**Evaluating the Cost-Benefit Dynamics of Cybersecurity Compliance Investments: A Multi-Sectoral Analysis Across Financial, Energy, and Intelligence Industries.**

**Abstract**

*This study examines the cost-benefit dynamics of cybersecurity compliance across the financial, energy, and military intelligence sectors, utilising open-access datasets from the BLS, Statista, Verizon DBIR, ENISA, and IBM. A one-way ANOVA, chi-square test, cost-benefit analysis, and logistic regression were employed to analyse sectoral differences in compliance costs, breach reductions, return on compliance investment (ROCI), and institutional success factors. Results show that financial institutions incur the highest average compliance costs ($30.94 million), while military intelligence yields the highest Return on Capital Invested (ROCI) (1.67). Compliance reduces breach incidents by 57.14% in finance, 50% in energy, and 48.57% in intelligence. Regression findings highlight workforce capacity (β = 3.06, p = .019) and training investment (β = 0.00044, p < .001) as strong predictors of compliance success, while budget constraints significantly hinder outcomes (β = -4.11, p < .001). It is recommended that regulatory bodies develop sector-specific frameworks, expand budget flexibility, institutionalise role-specific training, and incentivise automation and intelligence sharing.*

**Keywords: Cybersecurity compliance, Cost-benefit analysis, Sectoral comparison, Return on investment, Logistic regression**

**1. Introduction**

The rapid digitization of organizational processes across the financial, energy, and military intelligence sectors has elevated cybersecurity to a strategic imperative. As the volume of sensitive information stored and transmitted online increases, organizations face mounting pressure to comply with national and international data protection standards. Compliance has transitioned from a discretionary consideration to a legal obligation, serving as a cornerstone of operational resilience and reputational management. This necessity is underscored by the escalating complexity and scale of cyber threats, which pose significant financial, legal, and operational risks to organizations.

According to IBM (2024), the global average cost of a data breach reached $4.88 million in 2024, marking a 10% increase from the previous year and representing the highest figure on record. In the United States, the average cost rose to $9.36 million, highlighting the heightened vulnerability of American enterprises (Petrosyan, 2024). Sector-specific analyses reveal further disparities: Thompson (2024) reports that financial institutions experienced average breach costs of $6.08 million, second only to the healthcare industry. The energy sector, encompassing utilities and critical infrastructure, recorded average breach costs of $3.48 million, a 17.6% year-over-year increase (Upwind, 2025). Meanwhile, the military intelligence sector faced average breach costs of $3.65 million in 2023 (Sutton, 2023).

The financial implications of non-compliance are particularly severe, as financial institutions allocate approximately $30.9 million annually to compliance efforts (Mahanti, 2021). However, violations of regulations such as the Gramm-Leach-bliley Act (GLBA) can result in fines up to $100,000 per violation (Oberheiden, 2021), while breaches of the Sarbanes-Oxley Act (SOX) may incur criminal penalties, including imprisonment of up to 20 years (NS, 2025). In the energy sector, failure to adhere to industry-specific cybersecurity standards can result in substantial fines and operational disruptions. Enforcement under various energy regulations has intensified, as demonstrated by recent cases resulting in significant penalties for non-compliance (Merken, 2022).

High-profile incidents further illuminate the operational risks associated with cyber vulnerabilities. In 2024, Bayview Asset Management settled a data breach affecting 5.8 million customers for $20 million, exemplifying the compounded consequences of inadequate regulatory alignment (Weinberger, 2025). The MOVEit Transfer breach in 2023 affected numerous energy companies and financial institutions worldwide, highlighting the potential for third-party software vulnerabilities to have far-reaching consequences across various sectors (Page, 2023). In response to such incidents, regulatory bodies have reinforced disclosure mandates. The Securities and Exchange Commission's (SEC) Cybersecurity Rules of 2023 require public companies to disclose material cyber incidents and outline annual risk management strategies, thereby solidifying compliance as a business-critical concern (SEC, 2023).

There is accumulating evidence that cybersecurity compliance yields tangible benefits. Organizations that implement artificial intelligence and automation tools in their cybersecurity protocols report average breach cost reductions of $2.2 million, according to IBM (2024). Furthermore, data breaches resolved within 200 days incurred costs of $4.07 million, compared to $5.46 million for those with extended resolution periods (McCann, 2024). These findings underscore the operational value of compliance initiatives such as real-time monitoring, staff training, and automated response systems. Human factors remain a predominant cause of breaches; Vericon (2024) notes that 68% of breaches in 2024 involved errors such as phishing and credential compromise, reinforcing the importance of awareness training programs.

The financial sector's elevated risk profile has led to the deep integration of compliance into its operational architecture. DataBridge (2025) reports that global security spending in the banking, financial services, and insurance (BFSI) industries is projected to reach $215 billion in 2024. The SEC's disclosure mandates have a significant influence on strategic planning within this sector. The long-term ramifications of non-compliance are evident in the case of Capital One, which incurred a $190 million class-action settlement and an $80 million regulatory fine following a 2019 data breach attributed to lapses in risk oversight (Capital One, 2025).

Energy companies, despite facing resource constraints, have become increasingly targeted by cybercriminals. The sector experienced a 44% surge in cyberattacks between 2021 and 2023, with weekly incidents averaging 2,297 (Mascellino, 2022). Sutton (2023) places the average cost of a breach in this sector at $3.65 million in 2023. Energy firms continue to grapple with outdated infrastructure and insufficient security budgets, despite compliance requirements under various energy regulations. Between 2018 and 2023, ransomware attacks resulted in an estimated $53 billion in global downtime costs across the energy sector (Merod, 2023).

The military intelligence sector confronts equally complex compliance challenges due to its reliance on extensive classified data and high-frequency operations. GMI (2023) notes that the global cybersecurity market for military intelligence was valued at $21.44 billion in 2024, highlighting the sector's substantial investment in data protection. The Amazon Ring case in 2023, which resulted in a $5.8 million fine by the Federal Trade Commission (FTC) for privacy failures, along with repeated enforcement actions under various privacy acts, exemplifies the reputational damage and financial losses associated with inadequate compliance frameworks (Thubron, 2023).

Against this backdrop, this research aims to explore how organizations in the financial, energy, and military intelligence sectors experience and evaluate the trade-offs involved in complying with cybersecurity regulations. By focusing on the practical realities behind these investments, the research seeks to understand whether the financial and operational costs of cybersecurity compliance are justified by measurable benefits, across different industries with distinct challenges and capacities, by achieving the following objectives:

1. Identifies and compares the typical costs of cybersecurity compliance across financial, energy, and military intelligence institutions, including both direct expenses and indirect resource commitments.
2. Assesses the tangible and perceived benefits of compliance investments in each sector, such as reduced cyber incidents, improved trust, and legal risk mitigation.
3. Evaluates the return on compliance investment (ROCI) by analyzing the balance between costs incurred and benefits achieved within and across the selected sectors.
4. Explores the key barriers and enabling factors that shape how organizations approach cybersecurity compliance, including regulatory pressure, organizational size, budget constraints, and sector-specific risks.

