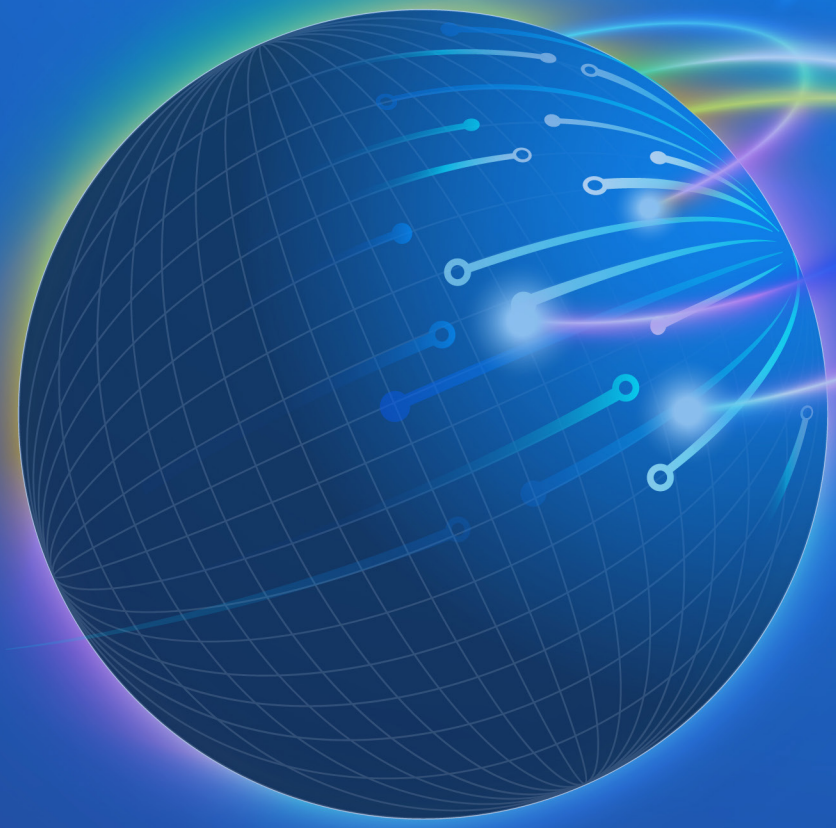
American Journal of Geospatial Technology (AJGT)

ISSN: 2833-8006 (ONLINE)

VOLUME 4 ISSUE 1 (2025)



PUBLISHED BY
E-PALLI PUBLISHERS, DELAWARE, USA

American Journal of Geospatial Technology (AJGT)

Volume 4 Issue 1, Year 2025
ISSN: 2833-8006 (Online)
DOI: https://doi.org/10.54536/ajgt.v4i1.5355
https://journals.e-palli.com/home/index.php/ajgt

From Reactive to Proactive: Engineering a Next-Generation Cyber Threat Response Emergency Operations Center (EOC) for Financial Institutions

Sk Monirul Islam Mahadi[1], Shuvo Kumar Mallik[2*], Nahid Raza Shatu[3], M Abeedur Rahman[4]

Article Information

Received: May 17, 2025

Accepted: June 20, 2025

Published: July 24, 2025

Keywords

Cyber Threat, EOC, Financial Institutions, Next-Generation

ABSTRACT

The financial sector remains one of the most targeted domains for cyberattacks, demanding advanced and adaptive cybersecurity strategies. Traditional Emergency Operations Centers (EOCs) are predominantly reactive, leaving financial institutions vulnerable to sophisticated and rapidly evolving threats. This paper proposes a transformative approach: designing a next-generation, proactive Cyber Threat Response EOC explicitly tailored for financial organizations. By synthesizing insights from case studies, expert interviews, and industry surveys, this study introduces a conceptual framework that integrates predictive analytics, threat intelligence, automation, and collaborative defense models. The framework aims to enhance early threat detection, reduce response times, and build organizational resilience against emergent cyber threats.

INTRODUCTION

The financial sector stands at the frontline of the global digital economy, serving as a critical backbone for commerce, investment, and individual wealth management (George, 2024). However, its centrality and reliance on vast, interconnected digital infrastructures have also rendered it one of the most targeted industries for cyberattacks. In recent years, cyber adversaries have grown increasingly sophisticated, evolving from opportunistic actors who deploy simple malware or engage in fraud to well-organized, persistent threat groups that execute coordinated ransomware campaigns, deploy banking trojans, orchestrate phishing schemes, and even engage in state-sponsored cyber espionage (Bardin, 2025). This rapidly shifting cyber-threat landscape demands a fundamental transformation in how financial institutions detect, respond to, and anticipate cyber incidents. Historically, Emergency Operations Centers (EOCs) within financial organizations have operated on reactive models (Jiang *et al.*, 2025). These traditional setups are typically designed to detect breaches and mobilize incident response teams in the event of an attack. While effective in specific legacy scenarios, this approach is no longer sufficient in today's rapidly evolving digital environment. Modern cyber threats occur at machine speed, exploiting vulnerabilities before they can be patched and leveraging automation to amplify damage across systems. In this context, time is of the essence. Delayed responses to cyber incidents can exacerbate the scale of the breach, leading to prolonged system downtime, substantial financial losses, regulatory penalties, and irreparable reputational damage (George *et al.*, 2024).

