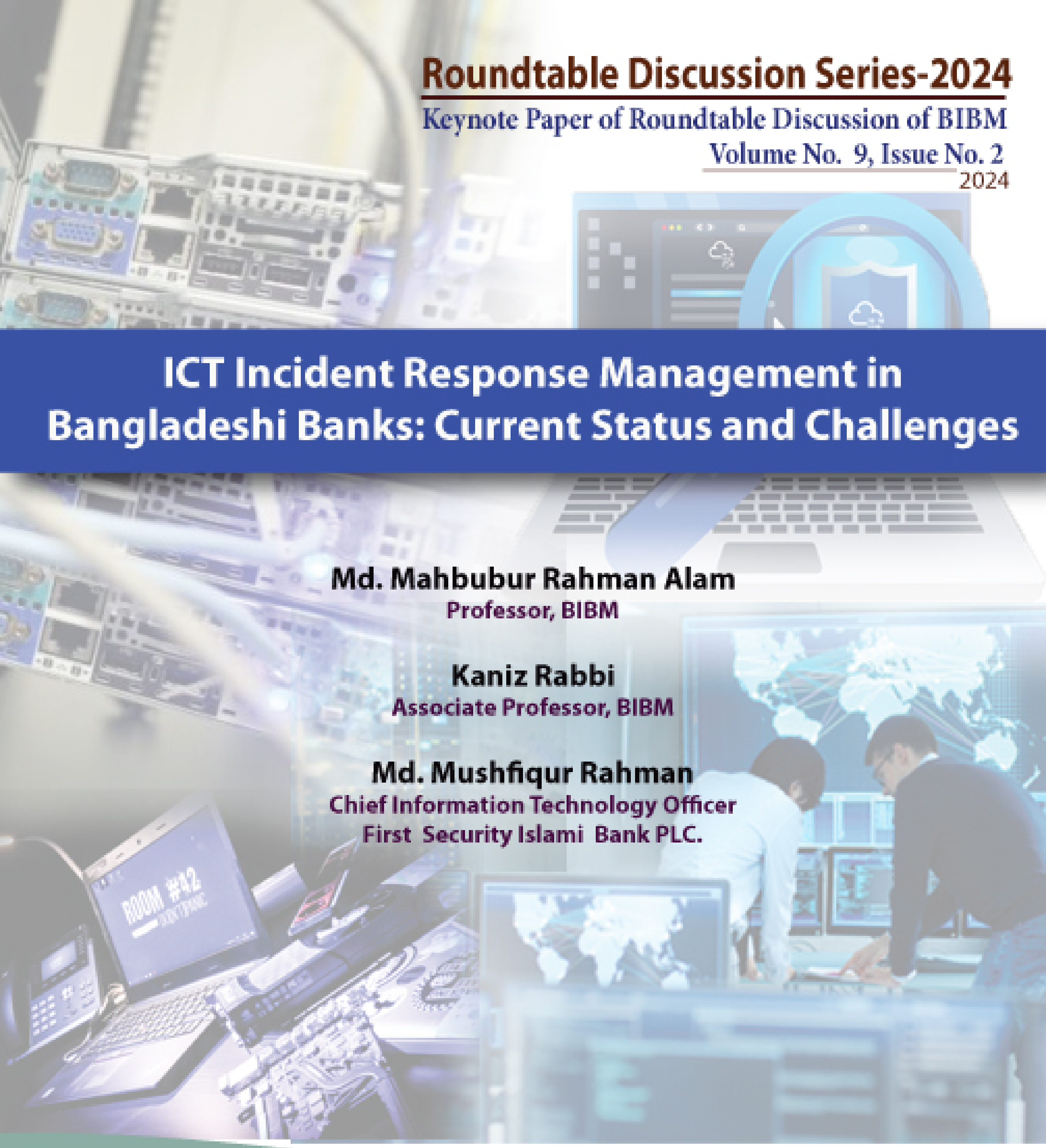


Roundtable Discussion Series-2024

Keynote Paper of Roundtable Discussion of BIBM

Volume No. 9, Issue No. 2

2024

ICT Incident Response Management in Bangladeshi Banks: Current Status and Challenges

Md. Mahbubur Rahman Alam
Professor, BIBM

Kaniz Rabbi
Associate Professor, BIBM

Md. Mushfiqur Rahman
Chief Information Technology Officer
First Security Islami Bank PLC.

Bangladesh Institute of Bank Management (BIBM)
Section No. 2, Mirpur, Dhaka-1216

Roundtable Discussion Series-2024

Keynote Paper of Roundtable Discussion of BIBM
Volume No. 9, Issue No. 2

ICT Incident Response Management in Bangladeshi Banks: Current Status and Challenges

Md. Mahbubur Rahman Alam
Professor, BIBM

Kaniz Rabbi
Associate Professor, BIBM

Md. Mushfiqur Rahman
Chief Information Technology Officer
First Security Islami Bank PLC.

Bangladesh Institute of Bank Management (BIBM)
Mirpur-2, Dhaka-1216, Bangladesh

ICT Incident Response Management in Bangladeshi Banks: Current Status and Challenges

Research Team	**Md. Mahbubur Rahman Alam** *Professor, BIBM* **Kaniz Rabbi** *Associate Professor, BIBM* **Md. Mushfiqur Rahman** *Chief Information Technology Officer* *First Security Islami Bank PLC.*
Editorial Advisor	**Md. Akhtaruzzaman, *PhD*.** *Director General, BIBM*
Editor	**Md. Shihab Uddin Khan** *Professor and Director (Research, Development & Consultancy), BIBM*
Support Team	***Research, Development and Consultancy Wing*** **Papon Tabassum,** *Assistant Senior Officer, BIBM* **Sk. Md. Azizur Rahman,** *Officer, BIBM* **Md. Awalad Hossain,** *Officer, BIBM* ***Publications-cum-Public Relations Section*** **Md. Al-Mamun Khan,** *Senior Officer, BIBM* **Md. Morshadur Rahman,** *Officer, BIBM*
Design & Illustration	**Md. Awalad Hossain,** *Officer, BIBM*
Published in	March, 2025

Published by Bangladesh Institute of Bank Management (BIBM)
Plot No. 4, Main Road No. 1 (South), Section No. 2
Mirpur, Dhaka-1216, Bangladesh.

PABX	:	48032091-4, 48032097-8, 48032104
E-mail	:	bibmresearch@bibm.org.bd
Web	:	www.bibm.org.bd

Copyright © BIBM 2025, All Rights Reserved

Printed by..

The views in this publication are of authors only and do not necessarily reflect the views of the institutions involved in this publication.

Foreword

It is with great pleasure that I present the findings of the keynote paper from the roundtable discussion held on 12 October, 2023 at BIBM, titled *"ICT Incident Response Management in Bangladeshi Banks: Current Status and Challenges."* As banks continue to adopt digital technologies, ICT incident response management has become a critical aspect of their operations. Efficient handling of ICT incidents not only improves service quality but also plays a pivotal role in ensuring client satisfaction. This study aims to shed light on the current state of ICT Incident Response Management, examining how banks in Bangladesh are addressing its challenges.

The paper addresses three key objectives: first, to assess the current state of ICT incident response in Bangladeshi banks; second, to identify the challenges and vulnerabilities of ICT incident response practices; and third, to recommend improvements and best practices for ICT incident response management in Bangladeshi banks. These findings are especially timely as customer expectations continue to evolve in the digital age, requiring banks to keep pace with technological advancements to remain competitive.

In offering this resource, we aim to provide valuable insights to banking professionals, financial institutions, regulators, academics, and general readers alike. This study serves as a practical guide for improving ICT incident response management systems, with a view to enhancing customer satisfaction and operational efficiency.

On behalf of BIBM, I trust that this paper will serve as an important tool for the banking community as it navigates the challenges posed by evolving digital technologies. We warmly welcome feedback from our esteemed readers, as your insights will contribute significantly to the refinement of our future research endeavors.

Md. Akhtaruzzaman, Ph.D.
Director General, BIBM

Acknowledgement

We have completed the research project with extensive support from many people. We would like to extend our gratitude to Dr. Md. Akhtaruzzaman, honorable Director General of BIBM for his valuable guidance and suggestions to complete the study comprehensively.

We would like to thank the respondents of our questionnaires and the learned discussants, who provided their valuable inputs for the successful finalization of the report. We are truly grateful to Mr. Md. Shihab Uddin Khan, Professor & Director (Research, Development & Consultancy), BIBM, for his opinion and observations about the paper. We are deeply thankful to all our faculty colleagues for their constructive feedback and positive suggestions, which helped us shape the research. Our appreciation extends to the bankers who took the time and effort to complete the research, providing us with vital insights.

Our honest indebtedness goes to research assistants, who have facilitated us to get very much useful information from different stakeholders across the country. Our sincere appreciation goes to Ms. Papon Tabassum, Assistant Senior Officer; Mr. Sk. Md. Azizur Rahman, Officer and Mr. Md. Awalad Hossain, Officer of BIBM for their support.

