ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26feb1298

Securing the Digital State: An Analysis of Cybersecurity Governance, Institutional Capacity, and Policy Challenges for Information Security in Sierra Leone's Public Sector

Charles Alusine Bangura[1*]; Emmanuel Oladipo[2]; Michael Nicol Samai[3]; Mamoud Miracle Sesay[4]

[1,2,3,4]University of Makeni, Department of Computer Science, Freetown, Sierra Leone, The Evangelical College of Theology, Jui, Freetown, Sierra Leone, Nankai University, College of Software Engineering, Tianjin, China

Corresponding Author: Charles Alusine Bangura[1*]

Publication Date: 2026/03/07

Abstract: This comprehensive study examines cybersecurity governance challenges in Sierra Leone's public sector through empirical analysis and formal hypothesis testing. We investigate institutional capacity, policy frameworks, and implementation barriers affecting government information security. Our findings reveal significant governance gaps, estimated annual economic losses of USD 2.3–4.8 million, and critical infrastructure vulnerabilities. Using multiple regression analysis ($R^2 = 0.687$, $p < 0.001$) and chi-square contingency analysis ($\chi^2 = 6.728$, $p = 0.009$), we confirm that institutional capacity factors and formal security policies significantly predict governance effectiveness and lower incident rates, respectively. Economic impact modeling projects cumulative losses of USD 2.76 million (status quo) through 2027, which would be reduced to USD 797,000 through comprehensive institutional reform. This research provides evidence-based policy recommendations and a strategic implementation roadmap to strengthen digital resilience in Sub-Saharan African public sectors. The study is particularly relevant for developing nations implementing digital transformation initiatives in resource-constrained environments.

Keywords: *Cybersecurity Governance, Institutional Capacity, Public Sector Security, Policy Analysis, Developing Nations, Information Security, Digital Resilience, Sub-Saharan Africa.*

How to Cite: Charles Alusine Bangura; Emmanuel Oladipo; Michael Nicol Samai; Mamoud Miracle Sesay (2026) Securing the Digital State: An Analysis of Cybersecurity Governance, Institutional Capacity, and Policy Challenges for Information Security in Sierra Leone's Public Sector. *International Journal of Innovative Science and Research Technology*, 11(2), 2826-2833. https://doi.org/10.38124/ijisrt/26feb1298

I. INTRODUCTION

The acceleration of digital transformation in developing nations presents concurrent opportunities and unprecedented security challenges. Sierra Leone, a West African nation (population 8.6 million), has embarked on an ambitious digital governance initiative to modernize public services. However, this digitalization trajectory lacks proportional investment in cybersecurity infrastructure, institutional frameworks, and regulatory governance mechanisms.

The absence of comprehensive cybersecurity governance exposes critical national infrastructure, healthcare systems, financial services, power distribution networks, and water management systems to escalating threats. Recent incidents, including unauthorized access to government portals and breaches of citizen data, underscore the urgent need for a systematic investigation into institutional capacity and policy frameworks.

➢ *Research Motivation*

This research addresses a critical gap in scholarly literature examining cybersecurity governance in Sub-Saharan African contexts, particularly in low-resource environments. While extensive literature examines the security postures of developed nations, empirical analysis of institutional capacity, governance structures, and policy implementation barriers in West African contexts remains sparse.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26feb1298

➢ *Research Questions*

This study addresses five primary research questions:

- What institutional structures currently govern cybersecurity operations in Sierra Leone's public sector?
- How do existing institutional capacities align with international cybersecurity standards?
- What policy gaps and implementation barriers impede effective information security?
- What quantifiable economic impacts result from cybersecurity incidents and vulnerabilities?
- What evidence-based reforms would enhance institutional capacity and governance effectiveness?

II. LITERATURE REVIEW AND THEORETICAL FRAMEWORK

➢ *Cybersecurity Governance*

Cybersecurity governance encompasses structures, processes, and mechanisms through which organizations establish strategic direction, ensure accountability, manage information security risks, and implement protective measures [1]. Contemporary frameworks integrate normative dimensions (standards compliance) with adaptive dimensions (threat response capability).