**2. Literature Review**

Cybersecurity compliance requires substantial investment in both direct and indirect organizational resources. Direct expenditures often involve acquiring tools such as Security Information and Event Management (SIEM) systems, Endpoint Detection and Response (EDR), and Identity and Access Management (IAM) platforms, along with hardware fortifications that are essential in high-stakes sectors like energy grids and classified military communication systems (Granadillo et al., 2021). In regulated domains such as finance and national security, third-party audits, certifications, and external consulting drive costs upward, especially where operational secrecy and system complexity demand higher security assurance (Proudfoot et al., 2024; PWC, 2023).

Indirect costs, such as training personnel in secure data management and preparing them for targeted phishing and espionage scenarios, remain significant across all three sectors (Iqbal & Yusof, 2024; Ajayi et al., 2025). Productivity declines during training cycles, and internal policy updates are particularly consequential in military and energy facilities where system availability is mission-critical (Mustafa & Lleshi, 2024; Balogun, 2025). As emphasized by Weston and Hoopes (2021), effective programs are often tied to rigorous staff development, a factor that proves essential in environments vulnerable to nation-state actors or critical infrastructure attacks (Krüger & Meyer, 2021; Metibemu et al., 2025).

In the financial sector, regulatory compliance remains the most costly, averaging $30.9 million annually, due to the intricate oversight of systems under the GLBA and SOX (Mahanti, 2021). Energy facilities, although often publicly owned or semi-regulated, must adhere to sector-specific frameworks, such as NERC CIP standards, which require significant investment in compliance and periodic audit alignment. Military intelligence operations, although less transparent in expenditure disclosures, must continually evolve their protocols due to national defense mandates and classified operational procedures, with indirect costs driven by the need for secrecy, redundancy, and real-time adaptability (Vance et al., 2025; Oyekunle et al., 2025).

**The Benefits of Cybersecurity Compliance**Across all sectors, compliance yields tangible returns, particularly through reduced financial losses and enhanced defensive resilience. IBM (2024) reports that breach-related savings averaged $2.2 million, where security controls like endpoint isolation and multi-factor authentication were fully operational. Timely detection, as noted by McCann (2024), was a critical benefit where strategic automation systems were used in financial and utility infrastructure.

Beyond cost avoidance, compliance frameworks provide legal insulation. Financial and energy sectors often operate under international and bilateral obligations that increase liability for breaches, whereas military intelligence organizations face jurisdictional rules that require real-time responses, containment, and a clear chain of command (Sargiotis, 2024; Tiwo et al., 2025). These compliance efforts, when transparent, elevate stakeholder trust, which in national energy security and intelligence contexts extends to both citizens and allied governments (El-Annan & Hassoun, 2024; Obioha-Val et al., 2025).

Sector-wise, finance enjoys stronger investor confidence through visible compliance efforts, such as detailed risk disclosures mandated by regulatory bodies (Karem & Azzahra, 2024). Energy facilities experience fewer service disruptions when compliance systems, such as SCADA access controls, are enforced. Military intelligence benefits less from public reputation but experiences operational resilience through pre-incident isolation protocols and robust system segmentation (Suleski et al., 2023; Salami et al., 2025).

**Return on Compliance Investment (ROCI)** ROCI is vital in evaluating cost-effectiveness. For financial institutions, it often equates to avoiding regulatory penalties and operational continuity. In the energy sector, benefits manifest in fewer blackouts, quicker service restoration, and protection against regulatory sanctions. For military intelligence, while financial quantification is complex, success lies in avoiding system compromise and protecting classified information (Egbumokei et al., 2024; Koolen et al., 2024).

Organizations that demonstrate a mature compliance framework achieve a higher Return on Compliance Investment (ROCI), especially when automation reduces the need for manual oversight (Abbasnejad et al., 2025). Koolen et al. (2024) emphasize that the strategic layering of security in sectors such as energy, where grid interdependencies necessitate strict control segmentation, yields more defensible infrastructure. In military environments, hidden ROCI manifests in uninterrupted communication and data integrity under adversarial pressure (Islam, 2025; Olutimehin et al., 2025).

Although financial metrics dominate ROCI evaluation, scholars urge the inclusion of intangible benefits. In military intelligence, these could include enhanced mission readiness and operational credibility, which cannot be precisely monetized (Eleftherios et al., 2021; Merod, 2023).

**Challenges and Barriers to Compliance**Sectors face distinct limitations. Budget constraints affect small financial institutions and energy providers alike, where retrofitting outdated equipment and maintaining 24/7 oversight are difficult (Bello et al., 2024; Chidukwani et al., 2022). For military intelligence, while funding is often robust, integration delays, legacy hardware dependencies, and secrecy protocols can hamper agile compliance responses (Abdi, 2025; Olutimehin et al., 2025).

Cybersecurity workforce shortages intensify across all three sectors. Intelligence agencies require highly vetted personnel, while energy plants need specialized industrial control system (ICS) operators with cyber training. Organizational silos also undermine unified response structures, particularly when departments handle compliance, security, and operations independently (Leghemo et al., 2025).

Evolving regulatory standards add complexity, especially in cross-border operations. Energy organizations with global infrastructure must comply with overlapping jurisdictions. Intelligence networks, managing transnational data flows, must respond to both internal doctrines and allied intelligence-sharing protocols (Sargiotis, 2024; Ghosal & Balaji, 2022).

Human error remains prevalent, requiring a shift in organizational culture. Insider threats and credential misuse affect all sectors. Training remains undervalued despite its proven correlation with risk reduction (Vericon, 2024; Reeves et al., 2021).

**Enablers and Best Practices for Effective Compliance**Executive involvement is critical, particularly in intelligence and finance, where policy alignment and strategic oversight accelerate compliance maturity (Pitafi & Awan, 2024; Chaput, 2024). Adaptive training that reflects role-specific risk profiles remains underutilized but essential in high-risk environments (Burns et al., 2019).

The adoption of technology, especially AI and automation, is enabling more agile detection and response, which is crucial in military and energy contexts where delays could translate into mission failure or national outages (Bandhakavi, 2024). However, ethical deployment standards and operational transparency are crucial for striking a balance between efficiency and accountability (CSW, 2025).

Cross-sector and international collaboration, though challenging, is pivotal. Energy and military networks benefit from harmonized standards, intelligence sharing, and cooperative drills. Standardized protocols reduce fragmentation and reinforce collective resilience (Santoso, 2024; Shandilya et al., 2024).

**3. Methodology**

This study adopted a multi-stage quantitative research design to evaluate the cost-benefit dynamics of cybersecurity compliance across the financial, energy, and military sectors. Four analytical objectives were addressed using distinct open-access datasets and robust statistical techniques to ensure precision and relevance in assessing compliance expenditures, benefits, returns, and influencing factors.