Finally, we extend our deepest thanks to everyone who, directly or indirectly, contributed to the success of this research. Your cooperation and encouragement have been greatly appreciated.

Md. Mahbubur Rahman Alam
Kaniz Rabbi
Md. Mushfiqur Rahman

Contents

Page No.

Foreword iii

Acknowledgement iv

List of Abbreviations ix

Executive Summary x

1.1 Background of the Study 1

1.2 Objectives of the Study 2

1.3 Methodology 3

1.4 Limitations 3

2. Literature Review 4

3. Data Analysis and Findings 9

3.1 Incidents Recorded in 2022 9

3.1.1 Categories of Incidents 9

3.1.2 Severity Levels of Incidents 12

3.1.3 Business Impact of Incidents 13

3.1.4 Reliance on Service Providers 14

3.2 Incident Response Capability Compliance with International/BB Standards 15

3.2.1 Incident Management Framework/Policies 15

3.2.2 Standards of the Framework/Policy 17

3.2.3 Alignment with the ICT Security Guidelines Version 4 (2023) of Bangladesh Bank 18

3.3 Computer Incident Response Team (CIRT)/ICT Emergency Response Team 20

3.3.1 Formation and Management of the CIRT 20

3.3.2 Roles and Responsibilities of the Incident Response Team 21

3.3.3 Basic Steps followed by the Incident Response Team 21

3.3.4 Reporting to the Bangladesh Bank Computer Incident Response Team 22

3.3.5 Subject Matter Experts (SMEs) within Computer Incident Response Teams 22

3.3.6 Quality of CIRT Members 23

3.3.7 Regular Drills or Exercises of CIRT 26

3.4. Security Operation Center (SOC) 27

3.4.1 Status of SOC 27

3.4.2 Threat Intelligence Platform 27

3.4.3 Integration with SIEM 28
3.4.4 24×7 Monitoring Security Logs 28
3.5 Preparation for Handling an Incident 29
3.5.1 Classifying Incidents 29
3.5.2 Standardized Process for Reporting Incidents Internally 29
3.5.3 Standardized Process for Reporting Incidents Externally 29
3.5.4 Decision Regarding Crises and Timely Activation of the Disaster Recovery Plan 30
3.5.5 Informing Bangladesh Bank 30
3.5.6 Escalation and Resolution Procedures 31
3.5.7 Tools to Track and Manage Incident Resolution Processes 31
3.5.8 Tracking Security Incidents 31
3.5.9 Simulated Events into Training 32
3.6 Incident Detection and Analysis 32
3.6.1 Incident Detection 32
3.6.2 Post Incident Analysis 33
3.6.3 Analyzing the Scope and Impact of ICT Incidents 34
3.6.4 Internal Incidents Reporting 34
3.6.5 External Incidents Reporting 35
3.6.6 Handling Incidents that have Potential to Escalate into Crises 35
3.6.7 Activation of a Disaster Recovery Plan 36
3.6.8 Informing Bangladesh Bank 36
3.6.9 Escalation and Resolution Procedures 37
3.6.10 Automated Mechanisms for Tracking Security Incidents 37
3.6.11 Simulation and Exercises 38
3.7 Containment, Eradication and Recovery 39
3.7.1 Containment 39
3.7.2 Eradication 39
3.7.3 Recovery Process Following a Security Incident 40
3.8 Post-Incident Activities and Digital Forensic 40
3.8.1 Post-Incident Activities 40
3.8.2 Digital Forensic 41
3.8.2.1 Awareness of the Laws And Regulation 42
3.8.2.2 Skills of the Forensic Team 42
3.9 Coordination and Communication 43
3.9.1 Coordination and Communication during Incident Response 43
3.9.2 Designated Spokespersons Responsible for Communicating 43
3.9.3 Communicating Findings and Recommendations to 44

Stakeholders
3.9.4 Communication Channels and Methods to Keep Customers Informed 45
3.9.5 Addressing Legal and Regulatory Requirements 45
3.10 Incident Documentation 46
3.10.1 Standardized Format for Documenting Incident 46
3.10.2 Software for Documenting Incident 46
3.10.3 Retention Periods for Incident Records 47
3.11 Continuous Improvement of Incident Management Process 48
3.12 Problems and Challenges Identified by Banks for Incident Management 49
3.13 Expected Roles of BIBM for Incident Management 50
3.14 Expectation from Bangladesh Bank 51
3.15 Roles of the Government 52
3.16 Recommendations 53
References 59

List of Figures

	Page No.
Figure 1: Percentage of Banks Experienced Different Types of Incidents	10
Figure 2: Incidents Classified by Component of Information System	10
Figure 3: Incidents Classified by CIA Triad	11
Figure 4: Incidents Classified by Severity Levels	12
Figure 5: Incidents Classified by Business Impact	13
Figure 6: Reliance on Service Providers	14
Figure 7: Quality of Incident Management Framework/Policies	15
Figure 8: Updating Incident Management Framework/Policies	16
Figure 9: Standards Followed to Develop Framework/Policies	18
Figure 10: Alignment with the ICT Security Guidelines of BB	19
Figure 11: Responsibility for Forming and Managing the CIRT	20
Figure 12: Analysis of Experience and Expertise of CIRT Members	26
Figure 13: Threat Intelligence Sources	27
Figure 14: Incident Detection Methods	33

List of Tables

	Page No.
Table 1: Background of CIRT Members	23
Table 2: Educational Background of CIRT Members	24
Table 3: Experience and Expertise of CIRT Members	25
Table 4: Problems and Challenges Identified by Banks	49
Table 5: Expected Roles of BIBM	51
Table 6: Expectation from Bangladesh Bank	52
Table 7: Expectation from Bangladesh Government	53

List of Abbreviations

ADC	Alternative Delivery Channel
ADs	Authorized Dealers
BB	Bangladesh Bank
BC	Business Continuity
BCP	Business Continuity Plan
BIBM	Bangladesh Institute of Bank Management
CBS	Core Banking System
CEO	Chief Executive Officer
CFE	Certified Fraud Examiner
CHFI	Computer Hacking Forensic Investigator
CIA	Confidentiality, Integrity, Availability
CIO	Chief Information Officer
CIRT	Computer Incident Response Team
CISO	Chief Information Security Officer
CITO	Chief Information Technology Officer
CRO	Chief Risk Officer
CTE	Certified Penetration Testing Engineer
DC	Data Center
DR	Disaster Recovery
FIs	Financial Institutions
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
IS	Information Systems
ISO	International Organization for Standardization
ISRM	Information Security and Risk Management
ITIL	Information Technology Infrastructure Library
MBA	Master of Business Administration
MD	Managing Director
NIST SP	National Institute of Standards and Technology Special Publication
PCIDSS	Payment Card Industry Data Security Standard
SLA	Service Level Agreement
SOC	Security Operations Center
TIP	Threat Intelligence Platform

Executive Summary

The keynote paper titled *"ICT Incident Response Management in Bangladeshi Banks: Current Status and Challenges"* provides an in-depth analysis of incident response practices within Bangladeshi banks. Drawing on data from 32 banks, including public, private, and foreign institutions, as well as discussions with security experts, the study highlights the current state of ICT incident management, identifies critical challenges, and offers recommendations to strengthen the sector's resilience in the face of ever-evolving cybersecurity threats.

While progress has been made in certain areas, such as the establishment of Security Operations Centers (SOCs) in 44% of surveyed banks and the proactive analysis of incident trends by 58% of banks, inconsistencies in preparedness, policy implementation, and resource allocation continue to hinder effective incident response.

Despite regulatory efforts, a lack of cybersecurity awareness persists across all organizational levels, from employees to board members. This gap impairs the ability of banks to respond effectively to incidents and highlights the need to cultivate a robust cybersecurity culture across the organization. At the same time, the rapid evolution of cyber threats demands that banks remain agile and invest in advanced technologies and regular training for their workforce. However, limited resources and insufficient upskilling programs leave many institutions ill-equipped to adapt to the growing complexity of cyberattacks.

The study also found that incident response policies are not updated frequently enough, with 28% of banks revising their policies only every three years and some failing to update them at all. While 58% of banks rated their policies as "Good," the fact that 16% deemed them "Poor" underscores the need for regular evaluation and refinement to ensure resilience. Compounding this issue is the severe shortage of skilled ICT professionals, which makes it difficult for banks to effectively manage incidents. To address this, banks must invest in training, foster partnerships with educational institutions, offer competitive compensation, and provide clear career paths to attract and retain top talent.

Incident reporting and communication also remain areas requiring improvement. While banks are required to report significant incidents to regulators like Bangladesh Bank, transparency in communicating breaches to customers and the public is lacking, which can erode trust. Collaboration among banks, regulators, and industry stakeholders is similarly underdeveloped, limiting the effectiveness of collective defenses against cyber threats. Although some banks participate in industry forums to share threat intelligence, more robust information-sharing mechanisms are needed to enhance sector-wide preparedness.