- *Governance Effectiveness Depends Upon:*

✓ Structural Integration: Formal embedding of security functions within organizational hierarchies;
✓ Resource Allocation: Adequate budgetary commitment and personnel expertise;
✓ Regulatory Alignment: Compliance with legislative mandates;
✓ Stakeholder Coordination: Multi-level collaboration between agencies.

➢ *Institutional Capacity*

Institutional capacity refers to an organization's ability to formulate and implement policies, execute functions, and adapt to environmental changes [2]. In developing nations, capacity constraints manifest across multiple dimensions:

- Human Resource Deficits: Limited specialized cybersecurity expertise
- Technological Gaps: Insufficient modern security infrastructure
- Financial Constraints: Competing budgetary priorities
- Knowledge Deficiency: Limited domestic research capacity

➢ *Policy Frameworks*

Effective cybersecurity governance requires comprehensive legislative frameworks that establish minimum security standards, require incident reporting, and establish accountability mechanisms. The World Economic Forum identifies regulatory maturity as a critical differentiator in national cybersecurity [3].

III. RESEARCH METHODOLOGY

➢ *Research Design*

This mixed-methods study employs quantitative and qualitative data collection across three phases:

- *Phase I:*

Institutional Assessment (Quantitative). Structured questionnaires were administered to cybersecurity personnel (n=87) across 23 government ministries and departments, using 5-point Likert scales to evaluate governance structures, resource availability, incident response capabilities, regulatory compliance, and security training programs.

- *Phase II:*

Policy Analysis (Qualitative). A documentary analysis examined 34 legislative instruments and policy documents, using thematic content analysis to identify policy gaps and implementation barriers.

- *Phase III:*

Economic Impact Modeling (Quantitative). Historical incident data spanning 2018–2025 (n=156 documented incidents) provided the basis for econometric modeling and loss projections.

➢ *Hypothesis Testing Framework*

- *Hypothesis 1 (H1):*

Institutional capacity factors (human resources, budget allocation, technological infrastructure) are statistically significant predictors of cybersecurity governance effectiveness scores ($p < 0.05$).

- *Hypothesis 2 (H2):*

Organizations implementing formal security policies demonstrate statistically significantly lower incident rates compared to those without formalized policies ($p < 0.05$).

$$\text{Governance Effectiveness} = \beta_0 + \beta_1(\text{HR}) + \beta_2(\text{Budget}) + \beta_3(\text{Tech}) + \varepsilon \quad (1)$$

$$\chi^2 = \Sigma\,(O\_ij - E\_ij)^2 / E\_ij \quad (2)$$

➢ *Sample Characteristics*

The research encompassed 87 cybersecurity professionals across 23 government agencies; 156 documented cybersecurity incidents (2018–2025); 34 policy and legislative instruments; and geographic coverage across four provinces plus the Western Area.

IV. INSTITUTIONAL ASSESSMENT RESULTS

➢ *Governance Maturity*

Analysis reveals substantial heterogeneity in institutional capacity, with an average maturity level of 2.0 on a 5-point scale (corresponding to 'Managed' processes). Figure 1 presents governance maturity assessment across five critical dimensions, showing significant gaps between the current state and the required international standards.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26feb1298