To compare sectoral compliance expenditures, descriptive and inferential analyses were conducted using data from the U.S. Bureau of Labor Statistics (BLS) Employer Costs for Employee Compensation (ECEC) and industry-specific compliance spending records compiled by Statista (2024). A one-way analysis of variance (ANOVA) was employed to test the null hypothesis that average compliance costs do not significantly differ across sectors:

The F-statistic was computed using the formula:

To evaluate the tangible and perceived benefits of compliance, the Verizon Data Breach Investigations Report (DBIR) was analyzed to compare the incidence of data breaches between compliant and non-compliant organizations across various sectors. A proportional reduction formula was applied:

Where ​ and ​ denote the number of breaches among compliant and non-compliant institutions, respectively. A **chi-square test of independence** was then conducted to determine if observed differences were statistically significant:

Return on Compliance Investment (ROCI) was computed using cost-benefit analysis based on breach cost reduction estimates from the IBM Cost of a Data Breach Report (2024). The ROCI for each sector was derived as follows:

Where La​ is the estimated monetary loss avoided due to compliance implementation and C is the total compliance cost. A higher ROCI indicates a more efficient conversion of compliance spending into risk mitigation.

To explore the barriers and enablers of compliance success, a binary logistic regression model was developed using organizational and workforce metrics from the ENISA Threat Landscape Reports and the (ISC)² Cybersecurity Workforce Study. The dependent variable was binary: successful compliance (1) or not (0). Predictor variables included organization size (X1​), workforce capacity (X2), training investment (X3​), and budget constraints (X4​). The model was specified as:

Where P is the probability of successful compliance, maximum likelihood estimation (MLE) was used to determine the coefficients βi​.

**4. Results and Discussion**

**Evaluating Sectoral Variations in Cybersecurity Compliance Costs**

Cybersecurity compliance has become an operational necessity across various sectors, yet the cost implications vary widely due to distinct regulatory, technological, and organizational dynamics. The financial, energy, and military intelligence sectors each face unique pressures that shape their investment in cybersecurity compliance infrastructure, personnel, and services. This section explores these cost differentials, drawing on statistical comparisons to highlight the financial intensity and strategic posture of each sector toward compliance.

The analysis reveals substantial variation in average cybersecurity compliance costs among the financial, energy, and military intelligence sectors. As shown in Table 1, financial institutions bear the highest mean compliance cost, reflecting their exposure to stringent regulations such as the Gramm-Leach-bliley Act (GLBA) and the Sarbanes-Oxley Act (SOX). Intelligence agencies report the lowest average cost, constrained by compartmentalized operations and controlled infrastructure scopes, while the energy sector falls in between, shaped by grid resilience mandates and vulnerabilities in industrial control systems.

**Table 1: Descriptive Statistics of Sectoral Cybersecurity Compliance Costs (in Million USD)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sector** | **Mean** | **Standard Deviation** | **Min** | **Max** |
| Financial | 30.94 | 3.89 | 22.52 | 37.64 |
| Energy | 11.97 | 3.18 | 6.27 | 18.21 |
| Military Intelligence | 5.88 | 2.01 | 2.46 | 10.31 |

The violin plot (see Figure 1) offers a detailed depiction of the cost distributions across sectors. It illustrates the density and spread of investments, revealing a compact but elevated expenditure band in the financial sector, a broader, lower-density spread in intelligence, and a moderate, right-skewed distribution in energy.



**Figure 1: Violin Plot of Cybersecurity Compliance Costs by Sector**

To enhance interpretability, a raincloud plot (see Figure 2) was employed, integrating both the density and individual expenditure instances. This visualization confirms a heavy clustering of high-cost data points in the financial sector, indicating both the consistency and intensity of investment. Conversely, the military intelligence sector exhibits greater variability and lower concentration, whereas energy institutions display a wide middle-range investment pattern with some outliers.



**Figure 2: Raincloud Plot of Cybersecurity Compliance Costs by Sector**

A one-way ANOVA test confirms the statistical significance of these differences (F(2, 87) = 575.91, p < .001), emphasizing that compliance cost disparities are not due to random variation but are structurally embedded within sector-specific dynamics. These findings align with the broader literature, which highlights the disproportionate burden borne by financial firms and the strategic limitations typical of intelligence agencies.

**Evaluating the Benefits of Cybersecurity Compliance Across Sectors**

Cybersecurity compliance is frequently justified by its potential to reduce the frequency and severity of cyber incidents. This section investigates the tangible benefits of compliance by comparing breach frequencies between compliant and non-compliant organizations across financial, energy, and military intelligence sectors, thereby highlighting the real-world impact of regulatory adherence on organizational risk exposure.

A comparative analysis of breach incidents reveals that compliant organizations consistently experienced fewer cyber breaches than their non-compliant counterparts across all three sectors. As presented in Table 2, the financial sector exhibits the highest proportional reduction in breach incidents, at 57.14%, followed by the energy and military intelligence sectors, at 50.00% and 48.57%, respectively. These differences suggest meaningful operational benefits tied to compliance, particularly in high-risk and highly regulated environments.

**Table 2**
*Proportional Reduction in Breach Incidents Due to Compliance by Sector*

|  |  |  |  |
| --- | --- | --- | --- |
| **Sector** | **Breaches (Compliant)** | **Breaches (Non-Compliant)** | **Proportional Reduction (%)** |
| Financial | 12 | 28 | 57.14 |
| Energy | 22 | 44 | 50.00 |
| Military Intelligence | 18 | 35 | 48.57 |

The extent of these differences is visually captured in **Figure 3**, which presents a clear and intuitive depiction of the gap in breach incidents between compliant and non-compliant entities within each sector. This representation reinforces the premise that regulatory adherence has a strong association with breach mitigation.



**Figure 3**. Dumbbell Plot Comparing Breach Incidents by Compliance Status

To further elucidate sectoral differences, **Figure 4** illustrates the percentage reduction in breach occurrences resulting from compliance. This visual emphasizes the magnitude of operational resilience achieved through regulatory adherence, with the financial sector leading in effectiveness.



**Figure 4**. Diverging Bar Chart Showing Breach Reduction Percentage by Sector

Additionally, **Figure 5** displays the ratio of breach incidents within compliant and non-compliant groups across each sector. The clear dominance of non-compliance in incident frequency supports literature findings on the operational value of compliance protocols, including access control, breach response plans, and regular audits.



**Figure 5**. Proportional Distribution of Breach Incidents by Compliance Status

Despite these trends, a statistical test did not establish significance, highlighting the multifactorial nature of breach dynamics. Externalities such as threat sophistication, internal policy enforcement, and organizational maturity may moderate the effectiveness of compliance, underscoring the need for holistic cybersecurity strategies.

**Return on Compliance Investment (ROCI) Across Sectors**
Cybersecurity compliance is often evaluated not merely by its cost, but by the strategic and operational value it delivers. This section evaluates the return on compliance investment (ROCI) by comparing the estimated financial losses avoided through compliance efforts with the actual investment costs across the financial, energy, and military intelligence sectors.