Another notable finding is that only 33% of banks conduct regular drills to test their ICT Emergency Response Teams, which are essential for maintaining readiness in the face of real-world crises. Compliance with Bangladesh Bank's ICT Security Guidelines Version 4 (2023) also poses challenges, with only 16% of banks reporting full alignment. Many institutions face hurdles such as time constraints, lack of strategic alignment, and insufficient awareness among senior management. Additionally, while most banks manage their incident response teams internally, reliance on external vendors remains prevalent, requiring a careful balance between internal expertise and external support.

The study highlights other critical gaps, such as the lack of digital forensic capabilities, with only 20% of banks maintaining dedicated forensic teams to investigate and resolve incidents. Moreover, only 27% of banks use software for incident documentation, relying instead on manual methods, which limits efficiency and security. Retention periods for incident records also vary significantly, with some banks adopting long-term retention strategies while others archive records after as little as one year.

To address these challenges, the study recommends fostering a cybersecurity-aware culture across all organizational levels and ensuring continuous investment in advanced technologies and workforce training. Regular updates and rigorous evaluation of incident response policies are critical for maintaining resilience. Banks must also bridge the talent gap by offering attractive career opportunities and collaborating with academic institutions to develop specialized training programs. Improving transparency in incident reporting and enhancing collaboration among stakeholders are equally essential for building trust and strengthening collective defenses. Conducting frequent drills, expanding digital forensic capabilities, and adopting specialized incident management software can further improve preparedness. Finally, aligning more closely with regulatory guidelines and establishing well-resourced SOCs are necessary steps to bolster cybersecurity infrastructure.

The findings from the paper emphasize the urgent need for Bangladeshi banks to prioritize ICT incident response management as a cornerstone of their cybersecurity strategy. By addressing existing gaps and adopting a proactive, collaborative approach, banks can enhance their ability to respond to incidents effectively and safeguard their operations against the growing complexity of cyber threats. Continuous improvement, combined with strong partnerships and a commitment to innovation, will be pivotal in ensuring the security and resilience of the banking sector.

ICT Incident Response Management in Bangladeshi Banks: Current Status and Challenges

1.1 Background of the Study

In recent years, the banking sector in Bangladesh has witnessed significant growth and modernization, largely driven by advancements in Information and Communication Technology (ICT). The adoption of digital banking services, online transactions, and the integration of ICT systems have not only facilitated financial inclusion but have also exposed the banking industry to various cybersecurity threats and incidents. As a result, the need for robust ICT incident response management has become paramount to safeguard the financial stability and security of the nation.

ICT incident means any occurrence compromising the availability, legitimacy, integrity or confidentiality of stored, communicated or processed data or of the related services offered by, or available through network and information systems. According to ISO 27000, security incident is: “a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.” And ISO 27001 defines a security incident as an unwanted event that could endanger the confidentiality, integrity, or availability of information, whereas an event is any kind of technical occurrence or an activity that could indicate a possible breach of data. Examples of ICT incidents include- computer system interruption, unauthorized or inappropriate revelation of sensitive data, suspected or actual breaches, compromises, or other unlawful access to computer systems, data, applications, or accounts, illegal changes to computers or software, damage or theft of computer equipment or other data storage devices and media (e.g., laptop, USB drive) used to store private/sensitive information, denial of service attack or any other attack that prevents or weakens the authorized use of networks, systems, or applications, interfering with the planned use or inappropriate or improper usage of information technology resources, etc. Why is incident management important? As information system is crucial for the survival of any organization in today’s world, we need a comprehensive incident response policy to recognize real security incidents, get the situation under control, lower the damage caused by an invader, and lessen the time and costs of recovery. Incident management’s significance cannot be exaggerated as it is the bedrock of a vigorous set-up. By promptly recognising and resolving incidents, incident management minimizes the effect on critical systems, data and an organization’s reputation.

ICT incidents in Bangladeshi banks not only have a direct impact on the affected banks but also pose systemic risks to the broader financial ecosystem of Bangladesh. They can result in financial losses, reputational damage, and erosion of customer trust, potentially leading to a loss of confidence in the country's financial institutions. The existing literature on ICT incident response management predominantly focuses on developed economies, and there is a notable scarcity of research concerning the specific challenges and current status of incident response practices in Bangladeshi banks. This study aims to bridge this gap by conducting a comprehensive assessment of the ICT incident response management framework within Bangladeshi banks, identifying the challenges they face, and proposing strategies to enhance their cybersecurity resilience.

1.2 Objectives of the Study

The paper aims to examine the state of ICT Incident Response Management in Bangladeshi banks. The specific objectives of the study are: one, to assess the current state of ICT incident response in Bangladeshi banks; two, to identify challenges and vulnerabilities of ICT incident response practice; and three, to recommend improvements and best practices of ICT incident response management in Bangladeshi banks.

1.3 Methodology

This study employs a mixed-method approach, gathering primary data primarily from the IT departments of banks via semi-structured questionnaires. Out of 61 questionnaires distributed among the banking sector, responses were received from 32 banks, encompassing 3 government banks, 26 private commercial banks (including 4 Islamic banks), and 3 foreign commercial banks. Additionally, insights from 10 Heads of Security were obtained through discussions to provide a comprehensive understanding of ICT Incident Response Management in Bangladesh. The primary data is supplemented by a review of secondary sources, including publications and circulars from Bangladesh Bank (BB), annual reports of banks, previous reports of BIBM, policy guidelines, and relevant research articles. The report presents its findings primarily through tables and some graphical representations, with finalization pending input and feedback from participants and banking sector experts who participated in the roundtable discussion.

1.4 Limitations

Several limitations constrained the depth of our study. One significant obstacle was the need to maintain the confidentiality of sensitive information. Each bank holds its own proprietary data, which cannot be disclosed to external parties. Additionally, some banks were reluctant to share their security-related information due to concerns about potential cyberattacks, resulting in hesitancy in responding to our questionnaire. It's crucial to note that the data collected in this study is specific to the banking sector in Bangladesh and does not encompass other sectors of the economy. Furthermore, the dataset was derived from responses received from only 32 banks. Therefore, these limitations should be considered when making decisions or formulating policies related to ICT Incident Response Management.

2. Literature Review

Information and Communication Technology (ICT) has revolutionized the banking sector worldwide, enabling more efficient and convenient financial services. However, this digital transformation has also exposed banks to a new set of risks, including cyber threats. To safeguard their operations and customers' sensitive data, banks have implemented Incident Response Management (IRM) strategies. This literature review explores the current status and challenges of ICT Incident Response Management in banks, with a focus on recent research and developments.

Standard incident response methodologies exist for organisations to use in their response to security incidents across a wide range of impact severities (Northcutt, 1998; West-Brown et al., 2003; Grance et al., 2004; Murray, 2007). Various guidelines and standards define best practice and propose activities for operative and well-organized incident management. Some prominent guidelines in relation to information security incident management are: The ISO/IEC 27035 Standard, The ITIL Framework, NIST Special Publication 800-61, ENISA and SANS, etc.

According to NIST SP 800-82 Rev. 2, computer security incident is an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. Effective response to information security incidents is a critical function of modern organisations. For the purposes of Incident Response (IR), a cyber incident can be defined as any event that compromises information confidentiality, integrity, and/or availability—core principles of information security that are often referred to as the "CIA triad" (https://fieldeffect.com/blog/digital-forensics-incident-response).

Incident response refers to the formal, structured methods by which organisations engage teams to detect and eradicate information security incidents (West-Brown, 2003; Wiik et al., 2005). The ultimate goal is to minimise the effects of a successful attack and to ensure an expedient recovery (Van Wyk et al., 2001; Wiik et al., 2005). Successful security incidents can cost organisations severely across a variety of impact criteria, including reputation, productivity and direct financial costs attributed to lost business as well as legal and regulatory penalties.

Two of the most important parts of incident management are the existence of guidelines for communication and prioritization of incidents as well as the use of an evaluation process to gain experience from previous incidents (Paul et.al, 2011). As part of an incident management aptitude, organizations should have an incident management policy, a plan and procedures, all of which should be custom-made to the specific organization's requirements. According to ISO/IEC 27035:2011(E), it is important to have a planned approach to reporting of vulnerabilities that have not yet been exploited. Incident management is not purely an IT related issue as information security incidents threaten an organization as a whole. Having a well-planned and tailored incident management capability is therefore important for organizations in order to protect information.

A formative report by Knight and Pretty (1996) established a direct causal relationship between organisations that successfully recovered from catastrophes and their effective response to the incident. Further, although not all incidents necessarily turn into catastrophes, the ability of an organisation to effectively mitigate an incident plays a key role in preventing incidents from escalating into a catastrophe.

According to ITIL, “Classifying and categorizing IT incidents helps identify and route incidents to the right technician, saving time and effort. For example, incidents can be classified as major or minor incidents based on their impact on the business and their urgency. Typically, major incidents are the ones that affect business-critical services, thus affecting the entire organization, and need immediate resolutions. Minor incidents usually impact a single user or a department, and might have a documented resolution in place already."