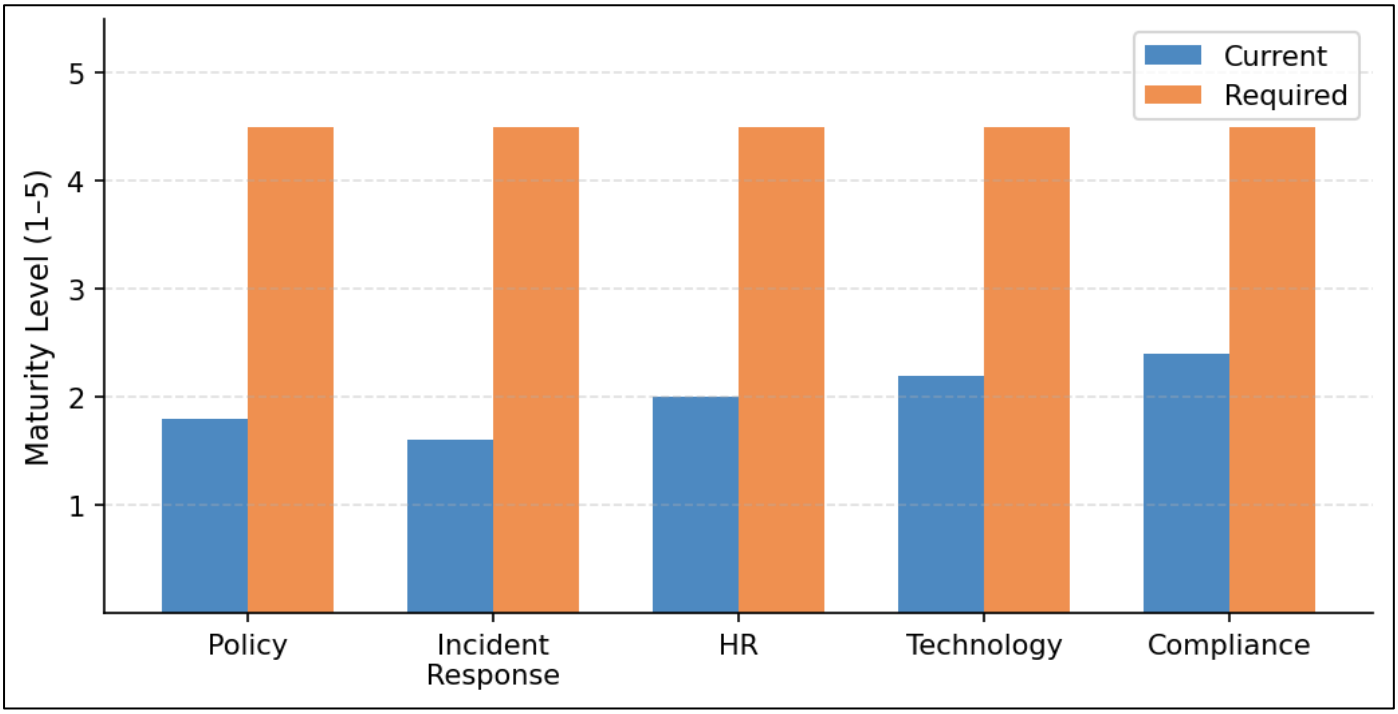

Fig 1 Cybersecurity Governance Maturity Assessment Showing a Significant gap Between the Current State and the Required International Standards.

➢ *Institutional Capacity Metrics*

Table 1 presents institutional capacity assessment across three primary dimensions. Key finding: Only 26% of government agencies maintain adequate numbers of dedicated security personnel; only 17% have deployed SIEM systems.

Table 1 Institutional Capacity Assessment Metrics (n=87 Respondents, 23 Organizations)

Capacity Dimension	Mean	SD	Range	% Adequate
Human Resources				
Dedicated Security Personnel	2.3	1.8	0–8	26%
Certified Personnel	1.1	0.9	0–4	11%
Training (hrs/year)	6.4	8.2	0–32	19%
Technology				
Firewalls Deployed	18/23	–	–	78%
SIEM Systems	4/23	–	–	17%
Endpoint Protection	9/23	–	–	39%
Financial				
Annual Budget (USD)	18,400	26,500	1.2K–89K	22%
% of IT Budget	3.2%	4.1%	0.5%–14%	28%

➢ *Regression Analysis: Hypothesis 1*

Multiple linear regression testing H1 yielded:

$$\hat{GE} = 0.52 + 0.34(\text{HR Cap.}) + 0.28(\text{Budget}) + 0.31(\text{Tech.}) + e$$

Model Statistics: $R^2 = 0.687$ ($p < 0.001$); Adjusted $R^2 = 0.671$; $F(3,83) = 42.14$; $n = 87$.

- *H1 Conclusion:*

All three capacity variables demonstrated statistically significant positive relationships with governance effectiveness ($p < 0.01$). We reject the null hypothesis. Human resource capacity emerged as the strongest predictor ($\beta = 0.341$).