Despite increased investments in cybersecurity technologies ranging from advanced firewalls to threat intelligence platforms, many financial institutions remain constrained by reactive mindsets and siloed operational models. These organizations often face challenges such as fragmented situational awareness (SA), lack of coordination across departments, limited access to real-time data, and insufficient predictive capabilities. Consequently, cyber incidents are often addressed in isolation, with critical decisions made based on incomplete or outdated information. This hampers the institution's ability to mount an effective, timely, and holistic response (Smidt *et al.*, 2024).

A key weakness in traditional EOCs is the lack of integration between cyber situational awareness (CSA), incident response processes, and business continuity planning. As threat actors deploy increasingly advanced tactics, financial institutions require more than just reactive tools. They need the foresight and agility to anticipate, prepare for, and neutralize threats before they cause harm. This necessitates a paradigm shift from reactive containment to proactive orchestration of cyber defense (Arora, 2025).

The envisioned transformation centers on the development of a next-generation Cyber Threat Response Emergency Operations Center (EOC), a dynamic, intelligent, and agile hub that can predict threats, assess risks in real time, and coordinate cross-functional responses across the enterprise. This advanced EOC would be underpinned by a robust technological architecture featuring artificial intelligence (AI) driven predictive analytics, automated threat detection, and real-time data integration (Nazir *et al.*, 2025). Equally important is the adoption of shared intelligence frameworks that foster collaboration between internal teams and external partners, including government agencies, cybersecurity firms, and other financial institutions.

Such an evolution calls for an interdisciplinary approach,

[1] Department of Cybersecurity at Rowan University, Glassboro, New Jersey, USA.
[2] Department of Economics, Southeast University, Dhaka, Bangladesh.
[3] Senior Executive MI and Operations Credit Control Service, HSBC Banglades
[4] Assistant Professor, Department of Economics, Southeast University, Dhaka, Bangladesh.
[*] Corresponding author's e-mail: nextgenresearch.info@gmail.com

drawing insights from cybersecurity, data science, risk management, and systems engineering. It also requires a cultural shift within organizations, promoting a mindset of continuous learning, simulation-based preparedness, and cross-departmental collaboration. Proactively building cyber resilience is not merely a technological challenge; it is a strategic imperative for survival in an era of relentless digital threats.

This research proposes a comprehensive model for engineering a next-generation Cyber Threat Response EOC explicitly tailored for the financial sector. By integrating cyber situational awareness (CSA) frameworks with team situational awareness, this model aims to enhance decision-making, reduce response times, and elevate the overall cybersecurity posture of financial institutions. Through this shift from reactive to proactive operations, organizations can not only mitigate risks more effectively but also safeguard the trust and stability essential to the global financial ecosystem (Vasiliu-Feltes, 2024).

Research Questions

This study aims to investigate the transformation necessary for financial institutions to transition from a reactive to a proactive cyber threat response posture. The core research questions are:

- What are the defining characteristics of a next-generation, proactive cyber threat response EOC?
- How can predictive analytics and threat intelligence be optimally integrated into EOC workflows?
- What technological and architectural innovations are essential for building future-ready EOCs?
- What organizational models and staffing strategies best support proactive cybersecurity operations?
- How can the performance and return on investment (ROI) of such EOCs be effectively evaluated?

Research Objectives

- Define and validate the key features and functions of a next-generation proactive EOC.
- Construct a conceptual framework that enables real-time cyber situation awareness (CSA) and threat mitigation.
- Identify the enabling technologies, processes, and interdisciplinary skill sets required.
- Recommend implementation strategies and performance metrics that can guide organizations in transitioning to and maintaining proactive cyber defense operations.

LITERATURE REVIEW

The rapid digitization of financial institutions has significantly transformed the cybersecurity landscape, bringing both unprecedented opportunities and heightened risks (Vasiliu-Feltes, 2024). As financial organizations increasingly rely on interconnected digital infrastructure, cyber threats have become more complex and frequent, necessitating a shift from reactive to proactive cyber threat response mechanisms. This literature review explores critical perspectives on situational awareness (SA) in teams, cyber situational awareness (CSA), information sharing, and risk management, highlighting gaps and opportunities for engineering a next-generation Cyber Threat Response Emergency Operations Center (EOC) tailored for financial institutions in Bangladesh.

Situational awareness is foundational for effective cyber defense. Within team contexts, SA from multiple perspectives: individual awareness, shared awareness among members, and a combined collective awareness that supports coordinated action. Individual SA refers to a person's understanding of relevant environmental factors, whereas shared or team SA involves communication and mutual understanding across team members to form a coherent operational picture. In cybersecurity teams, this distinction is crucial since threat detection and incident response require rapid assimilation and interpretation of evolving information (Naseer *et al.*, 2024).