There are many factors that determine effectiveness of incident response. Among these are resourcing of the incident response capability, availability and application of technical expertise, and support from senior management. As Smith and Jamieson (2006) explained, the dynamic support of top management was ranked the most important issue. While top management is ultimately responsible and charged with the task of introducing and supporting vital projects with adequate capital and resources, they can also support information security as an important enterprise-wide function in many ways, including funding, allocation of human and monetary resources, promotion of buy-in, and stressing the significance of security to other groups among the organization (Kayworth and Whitten, 2010). A study by Kurowski and Fring (2011) stated that the professional skill of staffs is most relevant for carrying out analysis of incident. Security incident response refers to the process by which organizations engage dedicated or adhoc teams to identify and treat information security incidents (West-Brown, 2003; Wiik et al., 2005). Depending on the scope of the team, they can be either technical or multidisciplinary, featuring members across a variety of business lines, balancing a range of skills that may include the technical, diplomatic and organizational (Murray, 2007). Again, according to ISO/IEC 27035 standard, employees' responsiveness and involvement in incident management procedures are important. Big organizations may have dedicated teams available 24/7 to handle major incidents. In the incident management process resources are allocated to lessen and mitigate the effect of incidents and service unavailability in line with business priorities. The main objectives are to re-establish services as swiftly as possible in addition to limit adverse effect on business operations (https://www.manageengine.com/products/service-desk/itil-incident-management/what-is-itilincident-management.html).

An important activity in the incident response process is the capacity of the process to learn from the errors or mistakes made during the incident, learn which policies and activities are effective or useless, identify concerns in staffing and skills and to feed this knowledge back into the process (Northcutt, 1998; Killcrece et al., 2003; Grance et al., 2004). While major incident response methods such as the SANS and NIST models include 'post-mortem' or 'follow-up' activities post- incident, there is slight evidence to advise that organisations enthusiastically involve in adequate organisational learning and perfection of these incident response processes (Cooke, 2003). Current incident response literature instead emphasizes on technical responses to incidents, the initial phases of the process and forensic activities (Mitropolous et al., 2006; Turner, 2007; Zhang et al., 2009). However, if banks/FIs were to correctly learn from and accomplish their incident response capability, they would be able to leverage opportunities to learn from incidents to their best advantage and understand the benefits of a strong process and fortified security policy.

Incident response teams are the 'firefighters' within organisations, devoted to the preparation, identification, analysis and recovery from security incidents (Jaikumar, 2002). On the timeline of business continuity, incident response is the instantaneous action taken against a security breach, whereas disaster recovery and business continuity are longer-term concerns (Whitman & Mattord, 2005). Incident response is therefore the thoughts and actions commenced upon the detection of security incidents and the immediate actions taken in the short-term to diminish the organisation's exposure. However, an IR team is accountable for more than just straight actions against incidents. Instead, such teams will vigorously advise on security, develop security strategy and conduct security training and awareness programs (West-Brown et al., 2003). Therefore, the value of fielding effective and capable incident response teams is that they will primarily be effective in response to security breaches. However, in broader organisational role, IR teams can deliver knowledge and data to the organisation as a whole. An IR team must have a variety of talents, including technical, organisational and diplomatic skill in dealing both with the incident, management of the team and effective at negotiating during intense and stressful situations.

The root causes of numerous incidents within Bangladeshi banks often stem from breaches in cybersecurity practices. Researchers, both domestically and internationally, have conducted extensive studies addressing this critical issue. In the study titled 'Cybersecurity in Banking Sector of Bangladesh: Challenges and Policy Measures,' Khan (2018) underscores the importance of cybersecurity in Bangladesh's banking sector and emphasizes the necessity of robust incident response strategies to combat evolving cyber threats.

In a case study titled 'Information Security Practices in Banking Sector' by Islam & Ahmed (2019), the authors delve into information security practices, including incident response, within Bangladeshi banks, offering valuable insights into the current state of security measures. Moreover, Rahman & Bhuiyan (2017) explore the transformative impact of ICT in the banking sector in their study on 'The Impact of ICT in the Banking Sector of Bangladesh.' They touch on the imperative need for effective incident response mechanisms to safeguard critical financial infrastructure. Addressing the specific cyber threats faced by Bangladesh's banking sector, Haque & Mannan (2020) in their review on 'Cyber Threats and Cybersecurity in Bangladesh' identify challenges within incident response, including skill shortages and resource limitations. Saha & Khan (2019) present an overview of cybersecurity threats and challenges in incident response capacity building and collaboration among Bangladeshi banks in their study 'Cybersecurity Threats in Banking Sector: A Comprehensive Study on Bangladesh Perspective.' Ahmed & Salim (2020) shed light on ICT security issues in the financial sector of Bangladesh in their review titled 'ICT Security Issues in the Financial Sector of Bangladesh,' underscoring the critical need for effective incident response plans and coordinated efforts among banks. Hossain & Rahman (2019) propose policy recommendations aimed at enhancing cybersecurity in Bangladeshi banks, including the development of standardized incident response procedures. 'Strengthening Cybersecurity in Bangladeshi Banking Sector: Challenges and Way Forward' by Sikder & Rahman (2018) offers a comprehensive roadmap for fortifying cybersecurity. It places a strong emphasis on proactive incident response strategies and the significance of public-private partnerships in this endeavor. These studies collectively provide valuable insights into the challenges faced by Bangladeshi banks in the realm of cybersecurity and offer practical policy recommendations for bolstering incident response capabilities.

3. Data Analysis and Findings

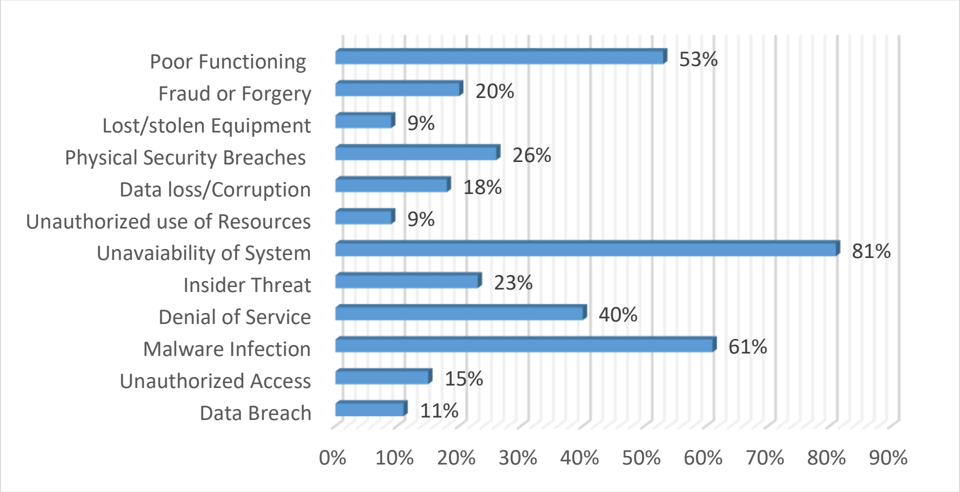
3.1 Incidents Recorded in 2022

ICT incident means any occurrence compromising the availability, legitimacy, integrity or confidentiality of stored, communicated or processed data or of the related services offered by, or available through network and information systems. A security incident is a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.

3.1.1 Categories of Incidents

In 2022, the banking sector witnessed a significant array of security incidents across various categories. Among these incidents, malware infection stood out as the most prevalent issue, accounting for a substantial 61% of the total banks (Figure-1). This indicates a pervasive threat from malicious software programs targeting banks, potentially aiming to steal sensitive data or compromise systems.

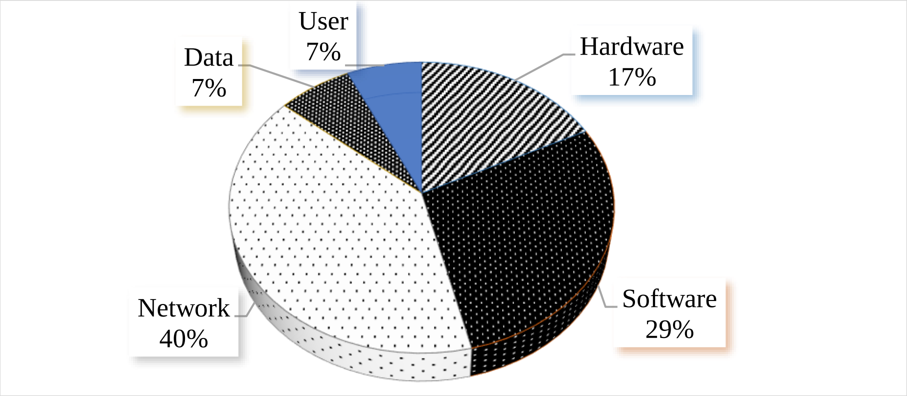
Figure 1: Percentage of Banks Experienced Different Types of Incidents



Source: BIBM Survey

Additionally, the high occurrence of unavailability of systems reported by 81% of banks suggests that disruptions in banking services and operations were a prevalent concern, impacting customer access and transactions. Unauthorized access, insider threats, and poor functioning also emerged as noteworthy challenges, with 15%, 23%, and 53% of banks, respectively.

