

Challenges in Implementing Cybersecurity Services in Bangladesh's Financial Sector: Survey Evidence and a Risk-Based Implementation Framework

Mr. Md Shahidullah

Head of Cyber Security, Cyber Sevcurity, Betopia Limited

Abstract

Financial institutions depend on digital services to deliver transactions and manage sensitive customer information, yet cybersecurity investments do not automatically translate into sustained protection. This paper examines organizational and operational barriers to implementing cybersecurity services in Bangladesh's banking and non-bank financial institution (NBFI) sector. It synthesizes the survey results reported in the author's thesis and proposes a practical risk-based implementation framework connecting risk assessment, business requirements, procurement, deployment, operational ownership, monitoring, and continual improvement. The thesis reports 554 survey responses and provides counts for eight implementation challenges. The most frequently endorsed issues were cybersecurity tool cost (530/554; 95.7%), limited employee cybersecurity awareness (523/554; 94.4%), insufficient resources for continuous monitoring (501/554; 90.4%), and management budget-approval difficulties (491/554; 88.6%). Weak cross-functional communication and inadequate qualified resources were also frequently reported (478/554; 86.3%), as was the absence of practical security policies and procedures (463/554; 83.6%). These descriptive results suggest that implementation barriers span financial, human, governance, and operational dimensions rather than technology selection alone. The proposed framework prioritizes business-aligned risk assessment, evidence-based business cases, transparent procurement, implementation readiness, defined service ownership, continuous monitoring, and periodic assurance. The findings are useful as an initial diagnostic for financial institutions, but should be interpreted cautiously because the thesis contains an inconsistent sample-size statement and does not fully document sampling, instrument validation, or inferential analysis. Further research should validate the results using a clearly defined sample and institution-level measures of cybersecurity outcomes.

Keywords-cybersecurity implementation; financial sector; Bangladesh; cybersecurity governance; risk assessment; security procurement; continuous monitoring

1. Introduction

Digital banking, electronic payments, interconnected platforms, and third-party technology services have expanded the attack surface of financial institutions. Protecting customer information and maintaining service availability require more than purchasing security products: controls must be appropriately

selected, integrated, configured, staffed, monitored, and periodically reviewed. Where any of these activities is neglected, a nominally deployed solution may offer limited operational value.

The author's thesis, "A Study of the Challenges of Implementing Cyber Security Services and Solutions in the Bangladeshi Financial Sector" (Bangladesh University of Professionals, 2023), identifies implementation and operational difficulties in banks and NBFIs. Its central concern is the gap between the availability of cybersecurity technologies and the organizational ability to procure, deploy, and operate them effectively. The thesis discusses technical controls-including security operations, identity and access management, endpoint protection, vulnerability management, data loss prevention, and network security-but also emphasizes budget approval, skills, awareness, communication, policies, and monitoring.

This paper condenses that work into a research-article structure, foregrounding the survey results and the proposed implementation process rather than reproducing the thesis's extensive catalogue of security products. It addresses three questions: (1) Which implementation barriers were most frequently reported? (2) What do these barriers imply for cybersecurity governance in financial institutions? (3) How can risk assessment be connected to procurement, deployment, and sustained operations?

2. Background and Related Work

Prior work cited in the thesis presents cybersecurity as a management and organizational challenge as well as a technical one. Atoum, Ootom, and Abu Ali (2014) describe a holistic approach to cybersecurity implementation, while the NIST Cybersecurity Framework provides a risk-oriented structure for organizing cybersecurity activities (NIST, 2018). Research on cybersecurity governance also highlights the importance of management attention, institutional pressures, and clear accountability (Yusif & Hafeez-Baig, 2021; Shaikh & Siponen, 2023). Studies of employee engagement point to the role of awareness and organizational culture in maintaining security practices (Reeves et al., 2021).

The thesis identifies a context-specific research gap: limited practical evidence on why cybersecurity solutions are not consistently purchased, implemented, and operated in Bangladesh's financial sector. Its contribution is therefore applied and process-oriented: it brings reported implementation barriers together with a proposed risk-based sequence for selecting, procuring, deploying, and maintaining controls. The available survey results are descriptive and do not establish causal relationships between individual barriers and security outcomes.

3. Methodology

3.1 Research design and data source

This paper uses a secondary analysis of the survey counts reported in the author's thesis. The thesis describes a questionnaire survey directed at personnel associated with banks and NBFIs, including IT, information security, management, and procurement functions. The results chapter reports 554 responses and tabulates "Yes" and "No" answers to eight statements about implementation challenges. The present paper does not claim to have collected new data.

3.2 Analysis

For each statement, the endorsement percentage was calculated as Yes responses divided by 554 and multiplied by 100. The values are descriptive frequencies; no significance tests, causal estimates, or institution-level comparisons are inferred. Percentages are rounded to one decimal place.