Research has emphasized that effective team SA depends heavily on communication processes that enable the construction of shared mental models (Carraro *et al.*, 2025). These shared models would allow teams to interpret data consistently, coordinate responses effectively, and make informed decisions promptly. In high-stakes environments, such as cyber defense, where information overload is common, maintaining synchronized team situational awareness (SA) is challenging but essential to avoid gaps in threat detection and mitigation.

Despite significant work on Team SA in fields like military operations, transportation, and emergency response, there is a limited exploration of Team SA explicitly tailored to the financial sector (Samunderu, 2024). Financial institutions face unique challenges due to their high-value targets, complex threat actors, and the regulatory environment in which they operate. This gap highlights the need for research on how team SA manifests in cyber threat response units within financial institutions, particularly in emerging economies such as Bangladesh.

Cyber situational awareness (CSA) extends traditional situational awareness (SA) concepts into the cyber domain, encompassing the perception of network events, comprehension of their significance, and projection of potential future impacts. CSA frameworks often build upon Endsley's three-level model of perception, understanding, and projection, but operationalizing these levels in cybersecurity environments remains an ongoing challenge (Hawash *et al.*, 2024).

Studies reveal that cyber defense analysts primarily focus on event detection and orientation corresponding to the first two levels of SA. Detection involves recognizing deviations from normal network states, while orientation pertains to understanding the context and implications of these events. However, there is a notable gap in explicitly incorporating predictive analytics (projection) into operational CSA. Analysts seldom articulate a need for forward-looking information to anticipate threat evolution and prepare preemptive responses, which

suggests an area ripe for advancement in EOCs.

Information requirements for effective CSA span multiple dimensions, ranging from technical indicators such as intrusion detection system alerts and malware signatures to broader intelligence on adversary tactics, techniques, and procedures (TTPs). Successful CSA frameworks integrate these layers to form a comprehensive understanding that supports strategic, operational, and tactical decision-making (Alsamhi *et al.*, 2024).

A common operational picture (COP) is a shared framework that presents unified situational data to decision-makers, enabling them to have aligned awareness and coordinated action. In multi-agency or multi-team cyber incident response, a COP helps overcome challenges related to geographical dispersion, organizational silos, and diverse expertise.

Effective COPs rely on technological solutions that aggregate and structure information, but equally important are shared institutional, cultural, and experiential backgrounds among decision-makers. Such commonality ensures that data is interpreted consistently, facilitating uniform understanding and joint prioritization of threats.

In the financial sector, particularly in contexts such as Bangladesh, where public-private partnerships are evolving, COPs can foster enhanced cooperation among banks, regulators, and law enforcement agencies. Yet, current practices show limited mechanisms for real-time collaborative information sharing, which hinders proactive threat detection and unified response efforts. The development of integrated platforms supporting dynamic COPs remains an essential objective for next-generation EOCs (Cespedes-Cubides & Jradi, 2024).

Financial institutions traditionally emphasize risk management as a core operational function. While credit and market risks have long dominated attention, operational risks, including cyber risks, have gained prominence alongside increasing technological dependence. Cyber risks are multifaceted, stemming from human error, system vulnerabilities, process failures, and external threat actors.

Operational cyber risk management involves identifying critical information assets, assessing vulnerabilities, and deploying safeguards. However, the complexity of cyber threats challenges conventional risk quantification methods, prompting the need for more adaptive and intelligence-driven approaches. Emerging models advocate incorporating intelligence beyond purely technical indicators, extending to organizational behaviors, threat actor motivations, and the broader cyber landscape. This holistic perspective supports both single-loop learning focused on immediate corrective actions and double-loop learning, which facilitates strategic changes in policies, workflows, and security postures (Auqui-Caceres & Furlan, 2023).

For financial institutions in Bangladesh, strengthening cyber risk management through advanced CSA and threat intelligence integration is vital. Institutional learning and adaptation must keep pace with the evolving threat environment to reduce vulnerabilities and enhance resilience. Threat intelligence has evolved into a multi-layered discipline encompassing strategic, operational, tactical, and technical information. Strategic intelligence supports long-term risk management, while operational intelligence focuses on imminent threats. Tactical intelligence details attacker methods, and technical intelligence provides granular indicators of compromise (Yu *et al.*, 2023).

Despite the richness of threat intelligence frameworks, financial sector EOCs often underutilize automation tools that could accelerate threat lifecycle management. Security Orchestration, Automation, and Response (SOAR) platforms have emerged to automate repetitive tasks, integrate disparate data sources, and orchestrate coordinated responses across tools and teams. However, the adoption of SOAR and predictive analytics within financial institutions remains inconsistent, particularly in developing markets. The limited integration of these technologies hinders the ability of EOCs to transition from reactive firefighting to proactive threat anticipation and mitigation (Negi *et al.*, 2024).