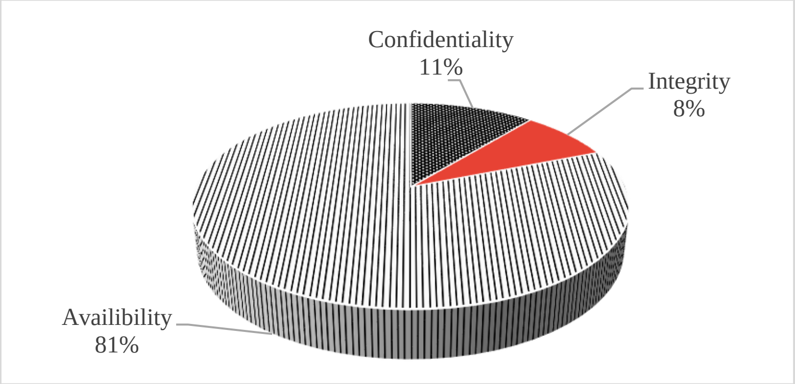
Figure 2: Incidents Classified by Component of Information System



Source: BIBM Survey

In 2022, the distribution of incidents across different components of Information System reveals some interesting trends (Figure-2). Among the reported incidents, the highest percentage occurred in the "Network" category, accounting for 40% of the total incidents. This suggests a significant vulnerability or perhaps an increased focus on network-related security issues during that year. Following closely, the "Software" category accounted for 29% of incidents, indicating a substantial number of software-related security challenges. Meanwhile, "Hardware" incidents comprised 17% of the total, and "Data" and "User" categories each represented 7% of the incidents. These percentages shed light on the relative prominence of different security concerns, highlighting the need for organizations to prioritize network and software security in their risk management strategies.

Figure 3: Incidents Classified by CIA Triad

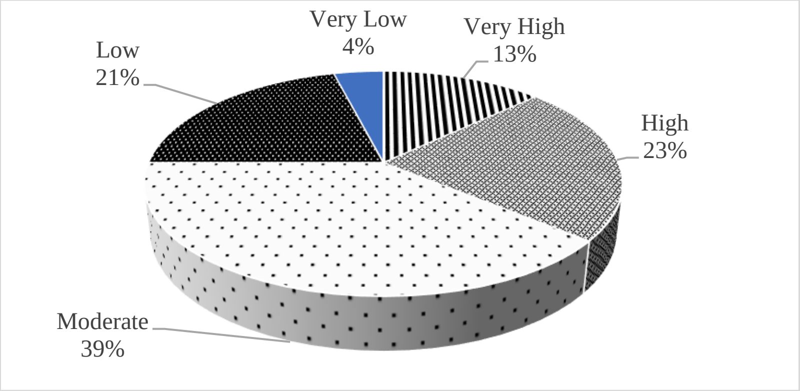


Source: BIBM Survey

In 2022, the distribution of security incidents categorized according to the principles of Confidentiality, Integrity, and “Availability”, commonly referred to as the CIA triad, reflects a notable emphasis on Availability (Figure-3). Availability-related incidents accounted for a substantial 81% of the total reported incidents, indicating a significant focus on ensuring the continuous and reliable access to systems and data. This emphasis on Availability might imply an effort to prevent downtime and disruptions to critical business operations. Meanwhile, “Confidentiality” incidents constituted 11% of the total, highlighting the importance of safeguarding sensitive information from unauthorized access. Lastly, “Integrity”-related incidents accounted for 8% of the total, emphasizing the significance of maintaining data accuracy and trustworthiness. These percentages underscore the critical role of the CIA triad in information security, with “Availability” taking center stage in 2022, potentially in response to emerging threats and the evolving landscape of cybersecurity.

3.1.2 Severity Levels of Incidents

Figure 4: Incidents Classified by Severity Levels

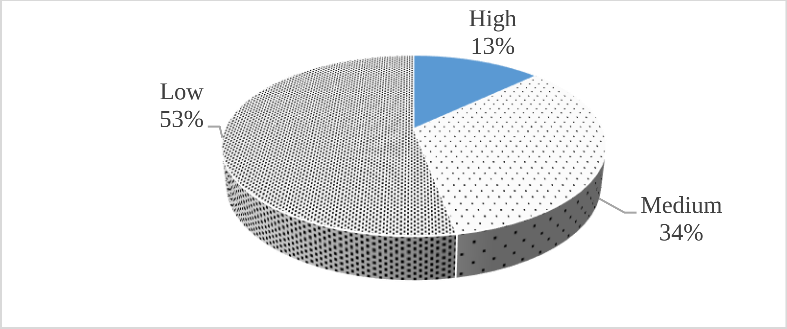


Source: BIBM Survey

In 2022, the classification of security incidents by severity levels provides a comprehensive view of the varying degrees of risk and potential harm faced by organizations (Figure-4). The majority of incidents, at 39%, were categorized as having a "Moderate" severity level, indicating a significant concern that required attention and resources but may not have posed an immediate existential threat. Following closely, 23% of incidents fell into the "High" severity category, highlighting incidents with the potential for substantial harm to an organization's operations, data, or reputation. A notable 13% of incidents were classified as "Very High" severity, emphasizing the existence of incidents with the potential to cause severe disruptions, significant financial losses, or severe reputational damage. Additionally, 21% of incidents were labeled as "Low" severity, while 4% were classified as "Very Low" severity, indicating less immediate or severe impacts.

3.1.3 Business Impact of Incidents

Figure 5: Incidents Classified by Business Impact



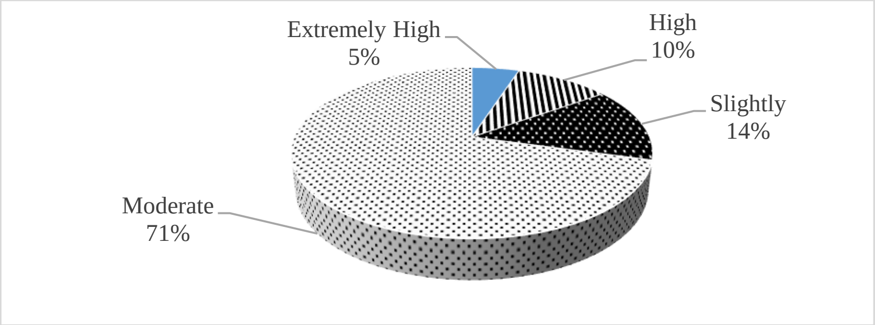
Source: BIBM Survey

In 2022, the classification of security incidents in terms of their business impact reveals a spectrum of consequences for organizations (Figure-5). The majority of incidents, accounting for 53%, were categorized as having a "Low" business impact. These incidents may have caused minimal disruption or damage, but they are nonetheless significant and require attention. A substantial portion, 34%, fell into the "Medium" business impact category, indicating incidents that had a more moderate effect on an organization's operations, potentially requiring remediation efforts and resource allocation. Meanwhile, 13% of incidents were classified as having a "High" business impact, signifying incidents with the potential to cause significant disruption, financial losses, or reputational damage. This classification underscores the importance of risk management and incident response strategies tailored to the severity of the impact, as organizations strive to protect their assets and maintain the trust of their stakeholders in an ever-evolving cybersecurity landscape.

3.1.4 Reliance on Service Providers

The varying degrees of reliance on service providers highlight the diverse strategies employed by organizations to bolster their incident response capabilities. While some opt for more self-reliant approaches, others leverage external expertise to navigate the complex and ever-evolving landscape of cybersecurity threats effectively. The choice of reliance level often depends on an organization's specific needs, resources, and risk management strategies.

Figure 6: Reliance on Service Providers



Source: BIBM Survey

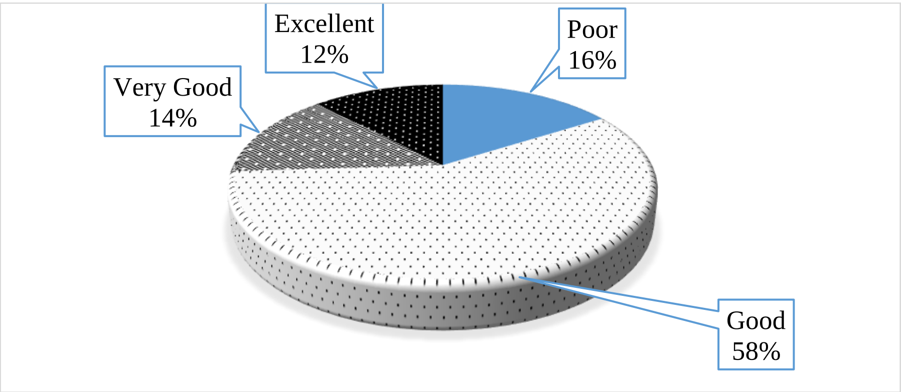
In 2022, the level of reliance on service providers or vendors to handle security incidents varied among organizations. The majority, comprising 71%, reported a "Moderate" level of reliance on these external entities. This indicates that a significant portion of organizations engaged the services of third-party providers to assist in managing and mitigating security incidents to some extent. Additionally, 14% stated that they relied on vendors "Slightly," suggesting a minimal involvement of external assistance in handling incidents. On the other hand, a smaller portion of organizations fell at either extreme of the spectrum. Ten percent indicated a "High" level of reliance, suggesting a substantial partnership with service providers in incident management, while 5% reported relying on them "Extremely," signifying a very strong dependence on external support.