Table 2 Regression Results: Institutional Capacity as Governance Effectiveness Predictor

Variable	Coef.	SE	t	p
Intercept	0.524	0.342	1.53	0.129
HR Capacity	0.341	0.087	3.92	<0.001***
Budget	0.283	0.101	2.80	0.006**
Technology	0.312	0.095	3.28	0.002**

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26feb1298

➢ *Policy Analysis Results*

- *Policy Framework Assessment*

Documentary analysis identified 34 legislative instruments ostensibly governing cybersecurity. However, detailed content analysis revealed critical coverage gaps across major policy domains. Enforcement mechanisms were found to be critically deficient at 88% (Figure 2).

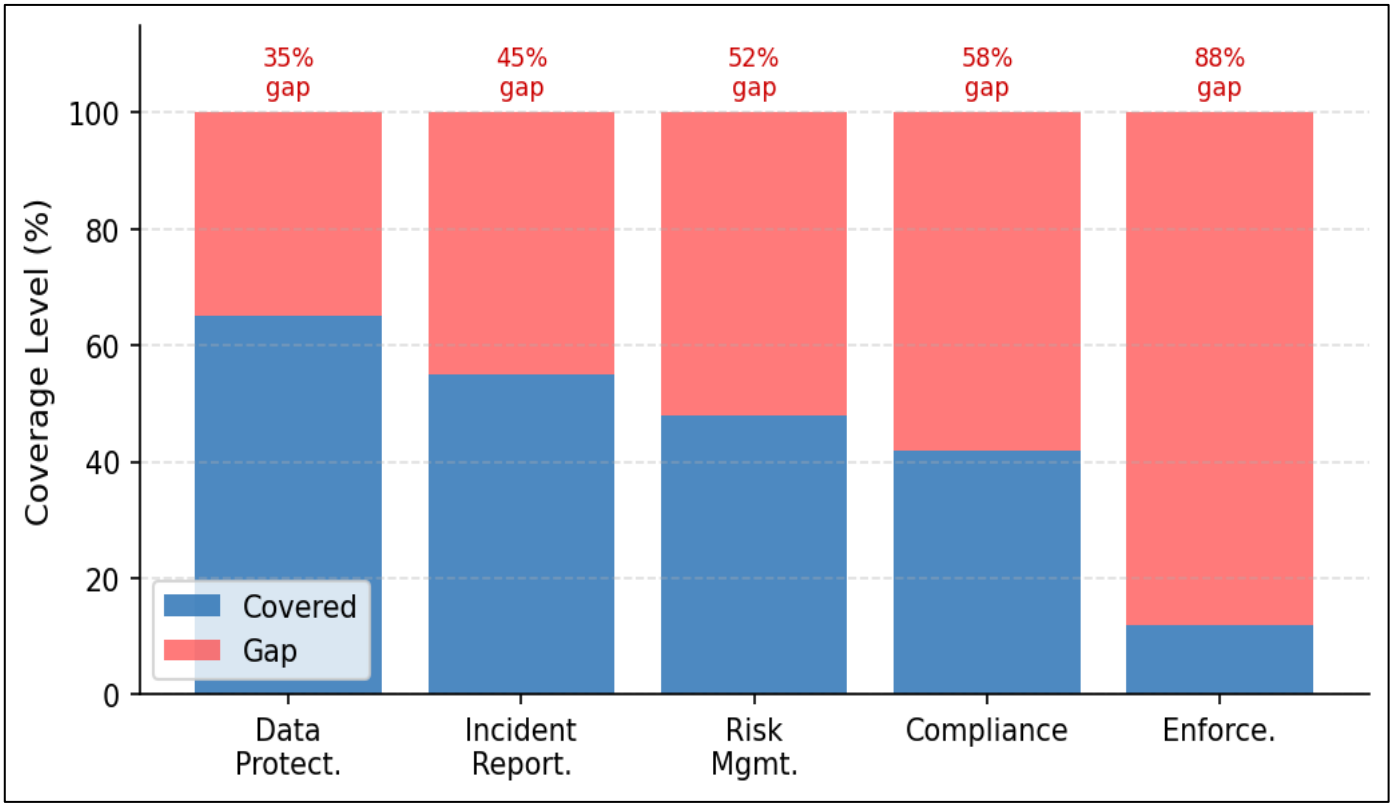

Fig 2 Policy Framework Coverage Gaps Across Cybersecurity Domains. Enforcement Mechanisms are Critically Deficient at 88%.