MATERIALS AND METHOD

This study employed two complementary data collection methods to explore the design and development of a next-generation cyber threat response Emergency Operations Center (EOC) tailored for financial institutions in Bangladesh. The first method involved distributing a structured questionnaire to participants engaged in a national-level cyber incident management exercise within the financial sector. The second method consisted of in-depth interviews with key leaders who facilitated coordination and cooperation conferences during the same exercise. Each dataset was analyzed separately before being combined for joint interpretation and analysis. The findings were then compared with existing theories to draw relevant conclusions.

The questionnaire was administered during a dedicated debrief session held several weeks after the exercise. Approximately 70 individuals participated in this session, which also included training elements. However, not all attendees were present during the distribution of the questionnaire. Before completing the survey, participants were informed about the study's objectives. Printed questionnaires were distributed, which took approximately 20 minutes to complete. In total, 42 responses were collected, although some questionnaires were only partially completed. Towards the end of the session, one of the researchers provided a brief presentation on emerging concepts related to common operational pictures (COP) and cyber situational awareness. Participation in the study was voluntary, and no compensation was provided.

Figure 1: The distribution of the participating organizations (N = 42).

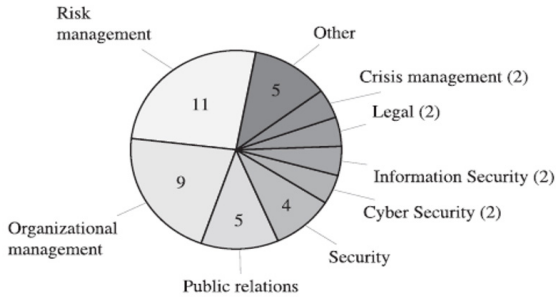


Figure 2: The distribution of the different roles of the participants (N = 42).

The questionnaire consisted of ten open-ended questions designed to address two primary research goals. The first seven questions aimed to identify essential information elements for a financial sector cyber threat response COP, clarify intended users, and understand information-sharing practices. The last three questions focused on exploring current systematic practices related to the creation and maintenance of a cyber threat Command and Control (COP). These questions were carefully developed to capture a broad range of perspectives and reflect real-world practices within the financial sector.

The questions asked included the following

1. What types of information are critical to include in a common operational picture for cyber threat response?
2. Which roles or positions within your organization are intended to use this operational picture?
3. What types of decisions should be supported by the situational awareness provided by the operational picture?
4. What information does your organization contribute to shared operational pictures?
5. Which external organizations could benefit from your organization's shared operational picture data?
6. How does your organization track cyber-related issues that could impact your operations?

No formal definitions of key terms, such as "cyber threat" or "common operational picture," were provided in the questionnaire, allowing respondents to express their interpretations of these concepts.

Respondents represented a diverse range of organizations within the financial sector, and their roles predominantly reflected strategic and managerial levels, as the exercise was designed as a tabletop scenario rather than a technical simulation. Many participants identified with risk management, crisis management, security, or information security functions.

For data analysis, responses were divided among the research team members, who independently coded answers by noting the frequency of recurring themes. Responses were categorized into three levels based on mention frequency: (i) frequently mentioned, (ii) occasionally mentioned, and (iii) rarely mentioned. Unique or outlier responses that provided valuable insight were also noted. The team then held multiple collaborative discussions to reach a consensus on the interpretation and documentation of the results. As part of the evaluation process for developing a next-generation Cyber Threat Response Emergency Operations Center (EOC) tailored for financial institutions in Bangladesh, participants were also asked whether they were willing to engage in future phases of the research. Their institutional affiliations and organizational roles are summarized in the visual data (see Figures 2 and 3). Two important points must be noted for interpreting the reported roles. First, the exercise was conducted in a tabletop format and did not involve live simulations of cyberattacks or technical drills within Network or Security Operations Centers (NOCs/SOCs). Instead, the participants targeted were from management-level positions, emphasizing strategic rather than operational perspectives.

Second, role classifications were based on self-identification. Although the questionnaire included predefined categories (such as Organizational Management, Public Relations, Cybersecurity, and Legal), most participants selected the 'Other' category. They provided their descriptors, such as Risk Management, Crisis Management, Security, and Information Security. These variations highlight the fluidity in role perceptions and should be taken into account when analyzing the data. For instance, those identifying as Security or Information Security did not categorize themselves under Cybersecurity, raising questions about the overlap and boundaries among these labels. It is apparent, however, that the predominant group comprises individuals engaged in risk management, aligned with definitions relevant to the financial sector context previously discussed.

To analyze the collected feedback, the responses were divided among the research team. Each team member subjectively categorized answer frequencies into three strata: frequently mentioned, occasionally mentioned or infrequently mentioned. Additionally, some unique insights, though mentioned by only one or two participants, were preserved for their potential value in informing EOC development. Consensus was achieved through collaborative discussion. The research team held several meetings to review and harmonize their interpretations, ensuring that the final documented outcomes reflect a balanced and agreed-upon understanding of the participants' inputs.