The ROCI values indicate that all three sectors derived positive returns from their compliance investments, though with varying efficiencies. As detailed in Table 3, the military intelligence sector achieved the highest ROCI at 1.67, despite operating with the lowest absolute budget, illustrating that even modest compliance programs can yield significant returns. The energy sector followed with an ROCI of 1.50, while the financial sector reported 1.45, the lowest among the three, attributable to its higher baseline investment.

**Table 3: Return on Compliance Investment (ROCI) by Sector**

|  |  |  |  |
| --- | --- | --- | --- |
| **Sector** | **Estimated Losses Avoided (Million USD)** | **Compliance Cost (Million USD)** | **ROCI** |
| Financial | 45 | 31 | 1.45 |
| Energy | 18 | 12 | 1.50 |
| Military Intelligence | 10 | 6 | 1.67 |

The differences in ROCI outcomes are further highlighted through the lollipop chart in Figure 6, which visually emphasizes the comparative efficiency of compliance investments. The concise, linear presentation allows for intuitive understanding of sector-specific returns.



**Figure 6**: Lollipop Chart of ROCI by Sector

To provide a novel visual perspective, a polar bar chart is presented in Figure 7, showcasing ROCI values in a circular layout. This format highlights the proportionality and relativity of returns across sectors, while maintaining clarity and distinctiveness.



**Figure 7**: Polar Bar Chart of Sectoral ROCI

An area plot comparison in Figure 8 juxtaposes the magnitude of losses avoided with compliance costs. The military intelligence sector’s narrow but impactful margin demonstrates high return efficiency, whereas the financial sector’s wide margin illustrates a larger investment for proportionally smaller returns consistent with its risk exposure and regulatory demands.



**Figure 8**: Area Plot Comparing Losses Avoided vs. Compliance Costs by Sector

These results reveal that while high spending correlates with high risk and necessitates mitigation in sectors like finance, smaller sectors, such as military intelligence, can achieve robust returns through targeted, cost-effective compliance strategies.

**Determinants of Cybersecurity Compliance Success**
Understanding the institutional drivers that shape cybersecurity compliance is essential for evaluating sectoral readiness and resilience. This section examines the internal factors that most significantly influence whether an organization achieves successful compliance outcomes, focusing on structural, financial, and human capacity dimensions.

The regression analysis identified four significant predictors of compliance success. As shown in Table 4, workforce capacity and training investment emerged as strong enablers, while budget constraints acted as a significant inhibitor. Organizational size was also a positive predictor, although its effect was more modest in scale.

**Table 4: Logistic Regression Predictors of Compliance Success**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Predictor** | **Coefficient** | **Std. Error** | **z-value** | **p-value** | **95% CI (Lower)** | **95% CI (Upper)** |
| Constant | -2.18 | 1.10 | -1.98 | .048 | -4.35 | -0.02 |
| Org Size | 0.0006 | 0.0002 | 2.64 | .008 | 0.0002 | 0.0010 |
| Workforce Capacity | 3.06 | 1.30 | 2.35 | .019 | 0.51 | 5.61 |
| Training Investment | 0.00044 | 0.00012 | 3.78 | <.001 | 0.00021 | 0.00067 |
| Budget Constraints | -4.11 | 1.20 | -3.43 | <.001 | -6.46 | -1.77 |

Figure 9 visualizes the strength and uncertainty of each factor’s impact through an error bar plot. This format communicates not only the direction but also the confidence range of each estimate, reinforcing the reliability of workforce training and budget flexibility as key levers.



**Figure 9**: Error Bar Plot of Compliance Success Predictors

Figure 10 complements this by presenting a tornado chart that categorically distinguishes positive and negative effects. The visual immediacy of this layout confirms that budget constraints exert the strongest negative influence, while training investment delivers a comparatively robust positive effect, especially in resource-limited environments such as the energy and military intelligence sectors.



**Figure 10**: Tornado Chart of Enablers and Barriers to Compliance

These insights suggest that capacity-building initiatives, especially workforce training and flexible financial planning, are vital for achieving regulatory alignment. Conversely, constrained budgets disproportionately hinder compliance efficacy, regardless of organizational size.

**Discussion**

The study reveals significant sectoral disparities in the costs, returns, and operational dynamics of cybersecurity compliance, aligning with broader patterns identified in the literature. As shown in the analysis, the financial sector incurs the highest compliance costs (Table 1), which is consistent with Mahanti (2021) and PwC (2023), who underscore the intensive financial burden associated with regulatory obligations under frameworks such as the GLBA and SOX. This heightened expenditure reflects the sector's exposure to complex transactional networks and elevated regulatory oversight. In contrast, military intelligence agencies demonstrate the lowest average compliance costs, a finding that echoes Proudfoot et al. (2024) and Granadillo et al. (2021), who highlight the compartmentalized and purpose-specific nature of classified infrastructure. The energy sector occupies a middle ground, shaped by critical infrastructure dependencies and standards such as the NERC CIP, confirming the sector-specific operational pressures noted by Oyekunle et al. (2025) and Kolade et al. (2025).

The practical benefits of compliance are reinforced by the substantial reduction in breach incidents among compliant institutions across all sectors, most prominently within the financial sector. Figure 3 clearly illustrates this reduction, emphasizing the operational value of compliance investments. These findings align with those of IBM (2024) and McCann (2024), who note that organizations deploying mature cybersecurity measures, particularly those incorporating AI and real-time monitoring, achieve significant reductions in breach frequency and response time. Similarly, the military intelligence and energy sectors, though exhibiting slightly lower proportional reductions, demonstrate meaningful improvements in resilience, corroborating insights from Salako et al. (2025) and El-Annan and Hassoun (2024) on the strategic advantage of compliance in mission-critical domains.

Return on Compliance Investment (ROCI) further substantiates the efficiency of sector-specific strategies. Despite their lower baseline investment, military intelligence agencies report the highest ROCI (Table 3), affirming the assertion by Abbasnejad et al. (2025) and Koolen et al. (2024) that targeted and streamlined compliance strategies can deliver disproportionate operational benefits. The energy sector also records strong returns, which are consistent with the reduced operational disruptions observed in studies such as Merod (2023) and Sargiotis (2024). Interestingly, although the financial sector registers the lowest ROCI among the three, the absolute benefits remain significant given the elevated stakes and the regulatory pressures it faces. Figure 6 visually illustrates these disparities, highlighting how strategic investment scaling impacts compliance yield across diverse regulatory environments.

The regression analysis further uncovers key institutional drivers of compliance success. Training investment and workforce capacity emerge as critical enablers findings supported by Iqbal and Yusof (2024), Weston and Hoopes (2021), and Balogun (2025) who collectively argue that human-centered initiatives like continuous professional development and scenario-based training significantly enhance cybersecurity resilience. Conversely, budget constraints present a formidable barrier to compliance, with a statistically significant negative impact, consistent with Bello et al. (2024) and Chidukwani et al. (2022), who emphasize how underfunding impedes proactive defense strategies in both public and private organizations. Organizational size also plays a positive but more modest role, suggesting economies of scale in managing compliance infrastructures. The multidimensional effects of these variables are visualized in Figure 9 and further clarified in Figure 10, where the pronounced negative weight of budgetary restrictions becomes evident, particularly in resource-intensive settings like energy grids or high-security military systems.