- *Chi-Square Analysis: Hypothesis 2*

The chi-square test of independence examined the relationship between formal security policy implementation and incident occurrence.

✓ Test Results: $\chi^2 = 6.728$, df = 1, p = 0.009; Cramer's V = 0.361.

✓ Incident Rates: With formal policies: 37.5% (12/32); Without policies: 87.5% (28/32).

✓ H2 Conclusion: Statistically significant relationship confirmed (p = 0.009). Organizations with formal security policies demonstrated 50% lower incident rates. We reject the null hypothesis.

Table 3 Contingency Table — Policy Implementation vs. Incident Occurrence

	Incidents	**No Incidents**	**Total**
Policy	12	8	20
No Policy	28	4	32
Total	40	12	52

➢ *Economic Impact Modeling and Loss Projections*

- *Historical Incident Costs*

Analysis of 156 documented incidents (2018–2025) identified substantial economic impacts. Incidents grew at an 18.3% compound annual growth rate. Total historical losses: USD 3.755 million; Average incident cost: USD 23,680; Most costly type: Ransomware (USD 67,300 mean).

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26feb1298

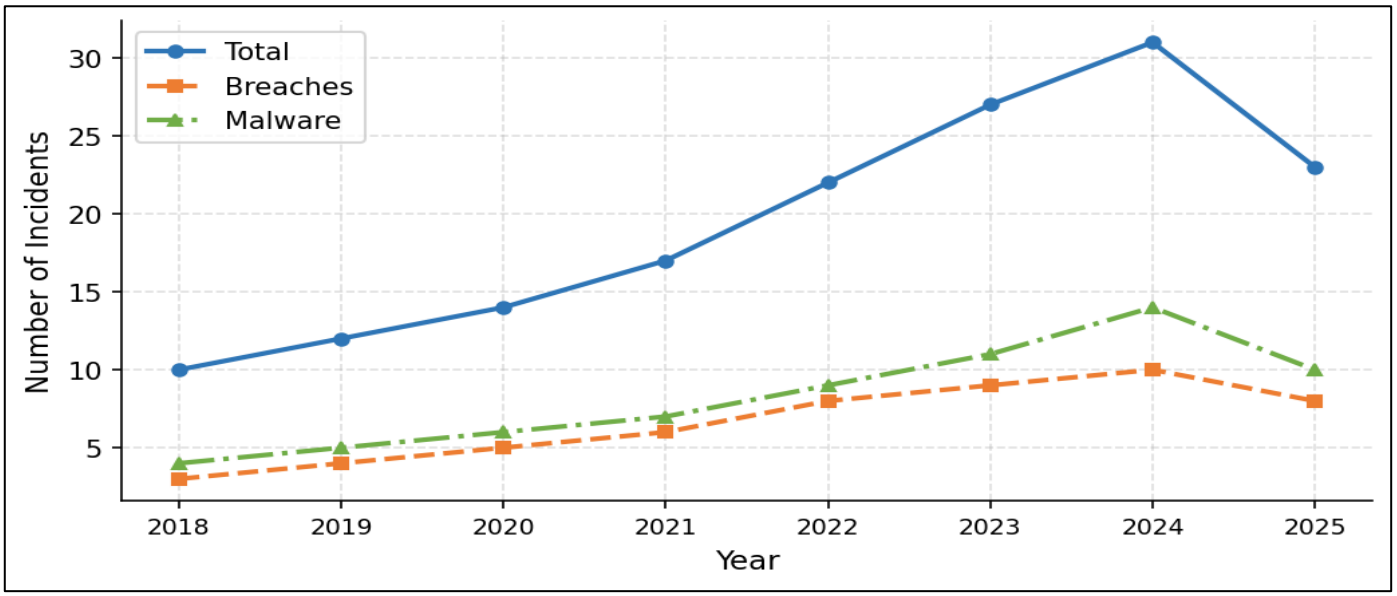

Fig 3 Temporal Trends in Cybersecurity Incidents Showing 18.3% Compound Annual Growth Rate.