Interviews

During the one-day strategic simulation, sector-specific coordination sessions were held twice, once at the beginning and again at the end of the exercise. These sessions were organized by institutional groupings relevant to the financial sector of Bangladesh. Five distinct forums were established: (i) for representatives from commercial banks, (ii) for stakeholders from microfinance institutions, (iii) for senior officials from the insurance sector, (iv) for representatives from capital market entities, and (v) for key actors from financial regulatory bodies and infrastructure operators. The heads of each of these five forums were interviewed (N = 5) to gain deeper insights into the challenges associated with building a shared Common Operational Picture (COP) and achieving Collective Situational Awareness (CSA) during the simulation. These interviews served as the primary source of data for understanding how cyber threats are currently perceived within different branches of the financial system.

Each interview was scheduled to last between one and one and a half hours and was conducted by two members of the research team in a semi-structured format. Interviews were conducted on-site at the respondents' offices. One researcher led the questioning, while the other primarily documented responses; however, both roles were shared to ensure thorough coverage. Following each session, interview notes were sent to the respective interviewees for validation and correction, ensuring the accuracy of recorded information. The interviews were conducted in the weeks immediately following the exercise, beginning the day after and concluding within a few weeks. The final session was held in early January. All questions from the exercise's original questionnaire were also presented during the interviews, offering an opportunity to enrich and clarify the broader data collection with more nuanced perspectives where needed.

RESULTS AND DISCUSSIONS

This section presents findings derived from both surveys and interviews conducted with stakeholders in the financial sector. The analysis is structured to address two research questions: (1) What information elements are critical for an effective–Common Operational Picture (COP) or Cyber Situational Awareness (CSA)? and (2) How is cyber threat perception and response framed in the financial sector?

Essential Information Elements in a Cyber COP (N = 42)

Most respondents (31 of 42) emphasized the importance of including reliable, verified information sourced from trusted channels. While rumors and unverified data were considered valid, there was a strong consensus on the need to differentiate them clearly. Many respondents (15 of 42) also emphasized the importance of incorporating current sub-goals and strategies related to crisis management, which are aligned with broader strategic objectives and the organizational ethos. A significant portion (10 of 42) emphasized the value of having a communications plan that details internal versus external information-sharing guidelines. Additionally, many participants called for documenting both past and planned actions, identifying stakeholders, and tracking collaborations. One respondent advocated for integrating triggers and indicators to assess evolving threats preemptively. Many expressed interests in predictive analyses, including normal and worst-case scenario forecasts. Interview feedback echoed these themes and emphasized the need for forward-looking perspectives and prompt management of rumors.

Target Audiences for a Cyber COP (N = 42)

The most frequently identified recipients were crisis management teams (29 of 42), including both central and regional units in larger organizations. Senior management, particularly CEOs and second-in-command executives, were also commonly cited (28 of 42), alongside incident and risk management teams, public relations officers, and various department heads. Some respondents proposed sharing the COP with all internal stakeholders and even external decision-makers. Interviewees added that contact information and predefined crisis-transition thresholds are crucial.

Decision-Making Supported by a Cyber COP (N = 40)

Most respondents (23 of 40) cited communications and public relations decisions as key outcomes. Many emphasized the importance of strategic alignment and prioritization of action, particularly under resource constraints. Some respondents highlighted operational choices such as workforce reallocation, trading suspensions, and IT infrastructure management. One respondent recommended proactively planning for post-crisis recovery. Interviews highlighted the value of principles-based decision-making and the central role of IT services in this context.

Information Contributions to External COPs (N = 41)

Respondents identified several types of valuable contributions: confirmed facts, situational assessments, internal resource status, actions taken, financial expertise, and forecasts. These inputs essentially correspond to the early phases of the established COP framework. Some respondents also emphasized the importance of strategic decision-sharing and coordination practices. Interviewees reinforced that the method and intent of communication are as critical as the data itself.

External Beneficiaries of Shared COP Information (N = 42)

Two main categories of beneficiaries were identified: financial sector stakeholders and governmental authorities. Nearly all respondents (40 of 42) mentioned financial institutions such as regulatory bodies and

industry associations. Many (32 of 42) also referenced civil authorities, such as the police and government ministries. Interviewees added that payment system actors and media should also be included.

Required External Information for Internal COPs (N = 42)

Respondents sought similar categories of information from others as they offered themselves: confirmed facts, situational awareness, system/resource statuses, actions taken, and strategic decisions. A notable distinction was a stronger demand for external factual data and less emphasis on acquiring domain expertise. Interviewees supported the necessity of factual insights and situational updates.

Key Information Providers (N = 41)

Government agencies, industry associations, and central financial entities were primary sources. The Swedish Civil Contingencies Agency, the Security Service, and the financial supervisory authority were frequently mentioned. Some responses also pointed to service providers and specific banks. Many acknowledged that information needs vary with situational context. Interviewees confirmed the necessity of involving different actors depending on the nature of the crisis.

