resilience. Incident response capability exhibited the strongest correlation with cyber security resilience, followed by risk mitigation and regulatory compliance. These findings suggest that improvements in technical controls alone are insufficient without effective response and recovery mechanisms.

The correlation coefficients are presented in **Table 3**.

Table 3: Pearson Correlation Matrix

Variable	Risk Mitigation	Incident Response Capability	Regulatory Compliance	Cyber security Resilience
Risk Mitigation	1			
Incident Response Capability	0.62**	1		
Regulatory Compliance	0.55**	0.59**	1	
Cyber security Resilience	0.68**	0.74**	0.61**	1

Note: ** Correlation is significant at *p* < 0.01.

Regression Analysis

Multiple linear regression analysis was performed to assess the predictive influence of risk mitigation, incident response capability, and regulatory compliance on cyber security resilience.

Regression Model

The multiple regression model is specified as follows:
CSR = β_0 + β_1(Risk Mitigation) + β_2(Incident Response Capability) + β_3(Regulatory Compliance) + ε
Where:

- **CSR** represents cyber security resilience (dependent variable),
- β_0 is the intercept,
- β_1, β_2, β_3 are the regression coefficients of the independent variables, and
- ε denotes the error term.

Basic Assumptions of the Regression Model

The analysis was conducted based on the following assumptions of multiple linear regression:

1. A linear relationship exists between the dependent variable and each independent variable.
2. The residuals are normally distributed.
3. Homoscedasticity of residuals is assumed across all levels of the independent variables.
4. The observations are independent.
5. Multicollinearity among the independent variables is minimal.

Regression Results

The analysis was conducted using a sample size of *n* = 148. The overall regression model was statistically significant, indicating that the independent variables collectively explain a substantial proportion of variance in cyber security resilience. The model yielded an **R² value of 0.62**, suggesting that **62% of the variance in cyber security resilience** is explained by the predictors.
Incident response capability emerged as the strongest predictor of cyber security resilience, followed by risk mitigation, while regulatory compliance demonstrated a statistically significant but comparatively weaker effect.

Table 4: Predicting Cyber security Resilience (n = 148)
Table 4a: Analysis of Variance (ANOVA) for Multiple Regression Model Predicting Cyber Security Resilience (n = 148)

Source	Sum of Squares	df	Mean Square	F-value	p-value
Regression	92.84	3	30.95	78.64	< 0.001
Residual	56.92	144	0.4		
Total	149.76	147			

Note: Dependent variable: Cyber security resilience.
The analysis of variance (ANOVA) table indicates that the multiple regression model is statistically significant. The obtained F-statistic (F = 78.64, p < 0.001) demonstrates that the independent variables—risk mitigation, incident response capability, and regulatory compliance—collectively have a significant effect on cyber security resilience. This result confirms the suitability of the regression model and supports the conclusion that the predictors jointly explain a substantial proportion of variance in cyber security resilience.

Table 4b: Multiple Regression Results Predicting Cyber Security Resilience (n = 148)

Source	Sum of Squares	df	Mean Square	F-value	p-value
Regression	92.84	3	30.95	78.64	< 0.001
Residual	56.92	144	0.4		
Total	149.76	147			

Visualization of Structural Relationships

To visually illustrate the relationships among the study variables, a structural path model was developed based on the regression results. **Figure 1** highlights the relative strength of each predictor's influence on cyber security resilience, emphasizing the dominant role of incident response capability.

The path analysis implies that incident response capability exerts the strongest influence on cyber security resilience, indicating that organizations with effective detection, response, and recovery mechanisms are better positioned to enhance resilience against cyber threats. Risk mitigation also demonstrates a substantial positive influence, suggesting that proactive preventive controls contribute meaningfully to resilience. Although regulatory compliance shows a statistically significant relationship, its comparatively weaker influence implies that compliance requirements alone are insufficient to ensure robust cyber security resilience without strong operational and response capabilities.

Figure 1 presents the standardized path coefficients derived from the regression analysis. Numerical values shown in the figure complement, but do not duplicate, the detailed statistical results presented in Table 4.

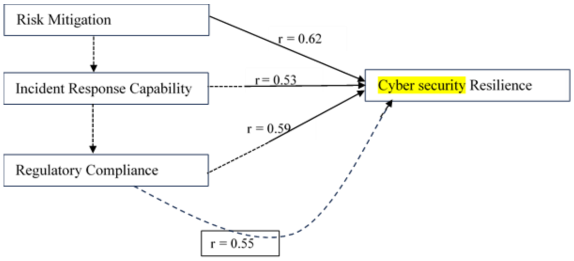

Figure 1: Structural Model of cyber security Resilience Predictors

DISCUSSION OF RESULTS

The objective of this study was to evaluate resilience outcomes in financial institutions by examining the roles of risk mitigation, incident response capability, and regulatory compliance. The findings provide empirical evidence that institutional resilience is not solely dependent on preventive technical controls or regulatory adherence, but rather on the effective integration of organizational, operational, and governance mechanisms. Overall, the results support the study's hypothesis that financial institutions with coordinated risk management processes, mature incident response capabilities, and proactive compliance approaches exhibit higher levels of cyber security resilience.