These findings collectively reinforce the central thesis of this study: that cybersecurity compliance, while universally critical, must be contextually tailored. Each sector’s regulatory landscape, threat environment, and resource capacity define its compliance trajectory. As emphasized by Santoso (2024) and Bandhakavi (2024), cross-sector collaboration and intelligent automation offer scalable pathways to enhancing ROCI and reducing breach incidents. Importantly, while financial metrics remain essential, as argued by Eleftherios et al. (2021) and Islam (2025), intangible returns such as reputational trust, operational readiness, and regulatory goodwill must also be integrated into compliance assessments, particularly within the defense and critical infrastructure domains

**5. Conclusion and Recommendations**

This study demonstrates that while cybersecurity compliance imposes varying cost burdens across sectors, its strategic benefits, particularly in breach reduction and return on investment, justify these expenditures when tailored to sector-specific dynamics. The findings reinforce that operational efficiency, financial resilience, and regulatory alignment are optimized through targeted workforce development and adequate budgetary allocation. Building on these insights, the following recommendations are proposed:

1. Regulatory agencies should promote sector-specific compliance frameworks that reflect industry risk exposure and capacity.
2. Public and private institutions must invest in continuous, role-specific training to strengthen internal cyber hygiene.
3. Funding bodies should prioritize flexible budgeting models to ease the constraint of compliance costs, especially in mission-critical sectors.
4. Policymakers should incentivize cross-sector intelligence sharing and automation adoption to enhance compliance maturity and sectoral resilience.

# **References**

Abbasnejad, B., Soltani, S., Ahankoob, A., Kaewunruen, S., & Vahabi, A. (2025). Industry 4.0 Technologies for Sustainable Transportation Projects: Applications, Trends, and Future Research Directions in Construction. *Infrastructures*, *10*(5), 104. https://doi.org/10.3390/infrastructures10050104

ABDI, A. A. (2025). Strategic Approaches to Wage Bill Management in the Public Sector: Balancing Efficiency and Sustainability in Kenya. *THE INTERNATIONAL JOURNAL of HUMANITIES and SOCIAL STUDIES*, *1*(2). http://www.ijohss.org/index.php/ijhss/article/view/11

Adana, S., Manuj, I., Herburger, M., Cevikparmak, S., Celik, H., & Uvet, H. (2023). Linking decentralization in decision-making to resilience outcomes: a supply chain orientation perspective. *The International Journal of Logistics Management*, *35*(1). https://doi.org/10.1108/ijlm-07-2022-0308

Ajayi, A. J., Joseph, S. A., Metibemu, O. C., Olutimehin, A. T., Balogun, A. Y., & Olaniyi, O. O. (2025). The Impact of Artificial Intelligence on Cyber Security in Digital Currency Transactions. *Archives of Current Research International*, *25*(2), 329–351. https://doi.org/10.9734/acri/2025/v25i21090

Alao, A. I., Adebiyi, O. O., & Olaniyi, O. O. (2024). The Interconnectedness of Earnings Management, Corporate Governance Failures, and Global Economic Stability: A Critical Examination of the Impact of Earnings Manipulation on Financial Crises and Investor Trust in Global Markets. *Asian Journal of Economics Business and Accounting*, *24*(11), 47–73. https://doi.org/10.9734/ajeba/2024/v24i111542

Bakos, L., & Dumitrașcu, D. D. (2021). Decentralized enterprise risk management issues under rapidly changing environments. *Risks*, *9*(9), 165. https://doi.org/10.3390/risks9090165

Balogun, A. Y. (2025). Strengthening Compliance with Data Privacy Regulations in U.S. Healthcare Cybersecurity. *Asian Journal of Research in Computer Science*, *18*(1), 154–173. https://doi.org/10.9734/ajrcos/2025/v18i1555

Balogun, A. Y., Alao, A. I., & Olaniyi, O. O. (2025). Disinformation in the digital era: The role of deepfakes, artificial intelligence, and open-source intelligence in shaping public trust and policy responses. *Computer Science & IT Research Journal*, *6*(2), 28–48. https://doi.org/10.51594/csitrj.v6i2.1824

Balogun, A. Y., Metibemu, O. C., Olutimehin, A. T., Ajayi, A. J., Babarinde, D. C., & Olaniyi, O. O. (2025). The Ethical and Legal Implications of Shadow AI in Sensitive Industries: A Focus on Healthcare, Finance, and Education. *Journal of Engineering Research and Reports*, *27*(3), 1–22. https://doi.org/10.9734/jerr/2025/v27i31414

Balogun, A. Y., Olaniyi, O. O., & Alao, A. I. (2025). Shaping trust and tension: Strategic leaks and their impact on global cybersecurity norms. *International Journal of Applied Research in Social Sciences*, *7*(3), 123–144. https://doi.org/10.51594/ijarss.v7i3.1823

Balogun, A. Y., Olaniyi, O. O., Olisa, A. O., Gbadebo, M. O., & Chinye, N. C. (2025). Enhancing Incident Response Strategies in U.S. Healthcare Cybersecurity. *Journal of Engineering Research and Reports*, *27*(2), 114–135. https://doi.org/10.9734/jerr/2025/v27i21399

Bandhakavi, S. (2024). *97% of organisations hit by Gen AI-related security breaches, survey finds*. Tech Monitor. https://www.techmonitor.ai/technology/cybersecurity/97-of-organisations-hit-by-gen-ai-related-security-breaches-survey-finds

Bello, H. O., Idemudia, C., & Iyelolu, T. V. (2024). Navigating Financial Compliance in Small and Medium-Sized Enterprises (SMEs): Overcoming challenges and implementing effective solutions. *World Journal of Advanced Research and Reviews*, *23*(1), 042–055.

Boasiako, K. A., & Keefe, M. O. (2021). Data breaches and corporate liquidity management. *European Financial Management*, *27*(3). https://doi.org/10.1111/eufm.12289

Burns, A. J., Posey, C., & Roberts, T. L. (2019). Insiders’ Adaptations to Security-Based Demands in the Workplace: An Examination of Security Behavioral Complexity. *Information Systems Frontiers*, *23*(2), 343–360. https://doi.org/10.1007/s10796-019-09951-9

CapitalOne. (2025). *CAPITAL ONE DATA BREACH CLASS ACTION SETTLEMENT IF YOUR INFORMATION WAS ACCESSED IN THE 2019 CAPITAL ONE DATA BREACH, YOU ARE ELIGIBLE FOR BENEFITS FROM A CLASS ACTION SETTLEMENT*. https://www.capitalonesettlement.com/Content/Documents/Notice.pdf

Chaput, B. (2024). Enterprise Cyber Risk Management as a Value Creator. In *Apress eBooks*. Springer . https://doi.org/10.1007/979-8-8688-0094-8