Systematic COP Practices (N = 38)

Out of 38 respondents, 29 confirmed that they had systematic practices, while nine did not. Some stated they lacked clarity on what constitutes a systematic COP approach.

Implementation Methods (N = 29)

COP implementation strategies included technical tools (monitoring systems, penetration tests), organizational structures (security departments, cross-functional teams), external collaboration (forums such as FIDI-FINANS and NFCERT), and procedural frameworks (the quadrant model, incident management protocols). Interviews provided more profound insight into organizational roles and inter-sector collaboration.

Tracking Cyber Threats (N = 41)

Approaches included internal teams (security and risk departments), partnerships with IT vendors and consultants, participation in external forums, and collaboration with authorities. Repeated references to answers from Section 5.1.9 suggest overlap in practices for COP maintenance and threat tracking. Interviews confirmed the diversity of mechanisms and highlighted the sector's dependency on continuous information exchange and dedicated personnel.

Perceived Cyber-Threats Interview Results

During in-depth interviews with cybersecurity professionals and executives within financial institutions in Bangladesh, participants consistently identified cyber threats as a primary concern. Their responses reflect a shift from general awareness to a more acute recognition of specific vulnerabilities that could impact the trust, continuity, and stability of the financial ecosystem.

Two primary types of cyber threats were emphasized

1. Continuity Disruptions – These include incidents such as denial-of-service (DoS) attacks, ransomware infections, and disruptions to core banking services, which could result in prolonged service outages or transactional rollbacks.

2. Data Breaches and Information Leaks – These are viewed as highly damaging, not only due to the financial implications but also because they could significantly undermine public confidence in the digital banking environment.

Interviewees also noted a dual-layered exposure to cyber risk. On the one hand, financial institutions must protect their IT infrastructure; on the other, they increasingly assume responsibility for managing or insuring against cyber threats on behalf of their customers, particularly in institutions exploring cyber insurance or managed services.

When asked about the most serious cyber threats, responses varied

• Infrastructure Attacks: Some highlighted threats to the country's financial infrastructure—particularly real-time gross settlement systems, national payment switches, and mobile banking platforms—as potentially catastrophic.

• Social Engineering: Several respondents highlighted social engineering as a significant threat. Phishing, fake banking apps, and vishing scams are on the rise, preying on customer trust and the sector's rapid shift to self-service banking.

• Insider Threats: There was widespread concern about employees misusing access, whether intentionally or unintentionally, particularly in back-office operations or during remote work arrangements. This was often cited as an underestimated risk.

The role of human error was consistently identified as a root vulnerability. With the widespread adoption of mobile and internet banking in Bangladesh, many consumers are vulnerable to scams, as weak digital literacy compounds the risk. Some stakeholders stressed that "the weakest link in cybersecurity is no longer the firewall, but the finger that clicks 'allow.'"

When discussing threat actors, respondents grouped them into four main categories

1. Financially Motivated Criminals: These actors use malware, fraudulent websites, and data scraping tools to steal directly from consumers or institutions.

2. Hacktivists and Ideologically Driven Actors: Though perceived as having limited capability in the region, their potential to disrupt or deface financial websites was acknowledged.

3. Insiders: Internal staff with elevated privileges or access to sensitive data were flagged as a critical risk, with

background screening, behavior monitoring, and activity logs suggested as countermeasures.

4. State and State-Sponsored Actors: While no specific examples were cited, several participants recognized these actors as a latent strategic threat, underscoring the importance of collaboration with national intelligence and defense agencies.

There was also widespread agreement that cyber threat intelligence sharing remains underdeveloped in Bangladesh. Financial institutions operate in silos, and industry-wide collaboration is minimal. This lack of coordinated situational awareness and mutual defense hinders proactive response and rapid adaptation to emerging threats.

The consequences of cyber incidents both intentional and accidental were described as potentially severe and cascading. Respondents stressed that disruptions to digital payment systems could cripple consumer confidence and daily commerce, particularly in an economy where digital transactions are rapidly replacing cash. One participant noted that, if forced to triage during a cyber crisis, institutions would prioritize keeping mobile payment systems online over mortgage processing systems due to societal impact.

Several participants expressed concern about regulatory deadlines for digital transformations being too aggressive, often leading to rushed IT projects. Such hurried deployments were perceived as inadvertently introducing security flaws, bugs, and configuration errors, thereby opening doors for exploitation.

Ultimately, the interview results paint a picture of a financial sector that is aware of its exposure but still developing the tools, coordination, and culture needed for a proactive response. The traditional view of cybersecurity as a reactive IT function is slowly evolving into a strategic, risk-informed discipline—but gaps remain in real-time monitoring, threat actor attribution, and cross-sector coordination. These insights directly inform the design priorities for a Next-Generation Cyber Threat Response EOC tailored to the needs and challenges of Bangladesh's financial sector.