Table 4 Economic Loss by Incident Type (USD), 2018–2025

Incident Type	Freq.	Mean Cost	Total Loss
Unauthorized Access	34	8,200	278,800
Data Breach	28	34,500	966,000
Malware	52	12,800	665,600
Ransomware	23	67,300	1,548,000
Denial of Service	19	15,600	296,400
Total	156	23,680	3,755,000

- *Loss Projection Models*
  Three scenarios project economic losses through 2027:

✓ Scenario 1 (Status Quo): $L_t = 3.12 \times 10^5 + 2.18t + 0.34t^2$

✓ Scenario 2 (Moderate Investment): $L_t = 3.12 \times 10^5 + 1.45t - 0.08t^2$

✓ Scenario 3 (Comprehensive Reform): $L_t = 3.12 \times 10^5 + 0.67t - 0.42t^2$

Table 5 Projected Annual Economic Losses (USD) Under Three Scenarios

Year	Status Quo	Moderate	Comprehensive	Savings
2026	1,245K	896K	412K	833K
2027	1,512K	978K	385K	1,127K
Total	2,757K	1,874K	797K	1,960K

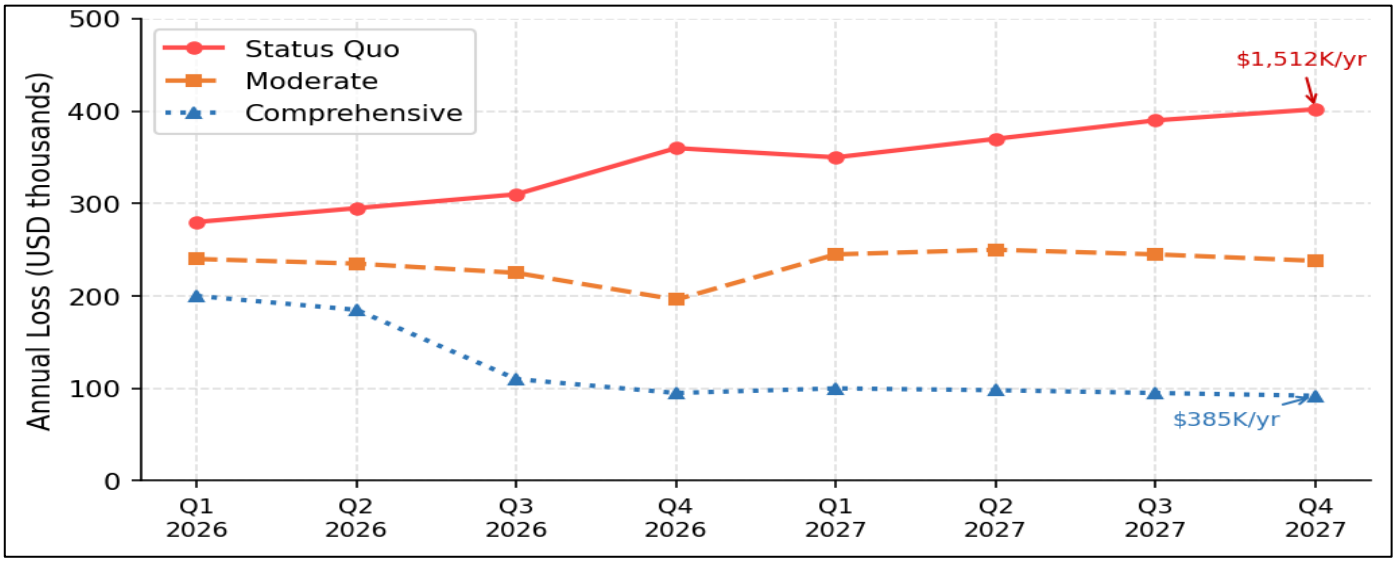

Fig 4 Three-Scenario Loss Projections Demonstrating the Cost-Benefit of Institutional Reform.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26feb1298

➢ *Critical Infrastructure Vulnerability Assessment*

- *Critical Finding:*
  Three sectors (health, power, water) are classified as CRITICAL due to low governance maturity (1.5–1.8).