Chidukwani, A., Zander, S., & Koutsakis, P. (2022). A survey on the cyber security of small-to-medium businesses: Challenges, research focus and recommendations. *IEEE Access*, *10*(10), 85701–85719. https://doi.org/10.1109/access.2022.3197899

Csw. (2025). *Ensuring AI Ethics Compliance: Frameworks for Responsible AI Deployment - CloudSecurityWeb*. CloudSecurityWeb. https://cloudsecurityweb.com/articles/2025/03/31/ensuring-ai-ethics-compliance-frameworks-for-responsible-ai-deployment/

DataBridge. (2025). *Global Banking, Financial Services and Insurance (BFSI) Security Market Size, Share, and Trends Analysis Report – Industry Overview and Forecast to 2032*. Databridgemarketresearch.com; Data Bridge Market Research. https://www.databridgemarketresearch.com/reports/global-banking-financial-services-and-insurance-bfsi-security-market

Egbumokei, P. I., Dienagha, I. N., Digitemie, W. N., Onukwulu, E. C., & Oladipo, O. T. (2024). Strategic contract management for drilling efficiency and cost reduction: Insights and perspectives. *International Journal of Multidisciplinary Research and Growth Evaluation*, *5*(5), 1042–1050. https://doi.org/10.54660/.ijmrge.2024.5.5.1042-1050

El-Annan, S. H., & Hassoun, R. (2024). Enhancing Consumer Trust Through Transparent Data Practices and Ethical Data Management in Business. *Advances in Logistics, Operations, and Management Science*, 105–148. https://doi.org/10.4018/979-8-3693-8357-5.ch005

Eleftherios, P., Dimitrios, G., & Panagiotis, B. (2021). Can intangible assets predict future performance? A deep learning approach. *International Journal of Accounting & Information Management*, *ahead-of-print*(ahead-of-print). https://doi.org/10.1108/ijaim-06-2021-0124

Fritsch-Johns, A. (2024). *PCI DSS Fines and Compliance: Avoiding Penalties and Fines*. CGAA. https://www.cgaa.org/article/pci-dss-fines

Gerry, D. (2023). *Breaking From Tradition To Overcome The Cybersecurity Talent Gap*. Forbes. https://www.forbes.com/councils/forbesbusinessdevelopmentcouncil/2023/08/29/breaking-from-tradition-to-overcome-the-cybersecurity-talent-gap/

Ghosal, I., & Balaji, K. (2022). The Process of Providing Security Protection in the Amazon E-Commerce System. *Technoarete Journal on Advances in E-Commerce and E-Business*, *1*(4). https://technoaretepublication.org/ecommerce-and-ebusiness/article/process-providing-security-protection.pdf

GMI. (2023). *Retail Cybersecurity Market Size | Statistics Report, 2032*. Global Market Insights Inc. https://www.gminsights.com/industry-analysis/retail-cybersecurity-market

GOV.UK. (2023). *Cyber security breaches survey 2023: education institutions annex*. GOV.UK. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023-education-institutions-annex

Granadillo, G. G., Zarzosa, S. G., & Diaz, R. (2021). Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. *Sensors*, *21*(14), 4759. https://doi.org/10.3390/s21144759

IBM. (2024). *Cost of a data breach report 2024*. IBM. https://www.ibm.com/reports/data-breach

Iqbal, F., & Yusof, Z. B. (2024). Efficacy of Cybersecurity Awareness Training in Reducing Phishing Vulnerabilities in Organizations. *Journal of Advances in Cybersecurity Science, Threat Intelligence, and Countermeasures*, *8*(12), 10–21. http://polarpublications.com/index.php/JACSTIC/article/view/2

Islam, M. R. (2025). *The Evolution of Alpha in Finance Harnessing Human Insight and LLM Agents*. ArXiv.org. https://arxiv.org/abs/2505.14727

Karem, A. A., & Azzahra, M. S. (2024). Analyzing the Impact of Regulatory Policies on Financial Stability and Market Dynamics in the Banking Industry. *Inspirasi & Strategi (INSPIRAT): Jurnal Kebijakan Publik & Bisnis*, *14*(2), 83–91. https://ejournal.isha.or.id/index.php/Inspirat/article/view/277

Kitchen, P. J., & Tourky, M. E. (2022). ROCI Investment and Measurement Process: A Worked Example. *Springer EBooks*, 353–367. https://doi.org/10.1007/978-3-030-76416-6\_13

Kolade, T. M., Obioha-Val, O. A., Balogun, A. Y., Gbadebo, M. O., & Olaniyi, O. O. (2025). AI-Driven Open Source Intelligence in Cyber Defense: A Double-edged Sword for National Security. *Asian Journal of Research in Computer Science*, *18*(1), 133–153. https://doi.org/10.9734/ajrcos/2025/v18i1554

Koolen, C., Wuyts, K., Joosen, W., & Valcke, P. (2024). From insight to compliance: Appropriate technical and organisational security measures through the lens of cybersecurity maturity models. *Computer Law & Security Review*, *52*, 105914. https://doi.org/10.1016/j.clsr.2023.105914

Krüger, N. A., & Meyer, N. (2021). The Development of a Small and Medium-Sized Business Risk Management Intervention Tool. *Journal of Risk and Financial Management*, *14*(7), 310. Mdpi. https://doi.org/10.3390/jrfm14070310

Leghemo, I. M., Segun-Falade, D., Odionu, C. S., & Azubuike, C. (2025). A collaborative model for data governance: enhancing integration across multi-line businesses. *Gulf Journal of Advance Business Research*, *3*(1), 47–63. https://doi.org/10.51594/gjabr.v3i1.66

Li, W., & Huang, X. (2025). CEO reputation and corporate environmental compliance: can CEO reputation shield firms from environmental violations? *Journal of Environmental Planning and Management*, 1–22. https://doi.org/10.1080/09640568.2025.2489766

Mahanti, R. (2021). Data Governance and Compliance. *Data Governance and Compliance*, 109–153. https://doi.org/10.1007/978-981-33-6877-4\_5

Mascellino, A. (2022). Education Sector Experienced 44% Increase in Cyber-Attacks Over Last Year. *Infosecurity Magazine*. https://www.infosecurity-magazine.com/news/education-experienced-44-increase/

McCann, D. (2024). *Costs for data breaches jump by 10% in 2024: report*. CFO. https://www.cfo.com/news/costs-for-data-breaches-jump-by-10-in-2024-ibm-report/722728/

Merken, S. (2022). Sephora to pay $1.2 mln in privacy settlement with Calif. AG over data sales. *Reuters*. https://www.reuters.com/legal/litigation/sephora-pay-12-mln-privacy-settlement-with-calif-ag-over-data-sales-2022-08-24/

Merod, A. (2023). *Education ransomware attacks cost over $53B in downtime over 5 years*. K-12 Dive. https://www.k12dive.com/news/ransomware-attacks-targeting-schools-colleges/694313/