Interpretation of Key Findings

The results indicate that all three examined factors—risk mitigation, incident response capability, and regulatory compliance have statistically significant positive relationships with cyber security resilience. Among these, incident response capability emerged as the strongest predictor of resilience. This finding underscores the importance of an institution's ability to detect, respond to, and recover from cyber incidents, rather than focusing exclusively on incident prevention. Given the inevitability of cyber-attacks in highly digitized financial environments, this result aligns with resilience theory, which emphasizes adaptive capacity and rapid recovery as core resilience attributes.

Risk mitigation also demonstrated a strong and significant influence on cyber security resilience. This suggests that structured risk assessment processes, vulnerability management, and preventive controls remain foundational to resilience by reducing the likelihood and potential impact of cyber incidents. However, the comparatively lower influence of regulatory compliance indicates that while compliance contributes to baseline security maturity, it is insufficient on its own to ensure resilience. This finding highlights the limitation of compliance-driven cyber security strategies that prioritize audit readiness over operational preparedness.

Summary of Key Findings

The findings of this study demonstrate that cyber security resilience in financial institutions is significantly influenced by the combined effects of risk mitigation strategies, incident response capability, and regulatory compliance practices. Among these factors, incident response capability emerged as the most critical determinant of cyber security resilience. This result supports the study's hypothesis that institutions adopting coordinated and proactive cyber security approaches exhibit higher levels of resilience.

The prominence of incident response capability aligns with existing empirical and conceptual literature on cyber resilience. Linkov et al. (2019) emphasize that cyber resilience is fundamentally defined by an organization's ability to sustain critical operations during disruptive events, while Eling and Schnell (2022) similarly report that effective post-incident response significantly shapes financial and reputational outcomes within the financial sector. Furthermore, Torkura et al. (2021) highlight that incident response maturity—particularly in areas such as communication protocols, escalation procedures, and decision-making structures—is a key driver of organizational resilience. The present study reinforces these findings by empirically demonstrating the dominant role of incident response capability relative to other governance factors.

Risk mitigation was also found to have a significant positive influence on cyber security resilience. This finding is consistent with Kopp et al. (2021), who showed that proactive risk management practices reduce systemic cyber risk exposure in financial institutions. However, the present study extends prior research by illustrating that risk mitigation contributes most effectively to resilience when integrated with incident response and recovery capabilities, rather than functioning as a standalone preventive measure.

Although regulatory compliance exhibited a statistically significant relationship with cyber security resilience, its comparatively weaker effect supports concerns raised in the literature regarding compliance-driven security approaches. Studies have cautioned that frameworks such as ISO/IEC 27001 and sector-specific regulatory requirements often promote minimum security baselines without ensuring adaptive or operational resilience (Eling et al., 2023). The findings of this study provide empirical support for this perspective, indicating that compliance alone contributes less to resilience than active response and mitigation capabilities. This underscores the need for regulators and organizations to shift emphasis from control adherence toward resilience-oriented outcomes.

Conclusion

This study evaluated resilience to cyber threats in financial institutions by examining the integrated roles of risk mitigation, incident response capability, and regulatory compliance. The findings demonstrate that cyber security resilience is a multidimensional construct shaped not only by preventive security controls but also by an institution's capacity to respond effectively to cyber incidents and recover critical operations. The results confirm that financial institutions operating in highly regulated and threat-intensive environments must move beyond traditional compliance-driven cyber security approaches toward resilience-oriented strategies.

Empirical evidence from the study shows that while risk mitigation and regulatory compliance remain essential foundations of cyber security governance, incident response capability is the most influential determinant of overall cyber security resilience. This underscores the reality that cyber incidents are inevitable within modern financial systems and that organizational preparedness, coordination, and recovery capacity are critical for minimizing operational disruption and financial loss. These findings support contemporary resilience theories that emphasize adaptability, continuity, and recovery over absolute prevention (Linkov et al., 2020; Eling & Schnell, 2022).

The study contributes to the existing body of cyber security resilience literature by empirically validating an integrated model that examines the combined and comparative influence of risk mitigation, incident response, and regulatory compliance within financial institutions. Unlike prior studies that often considered these dimensions in isolation, this research provides a more holistic understanding of the drivers of cyber security resilience in the

https://dx.doi.org/10.4314/swj.v20i4.55

financial sector. In doing so, it reinforces the ongoing shift from prevention-centric cyber security models toward resilience-focused frameworks that prioritize preparedness and adaptability.

From a practical perspective, the findings highlight the need for financial institutions to prioritize the development of mature incident response capabilities alongside traditional risk mitigation controls. This includes investments in response planning, regular incident simulation exercises, clearly defined escalation procedures, and the integration of cyber security response within broader business continuity and crisis management frameworks. While regulatory compliance contributes positively to resilience, its comparatively weaker influence suggests that compliance alone is insufficient to ensure preparedness for complex and evolving cyber threats.