3.3 Data-quality note

The thesis is internally inconsistent about sample size: the abstract and results table describe 554 participants, whereas the conclusion section refers to 117 respondents. The eight-item table sums to 554 responses per item and is used here as the basis for the calculations. Before journal submission, the author should verify the original dataset, confirm the final analytic sample, and reconcile this discrepancy. The thesis does not provide enough detail in the sections reviewed to establish the sampling frame, response rate, questionnaire validation, or missing-data treatment; these should be added if records are available.

4. Results

Table 1 presents the eight challenge statements and the corresponding response counts reported in the thesis. Cost was the most frequently endorsed barrier, followed by employee awareness, monitoring capacity, and management budget approval.

Reported challenge	Yes (n)	No (n)	Yes (%)
Cybersecurity tool cost	530	24	95.7%
Lack of employee cybersecurity awareness	523	31	94.4%
Insufficient resources for continuous monitoring	501	53	90.4%
Management budget-approval difficulty	491	63	88.6%
Weak communication/teamwork and shortage of qualified resources	478	76	86.3%
Absence of practical IT security policies, procedures, guidelines, and SOPs	463	91	83.6%
Insufficient presentation of need to senior management using risk/SROI	390	164	70.4%
Complexity of installation/configuration within the timeframe	297	257	53.6%

Table 1. Reported implementation challenges and calculated endorsement percentages (n = 554).

The reported pattern has four implications. First, cost and budget approval appear to constrain adoption, but affordability should be assessed across the control lifecycle-not only the initial purchase price. Second, the high endorsement of awareness-related challenges indicates that technical controls need to be reinforced by employee education and security culture. Third, continuous monitoring capacity was a

major concern, suggesting that organizations should assess staffing, service coverage, alert handling, and escalation arrangements before deployment. Fourth, the frequency of communication and policy-related issues points to the importance of clear accountability and operational procedures.

The two less frequently endorsed items remain material. Approximately 70.4% endorsed inadequate presentation of the business case to senior management, while 53.6% endorsed installation or configuration complexity within the required timeframe. These results suggest that cybersecurity proposals need to translate technical risk into business impact and that implementation planning should include integration, testing, training, and acceptance criteria.

5. A Risk-Based Cybersecurity Implementation Framework

Based on the process described in the thesis, a practical implementation framework can be organized into seven connected stages. The stages are intended as a management sequence, not as a claim that the survey experimentally validated the framework.

Stage 1 - Establish business context and asset priorities. Identify critical services, customer and transaction data, key systems, dependencies, regulatory obligations, and business continuity requirements. Involve business owners, IT, security, risk, compliance, procurement, and relevant third parties.

Stage 2 - Assess and prioritize risk. Inventory assets; identify credible threats and vulnerabilities; evaluate likelihood and business impact; review existing controls; and record residual risk. Prioritize remediation according to risk exposure and business criticality rather than vendor preference alone.

Stage 3 - Define requirements and build the business case. Translate priority risks into measurable control requirements. Estimate lifecycle costs, including licensing, integration, implementation, training, staffing, maintenance, and renewal. Explain risk reduction and service resilience in terms senior management can evaluate.

Stage 4 - Conduct transparent, risk-aligned procurement. Develop evaluation criteria before soliciting proposals. Assess functional fit, interoperability, scalability, support, data handling, vendor risk, service-level commitments, total cost of ownership, and exit arrangements. Document the rationale for selection.

Stage 5 - Prepare, deploy, and validate. Assign an accountable owner and implementation lead. Confirm prerequisites, dependencies, change approvals, rollback plans, test cases, and acceptance criteria. Conduct configuration reviews and user-acceptance testing before operational handover.

Stage 6 - Operate, monitor, and respond. Define who monitors alerts, investigates incidents, maintains rules and signatures, applies patches, manages access, and escalates events. Where internal capacity is limited, evaluate a managed service while retaining internal governance and oversight.

Stage 7 - Measure, assure, and improve. Review control coverage, vulnerability remediation time, monitoring coverage, incident response performance, policy exceptions, training completion, and audit findings. Reassess risk periodically and after material changes or incidents; feed lessons into budgets and the next procurement cycle.

The thesis proposes a risk-calculation expression: $\text{Risk} = (\text{Threat} \times \text{Vulnerability} \times \text{Probability of occurrence} \times \text{Impact}) / \text{Controls}$, with component scores described on a 0-10 scale. This expression can serve as a conceptual prioritization aid, but its operational use requires a defined scoring rubric, a treatment of zero or missing control values, calibration, and validation against observed outcomes.

Because the formula is not empirically validated in the thesis, it should not be presented as a standardized or validated risk model.