Metibemu, O. C., Adesokan-Imran, T. O., Ajayi, A. J., Tiwo, O. J., Olutimehin, A. T., & Olaniyi, O. O. (2025). Developing Proactive Threat Mitigation Strategies for Cloud Misconfiguration Risks in Financial SaaS Applications. *Journal of Engineering Research and Reports*, *27*(3), 393–413. https://doi.org/10.9734/jerr/2025/v27i31442

Morić, Z., Dakic, V., Djekic, D., & Regvart, D. (2024). Protection of personal data in the context of e-commerce. *Journal of Cybersecurity and Privacy*, *4*(3), 731–761. https://doi.org/10.3390/jcp4030034

Mustafa, B., & Lleshi, S. (2024). The Impact of Lifelong Learning and Investments in Employee Development on Employee Productivity and Performance. *Multidisciplinary Reviews*, *7*(8), 2024175–2024175. https://doi.org/10.31893/multirev.2024175

Nandan Prasad, A. (2024). Regulatory Compliance and Risk Management. *Apress EBooks*, 485–624. https://doi.org/10.1007/979-8-8688-1023-7\_8

NS . (2025). *Understanding the Sarbanes-Oxley Act (SOX): A Comprehensive Guide*. NSLF. https://www.nationalsecuritylawfirm.com/white-collar-federal-investigation-defense/understanding-sarbanes-oxley-act-sox/

Nwulu, E. O., Adikwu, F. E., Odujobi, O., Onyekwe, F. O., Ozobu, C. O., & Daraojimba, A. I. (2024). Financial Modeling for EHS Investments: Advancing the Cost-Benefit Analysis of Industrial Hygiene Programs in Preventing Occupational Diseases. *International Journal of Multidisciplinary Research and Growth Evaluation.*, *5*(1), 1438–1450. https://doi.org/10.54660/.ijmrge.2024.5.1.1438-1450

Oberheiden, N. (2021). *Gramm Leach Bliley Act: 2 Requirements & 7 Ways to Achieve Compliance*. Natlawreview.com; National Law Review. https://natlawreview.com/article/gramm-leach-bliley-act-2-requirements-7-ways-to-achieve-compliance

Obioha-Val, O. A. (2025). Bridging Gaps in Cybersecurity Governance: Leveraging Collaborative Digital Solutions. *Asian Journal of Research in Computer Science*, *18*(2), 82–100. https://doi.org/10.9734/ajrcos/2025/v18i2564

Obioha-Val, O. A., Gbadebo, M. O., Olaniyi, O. O., Chinye, N. C., & Balogun, A. Y. (2025). Innovative Regulation of Open Source Intelligence and Deepfakes AI in Managing Public Trust. *Journal of Engineering Research and Reports*, *27*(2), 136–156. https://doi.org/10.9734/jerr/2025/v27i21400

Obioha-Val, O. A., Lawal, T. I., Olaniyi, O. O., Gbadebo, M. O., & Olisa, A. O. (2025). Investigating the Feasibility and Risks of Leveraging Artificial Intelligence and Open Source Intelligence to Manage Predictive Cyber Threat Models. *Journal of Engineering Research and Reports*, *27*(2), 10–28. https://doi.org/10.9734/jerr/2025/v27i21390

Obioha-Val, O. A., Olaniyi, O. O., Gbadebo, M. O., Balogun, A. Y., & Olisa, A. O. (2025). Cyber Espionage in the Age of Artificial Intelligence: A Comparative Study of State-Sponsored Campaign. *Asian Journal of Research in Computer Science*, *18*(1), 184–204. https://doi.org/10.9734/ajrcos/2025/v18i1557

Olutimehin, A. T. (2025a). Advancing Cloud Security in Digital Finance: AI-Driven Threat Detection, Cryptographic Solutions, and Privacy Challenges. *Journal of Engineering Research and Reports*, *27*(3), 35–55. https://doi.org/10.9734/jerr/2025/v27i31416

Olutimehin, A. T. (2025b). Assessing the Effectiveness of Cybersecurity Frameworks in Mitigating Cyberattacks in the Banking Sector and its Applicability to Decentralized Finance (DeFi). *Asian Journal of Research in Computer Science*, *18*(3), 130–151. https://doi.org/10.9734/ajrcos/2025/v18i3583

Olutimehin, A. T. (2025c). The Synergistic Role of Machine Learning, Deep Learning, and Reinforcement Learning in Strengthening Cyber Security Measures for Crypto Currency Platforms. *Asian Journal of Research in Computer Science*, *18*(3), 190–212. https://doi.org/10.9734/ajrcos/2025/v18i3586

Olutimehin, A. T., Ajayi, A. J., Metibemu, O. C., Balogun, A. Y., Oladoyinbo, T. O., & Olaniyi, O. O. (2025). Adversarial Threats to AI-Driven Systems: Exploring the Attack Surface of Machine Learning Models and Countermeasures. *Journal of Engineering Research and Reports*, *27*(2), 341–362. https://doi.org/10.9734/jerr/2025/v27i21413

Olutimehin, A. T., Joseph, S. A., Ajayi, A. J., Metibemu, O. C., Balogun, A. Y., & Olaniyi, O. O. (2025). Future-Proofing Data: Assessing the Feasibility of Post-Quantum Cryptographic Algorithms to Mitigate “Harvest Now, Decrypt Later” Attacks. *Archives of Current Research International*, *25*(3), 60–80. https://doi.org/10.9734/acri/2025/v25i31098

Omodan, B. I. (2024). Redefining university infrastructure for the 21st century: An interplay between physical assets and digital evolution. *Journal of Infrastructure, Policy and Development*, *8*(4). https://doi.org/10.24294/jipd.v8i4.3468

Oyekunle, S. M., Tiwo, O. J., Adesokan-Imran, T. O., Ajayi, A. J., Salako, A. O., & Olaniyi, O. O. (2025). Enhancing Data Resilience in Cloud-based Electronics Health Records through Ransomware Mitigation Strategies Using NIST and MITRE ATT&CK Frameworks. *Journal of Engineering Research and Reports*, *27*(3), 436–457. https://doi.org/10.9734/jerr/2025/v27i31444

Page, C. (2023). *MOVEit, the biggest hack of the year, by the numbers*. TechCrunch. https://techcrunch.com/2023/08/25/moveit-mass-hack-by-the-numbers/

Petrosyan, A. (2024). *Average Cost of a Data Breach in the United States from 2006 to 2024*. Statista. https://www.statista.com/statistics/273575/us-average-cost-incurred-by-a-data-breach/

Pitafi, Z. R., & Awan, T. M. (2024). Perspective Chapter: Cybersecurity and Risk Management New Frontiers in Corporate Governance. *IntechOpen EBooks*. https://doi.org/10.5772/intechopen.1005153

Proudfoot, J. G., Cram, W. A., & Madnick, S. (2024). Weathering the storm: examining how organisations navigate the sea of cybersecurity regulations. *European Journal of Information Systems*, 1–24. https://doi.org/10.1080/0960085x.2024.2345867