Discussion

This section first revisits our methodological approach and discusses the findings in light of existing theoretical insights relevant to cyber risk management in the financial sector. We then outline the potential limitations of the study, as well as considerations around validity and reliability. Our study aims to deepen understanding of cyber risk management practices in Bangladesh's financial institutions, focusing particularly on the types of information required to build an effective common operational picture (COP) and perceptions of cyber threats. The data was gathered through surveys and interviews with key stakeholders across the financial sector, conducted alongside a multi-stakeholder cyber crisis simulation exercise (Mallik & Rahman, 2024).

Although digital transformation is widely recognized across the sector, the true gravity of cyber risks has only recently gained full appreciation. Interview responses revealed a strong demand for information that aligns with fundamental situational awareness needs such as current system status, impact assessment, and plausible future scenarios while awareness around adversary behavior and the root causes behind incidents remains limited. This suggests that while technical monitoring and penetration testing are actively employed, a more comprehensive, strategic understanding of cyber threats remains underdeveloped. Respondents frequently rely on external information-sharing forums or trusted individuals for threat intelligence rather than systematic internal analysis of their technical data. This gap highlights a significant challenge: the lack of processes to translate raw system events into actionable, higher-level insights that can inform risk management and decision-making in real time (Mallik, 2024).

A key finding is the widespread recognition of the critical role that trust plays in the financial system. Maintaining public confidence during a cyber crisis is considered vital, with many interviewees emphasizing the importance of managing communications carefully and ensuring that accurate and truthful information reaches both internal and external audiences. Trust in the financial system, often fragile and complex, can erode quickly when cyber incidents become publicly known, posing systemic risks that extend beyond technical damage (Mallik *et al.*, 2025). Interestingly, few participants focused on the motives or tactics of adversaries or questioned how specific situations arose. This may reflect the general crisis management mindset within financial institutions, which often centers on isolated or natural incidents rather than sustained, intelligent cyberattacks. However, understanding adversary strategy is crucial to anticipating threat evolution and making informed, strategic decisions. Our findings also reveal a desire to improve information sharing among stakeholders and with the media, recognizing that transparent and coordinated communication is key to preserving system-wide trust during cyber incidents. Yet, the absence of robust collaborative mechanisms remains a challenge that a Next-Generation Cyber Threat Response EOC must address. Regarding threat perceptions, many of the significant cyber risks identified globally including credential theft, data breaches, and disruptive malware—were also recognized by respondents in Bangladesh's financial sector. However, emerging concerns, such as the exploitation of novel technologies or disinformation campaigns, were not prominently mentioned, potentially reflecting differing threat landscapes or varying awareness levels among stakeholders (Mallik & Rahman, 2024).

Notably, cyber risk management responsibilities are often distributed: individual institutions tend to handle real-time intrusion detection, while intelligence gathering about threat actors is generally delegated to external agencies such as law enforcement. This division of labor underscores the need for an integrated EOC that can coordinate across institutions and agencies, enabling a

proactive and unified cyber defense posture. In summary, this study reveals a financial sector that is transitioning from reactive responses to a more proactive approach to cyber risk management. However, gaps remain in strategic situational awareness, adversary intelligence, and collaborative information sharing. Addressing these gaps through the design of a dedicated, next-generation Cyber Threat Response EOC will be vital to strengthening Bangladesh's financial sector resilience against evolving cyber threats.

CONCLUSIONS

This section summarizes conclusions related to the study's two primary research questions and offers recommendations for enhancing cybersecurity and risk management within Bangladesh's financial sector. The first research question focused on identifying the critical information elements needed to establish an effective Common Operational Picture (COP) for cyber situational awareness within financial institutions.

Analysis of stakeholder inputs revealed that information demands broadly align with key situational awareness requirements, such as understanding the impact of cyber incidents, monitoring how situations evolve, assessing plausible future developments, and ensuring the reliability and quality of underlying data.

However, several essential observations stand out

• There was limited interest in detailed information about adversary behaviors or the causal links between events and outcomes. This gap hinders the ability to develop a deeper understanding of the cyber threat landscape, which is essential for anticipating future threats posed by strategic adversaries.

• A strong emphasis on technical details was evident, even among senior management. While technical data is vital at the operational level, leadership should also focus on higher-level questions, such as who the adversaries are, what their objectives might be, and why and how incidents occur. This shift is critical for strategic decision-making.

• Information management emerged as a priority, with respondents highlighting the need for systematic approaches to handling, prioritizing, and communicating information. Given the financial sector's heavy reliance on public trust, carefully structured communication strategies are essential to maintaining confidence during cyber incidents.

The second research question examined how cyber threats are perceived by financial sector actors in Bangladesh. There is a broad consensus that cyber threats constitute a significant concern in risk management. The primary assets at risk include the availability of critical IT services and the confidentiality of sensitive information, both of which have direct implications for public trust in individual institutions and the sector as a whole. The perception of cyber threats varies across subsectors. For example, insurers face a dual layer of risk: safeguarding their IT infrastructure and managing the cyber risks they underwrite on behalf of their clients. Among the most serious threats identified are attacks targeting financial infrastructure, with social engineering techniques where attackers manipulate individuals to gain unauthorized access seen as the most dangerous vector. The erosion of public trust resulting from successful attacks is widely regarded as the most severe consequence. Common threats such as theft and fraud, often facilitated by social engineering, were frequently noted. Insider threats, originating from trusted individuals abusing their legitimate access, were also considered significant. The threat actors are generally viewed as financially motivated criminals, although politically or ideologically driven activists are also recognized as potential risks.