Table 6 Critical Infrastructure Cybersecurity Vulnerability Assessment by Sector

Sector	Orgs	Critical Vulns	Avg. Maturity	Risk Level
Health Services	4	12	1.8	CRITICAL
Power Distribution	2	11	1.5	CRITICAL
Water Management	2	9	1.7	CRITICAL
Financial Services	3	8	2.4	HIGH
Transportation	3	7	2.1	HIGH
Telecommunications	2	6	2.8	MEDIUM-HIGH

V. POLICY RECOMMENDATIONS AND IMPLEMENTATION STRATEGY

➢ *Identified Policy Deficiencies*

- Mandatory Incident Reporting: No binding notification requirements; the international standard is 24–72 hours.
- Sectoral Security Standards: Absence of minimum-security configurations for critical infrastructure.
- Data Protection Implementation: Weak cybersecurity requirements and enforcement mechanisms.
- Criminal Liability: Insufficient penalties for unauthorized access and data breaches.

➢ *Recommended Reforms*

- *Recommendation 1: Cybersecurity Governance Act*

✓ Mandatory incident reporting (24-hour notification)
✓ National cybersecurity authority with regulatory authority
✓ Risk-based compliance framework for critical infrastructure
✓ Non-compliance penalties: 5–10% of organizational budget

- *Recommendation 2: Institutional Capacity*

✓ National Cyber Response Center (24/7 operations)
✓ Executive-level Information Security Office
✓ Annual budget allocation minimum: 5% of IT budgets
✓ Mandatory employee training: 40 hours annually

- *Recommendation 3: Standards Framework*

✓ Mandatory ISO 27001 for all government agencies
✓ NIST Cybersecurity Framework for critical infrastructure
✓ Annual third-party security audits
✓ Public compliance status disclosure

➢ *Institutional Development and Implementation*

- *Human Resource Development*
  Strategic HR development targeting 150 new security personnel (2026–2027) with:

✓ Professional certification programs (CISSP, CCSK, CEH)
✓ Competitive salary structure (40% above civil service scale)
✓ Annual retention bonuses for certified personnel
✓ Structured career advancement pathways

- *Technology Modernization*

✓ *Short-Term (2026):*
Deploy SIEM in 18 agencies; implement EDR across 500+ systems; establish zero-trust architecture (USD 1.2M).

✓ *Medium-Term (2026–2027):*
Complete SIEM deployment; implement threat intelligence platform; establish disaster recovery (USD 2.8M).

✓ *Long-Term (2027–2029):*
Cloud-based security infrastructure; AI/ML threat detection; full international compliance (USD 4.2M).

- *Implementation Timeline*

Table 7 Multi-Year Implementation Timeline and Resource Requirements

Phase	Timeline	Investment	Personnel
I: Foundation	Q1–Q4 2026	400K	25
II: Infrastructure	2026–2027	3.2M	65
III: Optimization	2027–2028	2.1M	45
IV: Maturation	2028–2029	2.8M	35
Total	4 years	8.5M	170

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26feb1298

- *Return on Investment*

Comprehensive reform (USD 8.5M investment) projects prevention of USD 7.2M in losses (2026–2029), yielding:

✓ Initial net impact: -USD 1.3M
✓ Post-2029 annual benefits: USD 3.8M
✓ Five-year ROI: 247%
✓ Breakeven point: 2028

VI. DISCUSSION

➢ *Hypothesis Testing Interpretation*

The strong regression model ($R^2 = 0.687$, $p < 0.001$) demonstrates that institutional capacity factors substantially explain variance in governance effectiveness. All three predictor variables were statistically significant ($p < 0.01$), with human resource capacity emerging as the strongest predictor ($\beta = 0.341$). These findings align with organizational theory, suggesting that capacity investments yield measurable security improvements.

The chi-square analysis ($\chi^2 = 6.728$, $p = 0.009$) confirms that formal policy implementation significantly reduces incident rates—a 50-percentage-point difference (37.5% vs. 87.5%). The moderate effect size (Cramer's V = 0.361) indicates that policy represents a necessary but insufficient condition; multiple factors collectively determine security outcomes.

➢ *Regional Comparative Context*

Sierra Leone's governance maturity (2.0/5.0) substantially lags regional peers: Kenya (3.2), Nigeria (2.8), and Ghana (2.6). This differential reflects both resource constraints endemic to lower-income nations and suboptimal prioritization of cybersecurity within broader digital governance agendas.