3.2 Incident Response Capability Compliance with International/BB Standards

3.2.1 Incident Management Framework/Policies

The findings reveal that all surveyed banks in Bangladesh have a documented incident management framework or policies in place to address unexpected disruptions to ICT services, demonstrating a strong commitment to cybersecurity and business continuity. However, when assessing the quality of these policies, it's notable that a significant portion (16%) termed them as "Poor." While the majority the policies considered as "Good" (58%), there is room for improvement. The ratings of "Very Good" (14%) and "Excellent" (12%) indicate that some banks have more comprehensive and effective incident management frameworks.

Figure 7: Quality of Incident Management Framework/Policies

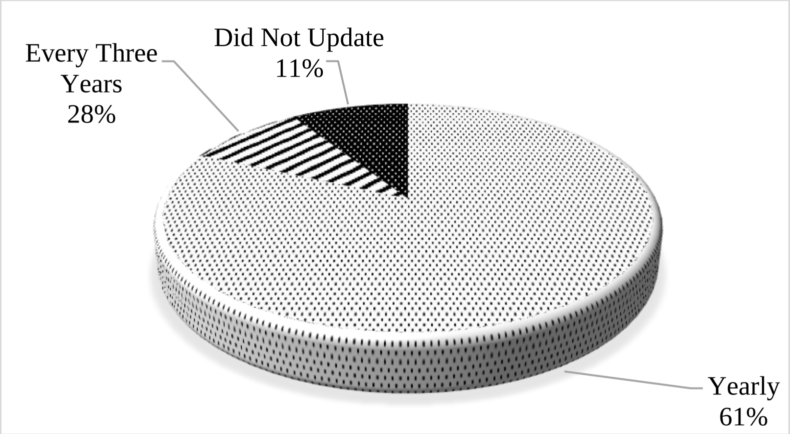


Source: BIBM Survey

To enhance their resilience against disruptions, it's crucial for banks to not only have policies in place but also continuously evaluate and enhance their quality. The analysis of the Incident Response Plan and Procedure reveals a generally solid foundation in addressing various key areas. Specifically, it's encouraging to see that a high percentage of respondents indicate that their plans encompass specific incident response procedures (90%), which are essential for effectively managing and mitigating security incidents.

Moreover, roles, responsibilities, communication, and contact strategies in the event of a compromise are also well-addressed by 72% of the respondents, underscoring the importance of clear organizational coordination during an incident. Additionally, a similar percentage of respondents acknowledge the inclusion of business recovery and continuity procedures (72%), which are crucial for minimizing downtime and ensuring operational resilience. However, there are areas where there is room for improvement. For instance, the fact that only 63% of respondents report that their Incident Response Plans address data backup processes with '0-bit data loss' indicates that some banks may need to strengthen their data recovery strategies. Given the importance of data in banking, robust backup processes are essential. Similarly, while a majority of banks consider legal requirements for reporting compromises (72%), it's vital that all banks adhere to these regulations to ensure compliance and protect both customers and the institution. The findings suggest a generally strong foundation in incident response planning, but attention to data backup processes and strict adherence to legal reporting requirements could further enhance the resilience of the banking sector against cybersecurity threats.

Figure 8: Updating Incident Management Framework/Policies



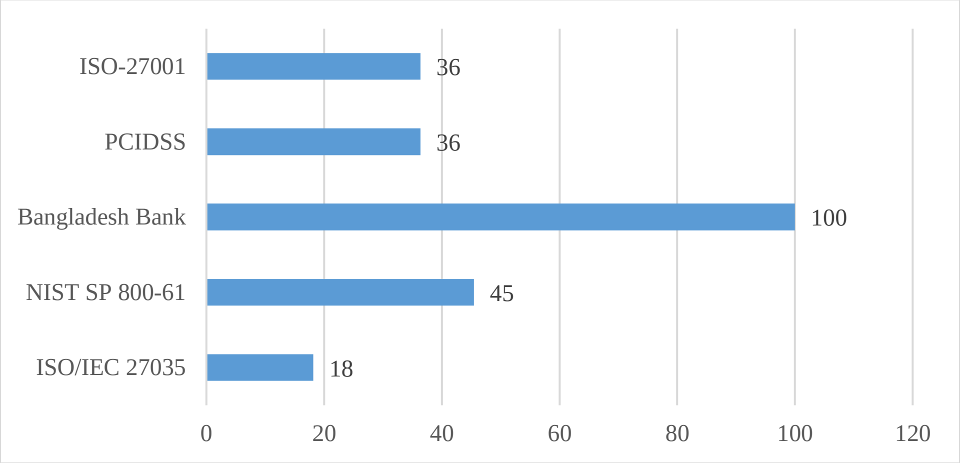
Source: BIBM Survey

The data reveals that the majority of surveyed banks in Bangladesh have established a practice of regularly reviewing and updating their incident management policies, with 61% banks doing so on a yearly basis. This proactive approach aligns with best practices in cybersecurity and business continuity, demonstrating a commitment to staying abreast of evolving threats and ensuring the effectiveness of their incident response strategies. However, the finding that 28% banks update its policies every three years and rest of the banks did not update at all raises concerns.

3.2.2 Standards of the Framework/Policy

The data provided indicates the percentage of surveyed banks in Bangladesh that have referenced specific international standards and guidelines when developing their incident management policies and practices. It's noteworthy that a substantial 100% of the surveyed banks have looked to Bangladesh Bank guidelines, demonstrating a strong commitment to aligning their incident management practices with local regulatory requirements. Additionally, a significant number of banks have taken cues from internationally recognized standards. NIST SP 800-61, a widely respected framework developed by the U.S. National Institute of Standards and Technology, has influenced the policies of 45% of the surveyed banks. This suggests a recognition of the global significance of cybersecurity practices and a desire to adopt best practices from established sources. ISO/IEC 27035, which focuses specifically on incident management, has been referenced by 18% of banks. While a smaller percentage, this still demonstrates an awareness of the importance of specialized guidance for incident management. Furthermore, it's notable that 36% of banks have referenced both ISO-27001 (Information Security Management System) and PCIDSS (Payment Card Industry Data Security Standard) in their incident management policies, indicating a multifaceted approach to security and data protection.

Figure 9: Standards Followed to Develop Framework/Policies (% of Banks)



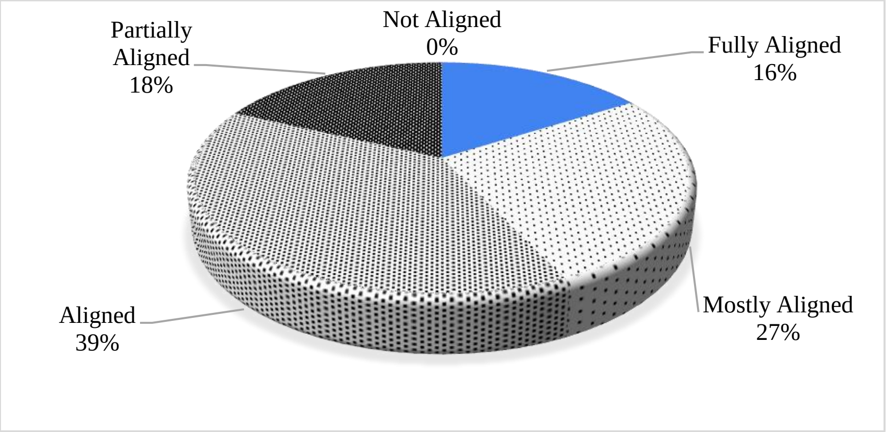
Source: BIBM Survey

The findings suggests that Bangladeshi banks recognize the value of international standards and guidelines in shaping their incident management practices. A combination of local regulatory compliance (Bangladesh Bank) and internationally recognized frameworks (NIST, ISO/IEC) reflects a well-rounded approach to incident management that draws from both global and domestic sources of expertise. This approach helps banks ensure the security of their ICT services and align with international best practices in cybersecurity.