REFERENCE

Alsamhi, S. H., Kumar, S., Hawbani, A., Shvetsov, A. V., Zhao, L., & Guizani, M. (2024). Synergy of human-centered ai and cyber-physical-social systems for enhanced cognitive situation awareness: applications, challenges and opportunities. *Cognitive Computation, 16*(5), 2735-2755.

Arora, A. (2025). *The Future of Cybersecurity: Trends and Innovations Shaping Tomorrow's Threat Landscape*. SSRN 5268161.

Auqui-Caceres, M. V., & Furlan, A. (2023). Revitalizing double-loop learning in organizational contexts: A systematic review and research agenda. *European Management Review, 20*(4), 741-761.

Bardin, J. S. (2025). Cyber Warfare. In *Computer and Information Security Handbook* (pp. 1345-1380). Morgan Kaufmann.

Carraro, M., Furlan, A., & Netland, T. (2025). Unlocking team performance: How shared mental models drive proactive problem-solving. *human relations, 78*(4), 407-437.

Cespedes-Cubides, A. S., & Jradi, M. (2024). A review of building digital twins to improve energy efficiency in the building operational stage. *Energy Informatics, 7*(1), 11.

George, A. S. (2024). Finance 4.0: The Transformation of Financial Services in the Digital Age. *Partners Universal Innovative Research Publication, 2*(3), 104-125.

George, A. S., Baskar, T., & Srikaanth, P. B. (2024). Cyber threats to critical infrastructure: assessing vulnerabilities across key sectors. *Partners Universal International Innovation Journal, 2*(1), 51-75.

Hawash, B., Mokhtar, U. A., Jeong, J. J., Maynard, S. B., Shukur, Z., Abdullah, S. N. H. S., ... & Ahmad, A. (2024). Cyber Situational Awareness in Security Operation Centres.

Jiang, P., Rowsell, J., & Schmidt, S. (2025). Crisis-ready telecom: Global approaches to emergency management in telecommunications. *Telecommunications Policy, 49*(4), 102914.

Mallik, S. K. (2024). Analyzing Banking Sector Risk and Capital Allocation: A Study on the Improvement of Risk-Weighted Assets and CRAR Compliance in

2023.

Mallik, S. K., & Rahman, M. A. (2024). An analysis of business students learning styles to improve the effectiveness of teaching methods.

Mallik, S. K., & Rahman, M. A. (2024). Smart agriculture as a driving technology for sustainability in intensive greenhouse production within smart manufacturing systems.

Mallik, S. K., Ali, M. R., Nahiduzzaman, D. M., Shoumik, S. C., & Torikul, M. (2025). Sustainable textile industry: Balancing growth and environmental concerns in Bangladesh.

Naseer, H., Desouza, K., Maynard, S. B., & Ahmad, A. (2024). Enabling cybersecurity incident response agility through dynamic capabilities: the role of real-time analytics. *European Journal of Information Systems, 33*(2), 200-220.

Nazir, A., Hussain, A., Singh, M., & Assad, A. (2025). A novel approach in cancer diagnosis: integrating holography microscopic medical imaging and deep learning techniques—challenges and future trends. *Biomedical Physics & Engineering Express, 11*(2), 022002.

Negi, P., Pathani, A., Bhatt, B. C., Swami, S., Singh, R., Gehlot, A., ... & Sikarwar, V. S. (2024). Integration of Industry 4.0 Technologies in Fire and Safety Management. *Fire, 7*(10), 335.

Samunderu, E. (2024). Challenges and Complexities Affecting African Air Transport Market Development: A Skills, Competency, and Capacity-Building Perspective. In *The Economic Effects of Air Transport Market Liberalisation: A Perspective Analysis of the Single African Air Transport Market (SAATM)* (pp. 499-639). Cham: Springer Nature Switzerland.

Smidt, H., Johansson, J., & Richter, T. (2024). Civil society under attack: The consequences for horizontal accountability institutions. *Studies in Comparative International Development,* 1-30.

Vasiliu-Feltes, I. (2024). Safeguarding financial resilience through digital trust and responsible innovation. *Journal of Risk Management in Financial Institutions, 17*(2), 130-141.

Vasiliu-Feltes, I. (2024). Safeguarding financial resilience through digital trust and responsible innovation. *Journal of Risk Management in Financial Institutions, 17*(2), 130-141.

Yu, Z., Wang, J., Tang, B., & Lu, L. (2023). Tactics and techniques classification in cyber threat intelligence. *The Computer Journal, 66*(8), 1870-1881.