6. Discussion

The survey results indicate that implementation barriers are interdependent. High tool cost may be intensified by weak business cases, unclear ownership, or procurement processes that focus on acquisition rather than the full operating lifecycle. A tool that is purchased without sufficient staffing, integration, runbooks, or escalation arrangements can become a control in name only. Accordingly, cybersecurity investment decisions should evaluate operational readiness alongside technical capability. The prominence of employee awareness reinforces the need to embed security responsibilities into daily work. Awareness activities should be role-based and continuous, supported by practical reporting channels and management reinforcement. Similarly, the reported absence of policies and standard operating procedures suggests that technical deployment should be accompanied by documented procedures for access management, change control, incident response, vulnerability remediation, backup and recovery, and third-party access.

The findings also support a lifecycle view of procurement. Evaluation should not stop at product features or acquisition price. Financial institutions should estimate total cost of ownership and test whether the organization can sustain monitoring, maintenance, upgrades, incident handling, and vendor support. Shared services or managed security services may help address capacity gaps, but outsourcing does not remove the institution's responsibility for risk ownership, oversight, and regulatory obligations.

These implications are consistent with risk-based cybersecurity governance approaches such as the NIST Cybersecurity Framework and holistic implementation models. However, the study's descriptive data do not demonstrate that any particular intervention will cause a measurable improvement. The framework should be treated as a practice-oriented synthesis that requires field validation.

7. Practical Recommendations

- Require a documented risk assessment and business owner before approving major cybersecurity purchases.
- Use lifecycle cost and operational-readiness criteria in procurement, not price or feature lists alone.
- Assign named owners for implementation, monitoring, incident response, patching, and periodic control review.
- Create and exercise standard operating procedures for priority security operations and incident escalation.
- Provide recurring, role-specific cybersecurity awareness and measure participation and behavioural outcomes.
- Track a small set of board-level indicators, including critical-risk treatment, monitoring coverage, remediation timeliness, incident trends, and unresolved audit findings.
- Review third-party and managed-service arrangements for service levels, escalation, data handling, evidence access, and exit/continuity plans.

8. Limitations and Future Research

This paper inherits limitations from the underlying thesis. The inconsistency between 554 responses in the results table and 117 respondents in the conclusion must be resolved. The available documentation

does not fully specify the sampling method, response rate, respondent distribution by institution or role, questionnaire development and validation, or the treatment of missing data. The eight-item results are self-reported and descriptive; they may reflect perceptions rather than independently audited control deficiencies. The study also does not provide inferential tests or longitudinal evidence that would establish relationships between barriers and security outcomes.

Future work should reconcile the dataset and publish a transparent methodology, including the sampling frame, survey instrument, respondent profile, ethics/consent procedures where applicable, and analysis plan. Researchers could compare banks and NBFIs by size, ownership, maturity, or digital-service exposure; test relationships among management support, skills, monitoring capability, and control effectiveness; and evaluate the proposed framework through case studies or pre/post implementation metrics. Objective measures-such as mean time to remediate critical vulnerabilities, alert triage times, incident recovery performance, audit exceptions, and control coverage-would strengthen the evidence base.

9. Conclusion

This paper reframes the author's thesis as an applied study of cybersecurity implementation barriers in Bangladesh's financial sector. In the thesis's eight-item results table, cost, employee awareness, monitoring capacity, management budget approval, cross-functional communication, and policy/procedure gaps were frequently endorsed. The pattern suggests that cybersecurity effectiveness depends on a coordinated combination of technology, people, governance, procurement, and sustained operations. A seven-stage risk-based framework is presented to connect asset prioritization and risk assessment with business cases, procurement, deployment validation, monitoring, and continual improvement. The survey findings offer a useful diagnostic, but the sample-size discrepancy and incomplete methodological reporting should be resolved before publication. The framework should be evaluated in future research using transparent sampling and measurable operational outcomes.

References

1. Atoum, I., Otoom, A., & Abu Ali, A. (2014). A holistic cyber security implementation framework. *Information Management & Computer Security*, 22(3), 251-264.
2. National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>
3. Reeves, A., Delfabbro, P., & Calic, D. (2021). Encouraging employee engagement with cybersecurity: How to tackle cyber fatigue. *SAGE Open*, 11(1). <https://doi.org/10.1177/21582440211000049>
4. Shaikh, F. A., & Siponen, M. (2023). Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity. *Computers & Security*, 124, 102974.
5. Yusif, S., & Hafeez-Baig, A. (2021). A conceptual model for cybersecurity governance. *Journal of Applied Security Research*, 16(4), 490-513.
6. Shahidullah, M. (2023). A Study of the Challenges of Implementing Cyber Security Services and Solutions in the Bangladeshi Financial Sector [Master's thesis, Bangladesh University of Professionals].