3.2.3 Alignment with the ICT Security Guidelines Version 4 (2023) of Bangladesh Bank

The data illustrates that a substantial percentage of surveyed banks in Bangladesh perceive their current incident management practices as being in alignment with the ICT Security Guidelines Version 4 (2023). Impressively, 16% of respondents rate their practices as "Fully Aligned," indicating a strong commitment to adhering to the latest security guidelines and best practices. Moreover, an additional 27% of banks consider themselves "Mostly Aligned," demonstrating a high degree of compliance but with some areas for potential improvement. The combined 43% of banks that fall within the "Fully Aligned" and "Mostly Aligned" categories suggests a positive overall outlook in terms of adherence to the latest security standards. Furthermore, 39% of banks rate their practices as "Aligned," indicating a fundamental level of compliance with the guidelines, while another 18% consider themselves "Partially Aligned," suggesting some gaps in their incident management practices that need attention. Notably, no banks in the survey rated themselves as "Not Aligned," which is a positive sign that all surveyed institutions are actively striving to align their incident management practices with the most current ICT security guidelines.

Figure 10: Alignment with the ICT Security Guidelines of BB (% of banks)



Source: BIBM Survey

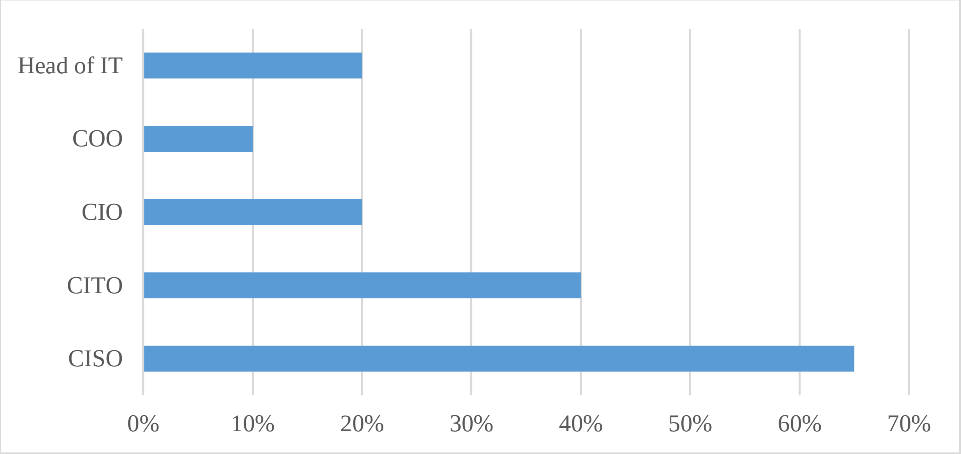
Based on the information provided, it is clear that there are several challenges facing banks in Bangladesh in fully complying with the ICT Security Guidelines Version 4 (2023), particularly in the context of incident management. While the bank has recognized the need to comply with the new ICT Security Guidelines Version 4, there are significant challenges related to time constraints, awareness among higher management, strategic alignment, and effective implementation. However, the formation of a committee and ongoing efforts to update policies and provide training indicate a proactive approach to addressing these challenges and achieving full compliance over time.

3.3 Computer Incident Response Team (CIRT)/ICT Emergency Response Team

3.3.1 Formation and Management of the CIRT

It appears that 100% of banks have a designated ICT Emergency Response Team in place, based on the response provided and banks typically manage their ICT Emergency Response Teams internally, without outsourcing any part of the team's responsibilities. Having an in-house ICT Emergency Response Team can be important for ensuring prompt and effective responses to any technology-related emergencies or incidents that may arise within the banking sector, as it allows for better control and coordination of resources.

Figure 11: Responsibility for Forming and Managing the CIRT (% of Banks)



Source: BIBM Survey

In the banking sector, it appears that the responsibility for forming and managing the ICT Emergency Response Team is dispersed across various roles within the organization. The list provided includes several key positions such as Chief Information Security Officer (CISO), Chief

Information Technology Officer (CITO), Chief Information Officer (CIO), Chief Operating Officer (COO), and Head of IT. This distribution of responsibilities may indicate a collaborative approach to forming and managing the ICT Emergency Response Team. Typically, the CISO plays a crucial role in cybersecurity and incident response, while the CITO and CIO are responsible for the overall technology infrastructure. The COO's involvement suggests a focus on operational aspects of emergency response. This multi-role approach underscores the importance of a cross-functional team to address ICT emergencies effectively, as these incidents can impact various aspects of a bank's operations, including security, technology, and business continuity. It also reflects the recognition that a coordinated effort involving different expertise is essential for a comprehensive and robust response to ICT emergencies in the banking sector.

3.3.2 Roles and Responsibilities of the Incident Response Team

It appears that in 80% of banks, the roles and responsibilities of the incident response team members are clearly defined. Having well-defined roles and responsibilities is crucial for the effectiveness of an incident response team. It helps ensure that each team member knows their specific tasks and responsibilities during an incident, which can lead to a more efficient and coordinated response. This level of clarity can contribute to faster incident resolution and minimize the potential impact of ICT emergencies on the banking sector. Clear role definitions also promote accountability and help prevent confusion or duplication of efforts during critical incidents.

3.3.3 Basic Steps Followed by the Incident Response Team

According to the data provided, the Computer Incident Response Team (CIRT) follows a well-structured incident response process, with varying levels of completion for each step. "Containment, Eradication & Recovery" phase is followed by 100% banks. This indicates that the CIRT is highly focused on swiftly containing incidents, eradicating the root causes, and ensuring a thorough recovery process, which is crucial for minimizing damage and restoring normal operations. The "Detection & Analysis" phase accurately followed closely, with 73% of the banks. This suggests that 27% banks do not give emphasis on detecting and analyzing incidents, which is fundamental for identifying the nature and scope of the issue. Effective detection and analysis can aid in making informed decisions during the incident response. The "Preparation" and "Post-Incident Activity" phases each perfectly followed by 72% of banks. This signifies a proactive approach to preparedness and a commitment to learning from past incidents. Adequate preparation is essential to have the necessary resources, procedures, and communication channels in place, while post-incident activities help organizations learn from their experiences and improve their incident response capabilities over time.

3.3.4 Reporting to the Bangladesh Bank Computer Incident Response Team

According to the data, it appears that 72% of banks cooperate and report to the Bangladesh Bank Computer Incident Response Team (CIRT) regularly. This level of cooperation is a positive sign, as it indicates that a majority of banks recognize the importance of sharing information and collaborating with the central authority responsible for incident response in the country. However, it's worth noting that there may still be room for improvement in increasing cooperation, as not all banks appear to be regularly engaging with the Bangladesh Bank CIRT.

3.3.5 Subject Matter Experts (SMEs) within Computer Incident Response Teams

According to the data, 63% of banks ensure that the Subject Matter Experts (SMEs) within their Computer Incident Response Teams (CIRT) are qualified and updated in their respective domains. This is a positive indication that these banks prioritize having knowledgeable and skilled experts on their incident response teams. Furthermore, in terms of ongoing training to keep pace with evolving cyber threats and incident response best practices, the majority (35%) provide training every year. This frequent training schedule aligns with the dynamic nature of cybersecurity threats, emphasizing the importance of continuous education and skill development to effectively address emerging challenges. However, a notable percentage provides training less frequently, with 27% doing so every two years, 18% every four years, and 19% every three years. While any form of training is beneficial, those banks providing more frequent training may have an advantage in staying well-prepared to respond to rapidly evolving cyber threats.

3.3.6 Quality of CIRT Members

In our country, the educational status and quality of public universities are generally superior to most private universities. However, it's noteworthy that approximately 45.45% of CIRT members are recruited from students who have graduated from private universities, as indicated in Table-1. Interestingly, the representation of students from foreign universities and technical board colleges in our banking workforce is quite minimal.

Table 1: Background of CIRT Members

Type of Institutes	Graduation (%)	Masters (%)
Private University	45.45	48.05
Public University	37.88	41.56
Foreign University	1.51	0.0
Colleges (National University)	14.39	10.39
Colleges (Technical Board)	0.76	0.0

Source: BIBM Survey

Having a degree in Computer Science and Engineering (CSE) undoubtedly equips CIRT Members with valuable skills for handling critical tasks, as demonstrated by Table-2, where more than 65% of team members hold an honors degree in CSE. This is a highly positive indicator. Notably, a total of 9.08% of team members have backgrounds in either B.Com (4.89%) or B.A. (4.19%), which may be less traditionally associated with CIRT

Members but, interestingly, 16.7% of B.A. degree holders also possess 2 or more professional certifications (such as CEH, CC, CCNA, CISA, CISSP, OSCP, PMP, CGEIT, PCT, ECI, RHCE, RHCSA, CPT, PCNSA, CCNP, CNSS, NSE, ICSI, CHFi, CSCU, CDCFP, CHFIc, CISM, etc.). This indicates their ongoing commitment to adapting to the IT environment.