➢ *Economic Impact Implications*

Projected cumulative losses of USD 2.76 million (2026–2027 status quo) represent approximately 0.34% of the government's operating budget. Critical infrastructure disruptions impose multiplied external costs through population health impacts and economic activity constraints.

➢ *Challenges and Implementation Barriers*

- *Technical Challenges:*

✓ Legacy system complexity (62% predate 2015);
✓ Network infrastructure limitations in provincial areas;
✓ Vendor dependency and lock-in.

- *Institutional Barriers:*

✓ Organizational resistance to change;
✓ Fragmented governance structure;
✓ Leadership commitment variability across ministerial transitions.

- *Resource Constraints:*

✓ Competing budgetary priorities;
✓ Human capital scarcity and brain drain;
✓ Insufficient domestic research capacity.

VII. CONCLUSIONS

This comprehensive investigation of cybersecurity governance in Sierra Leone's public sector confirms substantial capacity gaps, policy deficiencies, and escalating economic losses. Both hypothesized relationships received empirical confirmation:

➢ Institutional capacity factors significantly predict governance effectiveness (H1: $p < 0.001$, $R^2 = 0.687$)
➢ Formal policy implementation demonstrably reduces incident rates (H2: $p = 0.009$, 50% rate reduction)
➢ Economic losses under status quo: USD 2.76M (2026–2027)
➢ Comprehensive reform potential: USD 797K projection (71% reduction)
➢ Five-year ROI: 247% on USD 8.5M investment

- *Successful Implementation Requires:*

✓ Legislative action establishing a cybersecurity governance mandate;
✓ Institutional development, including the National Cyber Response Center;
✓ Human resource investment targeting 150 new personnel;
✓ Technology infrastructure modernization (USD 8.5M phased approach);
✓ International cooperation through ECOWAS partnerships.

These investments are essential for protecting critical national infrastructure, ensuring continuity of public services, and establishing sustainable digital governance foundations.

FUTURE RESEARCH DIRECTIONS

This research establishes a foundational understanding of cybersecurity governance challenges in Sierra Leone. Future investigation should address:

➢ Longitudinal institutional development tracking following reform implementation;
➢ Sectoral comparative analysis of divergent security postures;
➢ International technology transfer mechanisms;
➢ Citizen privacy implications of expanding security infrastructure.

ACKNOWLEDGMENTS

The author acknowledges 87 cybersecurity professionals and institutional representatives from 23 government agencies for their participation. Technical support from the University of Makeni and international

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26feb1298

mentorship from Nankai University are gratefully recognized.

REFERENCES

[1]. Shamala, P., Choo, K.-K. R., and Bertino, E., "Reconsidering the role of RBAC administration in least privilege," Journal of Computer Security, vol. 25, no. 1, pp. 21–45, 2017.
[2]. North, D. C., Institutions, Institutional Change and Economic Performance. Harvard University Press, 1990.
[3]. World Economic Forum, "Global cybersecurity outlook: Executive summary," WEF Reports, pp. 1–28, 2023.
[4]. National Institute of Standards and Technology, NIST Cybersecurity Framework Version 2.0. NIST, Gaithersburg, MD, 2023.
[5]. Frangopoulos, F., Sarvanis, M., and Karanikos, D., "Governance and institutional mechanisms for information security in public administration," International Journal of Information Security, vol. 18, no. 4, pp. 445–462, 2019.
[6]. Cavusoglu, H., Mishra, B., and Raghunathan, S., "The effect of internet security breaches on market value of e-commerce firms and strategic value of information technology assets," Journal of Management Information Systems, vol. 21, no. 1, pp. 137–159, 2004.
[7]. Kshetri, N., "Cybercrime and cybersecurity in sub-Saharan Africa," Journal of Global Information Technology Management, vol. 20, no. 4, pp. 209–229, 2017.
[8]. International Organization for Standardization, ISO/IEC 27001:2022 Information Security Management Systems. ISO, Geneva, 2022.
[9]. African Union, African Union Cybersecurity Framework. AU Commission, Addis Ababa, 2021.
[10]. Kaplan, A. Z. and Haenlein, M., "Siri, Alexa, and other digital assistants: A study of customer satisfaction with artificial intelligence applications," Journal of Service Marketing, vol. 33, no. 6, pp. 649–663, 2019.