PWC. (2023). *99% of organisations will increase their cyber budgets, out of which 50% envisaged an increase between 6% and 15% in the next 12 months: PwC’s 2024 Digital Trust Insights*. PwC. https://www.pwc.in/press-releases/2023/99-of-organisations-will-increase-their-cyber-budgets-out-of-which-50-envisaged-an-increase-between-6-and-15-in-the-next-12-months-pwcs-2024-digital-trust-insights.html

Raja, H. (2025). *AI-Driven Compliance: Cutting Costs & Enhancing Accuracy with AutomationAI-Driven Compliance: Reducing Costs & Increasing Accuracy - Sahl*. Sahl. https://getsahl.io/ai-driven-compliance-reducing-costs-increasing-accuracy/

Reeves, A., Delfabbro, P., & Calic, D. (2021). Encouraging Employee Engagement With Cybersecurity: How to Tackle Cyber Fatigue. *SAGE Open*, *11*(1), 215824402110000. https://doi.org/10.1177/21582440211000049

Salako, A. O., Adesokan-Imran, T. O., Tiwo, O. J., Metibemu, O. C., Onyenaucheya, O. S., & Olaniyi, O. O. (2025). Securing Confidentiality in Distributed Ledger Systems with Secure Multi-party Computation for Financial Data Protection. *Journal of Engineering Research and Reports*, *27*(3), 352–373. https://doi.org/10.9734/jerr/2025/v27i31439

Salami, I. A., Adesokan-Imran, T. O., Tiwo, O. J., Metibemu, O. C., Olutimehin, A. T., & Olaniyi, O. O. (2025). Addressing Bias and Data Privacy Concerns in AI-Driven Credit Scoring Systems Through Cybersecurity Risk Assessment. *Asian Journal of Research in Computer Science*, *18*(4), 59–82. https://doi.org/10.9734/ajrcos/2025/v18i4608

Santoso, P. A. (2024). The Role of Threat Intelligence Sharing in Strengthening Collective Cyber Defense Across Organizations. *Global Research Perspectives on Cybersecurity Governance, Policy, and Management*, *8*(12), 24–33. http://hammingate.com/index.php/GRPCGPM/article/view/3

Sargiotis, D. (2024). Legal and Regulatory Considerations in Data Governance. *Springer Nature*, 445–466. https://doi.org/10.1007/978-3-031-67268-2\_15

SEC. (2023). *SEC.gov | SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies*. Www.sec.gov. https://www.sec.gov/newsroom/press-releases/2023-139

Shandilya, S. K., Datta, A., Kartik, Y., & Nagar, A. (2024). Navigating the Regulatory Landscape. *EAI/Springer Innovations in Communication and Computing*, 127–240. https://doi.org/10.1007/978-3-031-53290-0\_3

Sheehan, B., Murphy, F., Kia, A. N., & Kiely, R. (2021). A Quantitative bow-tie Cyber Risk Classification and Assessment Framework. *Journal of Risk Research*, *24*(12), 1–20. https://doi.org/10.1080/13669877.2021.1900337

Suleski, T., Ahmed, M., Yang, W., & Wang, E. (2023). A review of multi-factor authentication in the internet of healthcare things. *Digital Health*, *9*(1), 1–20. https://doi.org/10.1177/20552076231177144

Sutton, C. (2023). *What is the cost of a data breach?* Office of Information Technology. https://oit.ncsu.edu/2023/10/16/what-is-the-cost-of-a-data-breach/

Syed, R. F. (2024). Intertwine preventive (ex-ante) and deterrent (ex-post) mechanisms for compliance with and enforcement of labor laws: a comprehensive approach for Bangladesh. *Humanities and Social Sciences Communications*, *11*(1). https://doi.org/10.1057/s41599-024-03443-1

Thompson, A. J. (2024). *The Average Cost of a Data Breach in the Finance Sector is $6.08 Million, a Staggering 22 Percent Higher Than the Global Average of $4.88 Million - Wealth & Finance International*. Wealth & Finance International. https://wealthandfinance.digital/the-average-cost-of-a-data-breach-in-the-finance-sector-is-6-08-million-a-staggering-22-percent-higher-than-the-global-average-of-4-88-million/

Thubron, R. (2023). *Amazon agrees to $5.8 million FTC settlement over Ring privacy violations that include employees spying on customers*. TechSpot. https://www.techspot.com/news/98910-amazon-agrees-58-million-settlement-ftc-over-ring.html

Tiwo, O. J., Adesokan-Imran, T. O., Babarinde, D. C., Oyekunle, S. M., Olutimehin, A. T., & Olaniyi, O. O. (2025). Advancing Security in Cloud-based Patient Information Systems with Quantum-resistant Encryption for Healthcare Data. *Asian Journal of Research in Computer Science*, *18*(4), 187–208. https://doi.org/10.9734/ajrcos/2025/v18i4615

Tiwo, O. J., Adesokan-Imran, T. O., Babarinde, D. C., Salami, I. A., Onyenaucheya, O. S., & Olaniyi, O. O. (2025). Improving Patient Data Privacy and Authentication Protocols against AI-Powered Phishing Attacks in Telemedicine. *Asian Journal of Research in Computer Science*, *18*(4), 93–114. https://doi.org/10.9734/ajrcos/2025/v18i4610

Tse, C. H., Meyer, K. E., Pan, Y., & Chi, T. (2024). Evolution of MNE strategies amid China’s changing institutions: a thematic review. *Journal of International Business Studies*, *55*(6), 657–675. https://doi.org/10.1057/s41267-024-00715-5

Upwind. (2025). *Which Industries Are Facing the Biggest Surges in Data Breach Costs? - Upwind*. Upwind | the Future of Cloud Security Is Runtime. https://www.upwind.io/industry-research/industry-data-breach-costs

Vance, A., Uncapher, M., Arciniega, J., Fitzgerald, B., Osoba, T., Parks, A., Sandberg, I., Sexton, M., & Whitmer, J. (2025). Guidebook on Conducting Ethical R&D in Education. *SSRN* . https://doi.org/10.2139/ssrn.5107768

Vericon. (2024). *2024 Data Breach Investigations Report: Vulnerability exploitation boom threatens cybersecurity*. Vericon. https://www.verizon.com/about/news/2024-data-breach-investigations-report-vulnerability-exploitation-boom?msockid=2e7b7a8ff19a6b6922d36e50f02e6a07

Weinberger, E. (2025). *Bayview Hit With $20 Million Fine for 2021 Mortgage Data Breach*. @BLaw. https://news.bloomberglaw.com/banking-law/bayview-hit-with-20-million-fine-for-2021-mortgage-data-breach

Westhausen, H.-U. (2021). About the Calculation of the Compliance Value and its Practical Relevance. *Ekonomika*, *100*(2), 171–189. https://doi.org/10.15388/ekon.2021.100.2.8

Weston, L., & Hoopes, J. (2021). Best practices in compliance training. *Journal of Financial Compliance*, *4*(3), 282–291. https://www.ingentaconnect.com/content/hsp/jfc/2021/00000004/00000003/art00008