From a policy standpoint, the results suggest that regulators and policymakers may consider complementing existing compliance requirements with resilience-oriented metrics that assess incident response readiness, recovery effectiveness, and adaptive capacity. Emphasizing operational resilience alongside control adherence may better position financial institutions to withstand and recover from increasingly sophisticated cyber threats.

Overall, this study provides actionable insights for both practitioners and policymakers by demonstrating that cyber security resilience in financial institutions is best achieved through a balanced and integrated approach that combines proactive risk mitigation, robust incident response capability, and supportive regulatory frameworks.

Recommendations

Based on the findings of this study, financial institutions should prioritize the continuous development of incident response capabilities as a core component of cyber security resilience. This includes regular cyber incident simulations, clearly defined escalation procedures, and the establishment of cross-functional response teams that enable rapid and coordinated decision-making during cyber incidents. Incident response should be fully integrated into enterprise risk management and business continuity planning to minimize operational disruption and financial loss.

Institutions are also encouraged to adopt integrated cyber resilience frameworks that align risk mitigation, incident response, and regulatory compliance activities. Rather than treating these functions as isolated domains, organizations should ensure that risk assessments directly inform response planning and that compliance efforts support resilience objectives rather than purely audit-driven outcomes. In this regard, regulatory bodies and institutional leaders should place greater emphasis on resilience-oriented performance indicators, such as response readiness, recovery capability, and operational continuity, alongside traditional compliance metrics.

Furthermore, effective cyber security resilience requires strong governance structures and organization-wide awareness. Executive-level oversight, clearly defined accountability mechanisms, and inclusive training programs that extend beyond technical staff to senior management and non-technical stakeholders are essential for strengthening cyber preparedness and response effectiveness. Finally, future research may build on this study by adopting longitudinal designs to examine how cyber security resilience evolves over time, incorporating qualitative approaches to explore organizational and cultural factors influencing incident response effectiveness, and expanding analyses across diverse financial systems and regulatory environments to enhance the generalizability of findings.

REFERENCES

Eling, M., & Jung, K. (2021). Cyber risk governance: A framework for financial institutions. *Journal of Risk Finance, 22*(3), 219–234. https://doi.org/10.1108/JRF-01-2021-0012

Eling, M., McShane, M., & Nguyen, T. (2023). Cyber risk management: History and future research directions. *Risk Management and Insurance Review, 26*(1), 5–33. https://doi.org/10.1111/rmir.12219

Eling, M., & Schnell, W. (2022). What do we know about cyber risk and cyber risk management? *Journal of Risk and Insurance, 89*(2), 275–308. https://doi.org/10.1111/jori.12355

European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union, L119*, 1–88.

International Organization for Standardization & International Electrotechnical Commission. (2022). *ISO/IEC 27001:2022 information security, cybersecurity and privacy protection—Information security management systems—Requirements*. ISO.

Kopp, E., Kaffenberger, L., & Wilson, C. (2021). Cyber risk, market failures, and financial stability. *IMF Working Papers, 2021*(185). https://doi.org/10.5089/9781513595155.001

Linkov, I., Trump, B. D., & Florin, M. V. (2020). *Cyber resilience: A systems approach to cyber risk*. Springer Nature. https://doi.org/10.1007/978-3-030-31875-7

National Institute of Standards and Technology. (2024). *Cybersecurity framework* (Version 2.0). NIST.

Organisation for Economic Co-operation and Development. (2023). *Cyber resilience in the financial sector*. OECD Publishing. https://doi.org/10.1787/5f9b6c8a-en

Payment Card Industry Security Standards Council. (2022). *Payment Card Industry data security standard* (Version 4.0). PCI SSC.

PwC. (2022). *Global digital trust insights: Financial services focus*. PricewaterhouseCoopers.

Radanliev, P., De Roure, D., Burnap, P., & Nicolescu, R. (2020). Cyber risk analytics for cyber insurance and cyber risk governance. *Journal of Cybersecurity, 6*(1), tyaa003. https://doi.org/10.1093/cybsec/tyaa003

Srinidhi, B., Yan, J., & Tayi, G. K. (2021). Cybersecurity risk management: A strategic governance perspective. *MIS Quarterly, 45*(2), 923–948. https://doi.org/10.25300/MISQ/2021/15846

Torkura, K. A., Cheng, F., & Meinel, C. (2021). Cloud security incident response automation. *IEEE Transactions on Cloud Computing, 9*(2), 532–545. https://doi.org/10.1109/TCC.2018.2794265

World Economic Forum. (2021). *Cyber resilience in financial services: A global perspective*. World Economic Forum.

Zhao, L., Xue, L., & Whinston, A. B. (2024). Organizational resilience to cyber incidents: Evidence from financial institutions. *Information Systems Research, 35*(1), 77–96. https://doi.org/10.1287/isre.2023.1201