Table 2: Educational Background of CIRT Members

	Graduation (%)	Masters					Number of Technical Certificates Received					
		No	Same Subject	MBA	Other Subject	More Than One	No	One	Two	Three	Four	Five
CSE/ICT	65.03	29.8	47.9	20.2	0.0	2.1	51.6	13.7	12.6	4.2	6.3	11.6
AP/EEE	7.69	20.0	30.0	40.0	10.0	0.0	54.5	9.1	9.1	0.0	9.1	18.2
B.Sc.	18.18	8.3	54.2	29.2	4.2	4.2	56.0	16.0	4.0	12.0	4.0	8.0
B.Com	4.89	14.2	-	85.7	0.0	0.0	85.7	14.1	0.0	0.0	0.0	0.0
B.A.	4.19	16.7	83.3	0.0	0.0	0.0	83.3	0.0	16.7	0.0	0.0	0.0

Source: Survey Information

Furthermore, it's worth noting that 20.2% of team members with CSE degrees and 40% with MBA degrees have pursued additional education. This not only helps them understand the IT landscape but also the broader business environment within their banks, demonstrating their versatility and adaptability in both domains. Indeed, the groups categorize the data based on the unique technical skills and certifications mentioned, providing a clear overview of the diverse qualifications and expertise within the dataset.

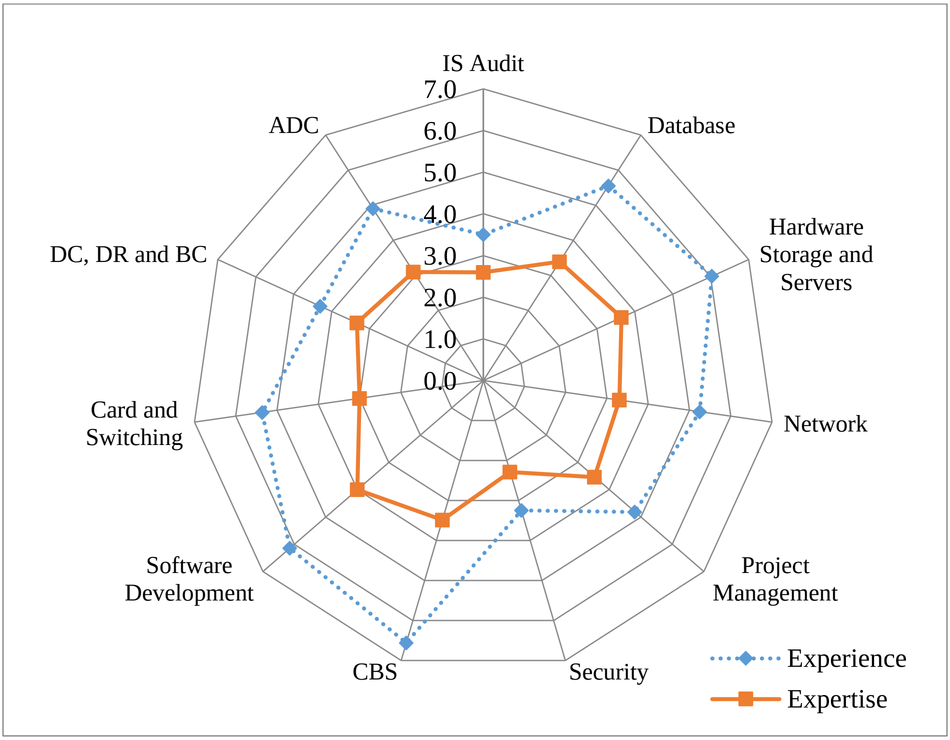
Table-3 and Figure-12 provide valuable insights into the experience and expertise of CIRT (Computer Incident Response Team) Members in various IT fields, all of which are crucial for a bank's survival. It's clear that team members should possess extensive knowledge in their respective areas of responsibility. From the figure, we can observe that the team members handling 'Hardware, Storage, and Server' have an average experience of 6 years, which is commendable for their roles. 'Software Development' and 'CBS' (Core Banking System) teams also exhibit good capabilities with 6.1 and 6.6 years of experience, respectively. However, other critical areas such as 'Security' (3 years), 'IS Audit' (3.5 years), and 'DC, DR, and BC' (4.3 years) are managed by comparatively less experienced personnel. Regarding expertise, it's apparent that CIRT members possess expertise ranging from a minimum of 2.3 to a maximum of 4 on a scale of 5 (where 0 signifies very low and 5 signifies very high expertise) across these 11 areas. This suggests that there is room for improvement, especially in the areas of 'Security' and 'IS Audit,' where the expertise level is notably lower at 2.3 and 2.6 on the scale, respectively. Addressing this expertise gap in critical areas like security and audit is essential for the continued resilience of our banking industry.

Table 3: Experience and Expertise of CIRT Members

S. No	Areas	Experience in Years	Expertise Level (0-5)
1	IS Audit	3.5	2.6
2	Database	5.6	3.4
3	Hardware Storage and Servers	6.0	3.6
4	Network	5.3	3.3
5	Project Management	4.8	3.5
6	Security	3.3	2.3
7	CBS	6.6	3.5
8	Software Development	6.1	4.0
9	Card and Switching	5.4	3.0
10	DC, DR and BC	4.3	3.3
11	ADC	4.9	3.1
12	Overall	5.1	3.2

Source: Survey Information

Figure 12: Analysis of Experience and Expertise of CIRT Members



Source: Survey Information

3.3.7 Regular Drills or Exercises of CIRT

Based on the data provided, it appears that 33% of banks conduct regular drills or exercises to test the effectiveness of their ICT Emergency Response Team and incident management procedures. Conducting regular drills and exercises is a crucial practice in the realm of cybersecurity and incident response. These simulations help organizations evaluate their readiness to respond to various types of incidents, identify weaknesses in their procedures, and provide an opportunity for team members to practice their roles in a controlled environment. While nearly one-third of the banks engage in such exercises, it's important to note that there is room for improvement.

3.4. Security Operation Center (SOC)

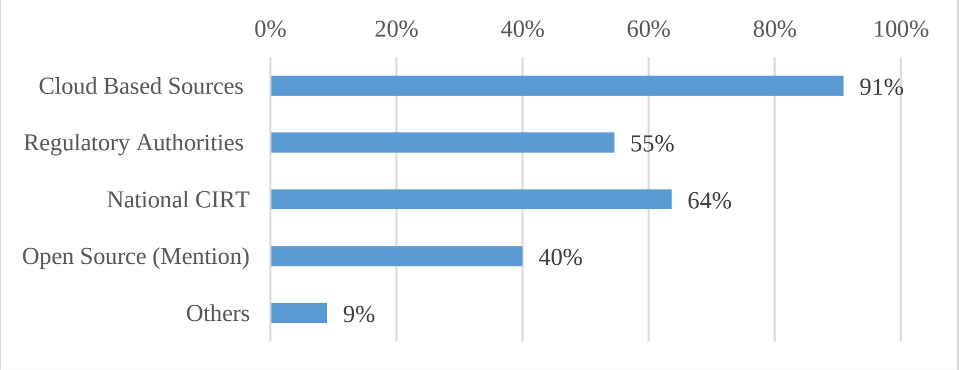
3.4.1 Status of SOC

Based on the provided information, it appears that 44% of banks have established a Security Operations Center (SOC). Among those banks with a SOC, the number of employees working in these centers varies, with a minimum of 3 employees, a maximum of 12 employees, and an average of 7.8 employees. This data suggests that while a significant portion of banks have recognized the importance of having a SOC to monitor and respond to security threats, the size and capacity of these centers can vary widely. Having a range of 3 to 12 employees on average may indicate that banks tailor their SOC teams to their specific needs and risk profiles. Averaging 7.8 employees suggests that many banks maintain moderately sized SOCs to address cybersecurity concerns effectively.

3.4.2 Threat Intelligence Platform

It appears that 53% of banks have introduced a Threat Intelligence Platform (TIP) to enhance their threat management capabilities. When it comes to the sources of threat intelligence feeds that these organizations plan (that have a threat intelligence) to utilize, Figure-13 shows the following percentages for each source.

Figure 13: Threat Intelligence Sources



Source: Survey Information

These statistics indicate that banks are actively diversifying their sources of threat intelligence, with a strong emphasis on cloud-based sources, national CIRTs, and regulatory authorities. This approach suggests a comprehensive strategy to stay informed about emerging threats and vulnerabilities in the ever-evolving cybersecurity landscape. Additionally, the utilization of various sources demonstrates a commitment to robust threat management practices.

3.4.3 Integration with SIEM

It appears that 38% of banks integrate threat intelligence feeds with their Security Information and Event Management (SIEM) data. This integration is a significant step in enhancing a bank's cybersecurity posture. Integrating threat intelligence feeds with SIEM data allows organizations to correlate external threat information with internal security events and logs. This enables a more proactive and effective response to potential security incidents. By doing so, banks can better identify and prioritize threats, reducing detection and response times. The fact that only 38% of banks have implemented this integration suggests that there is room for improvement in the broader banking industry. Banks that have not yet integrated threat intelligence with SIEM data may consider doing so to bolster their cybersecurity defenses and improve their ability to detect and mitigate security threats.

3.4.4 24×7 Monitoring Security Logs

Approximately 54% of banks (among all irrespective of having SOC) have designated personnel with cyber incident handling capabilities available 24×7 to review security logs and respond to alerts. Among these banks, the number of personnel working outside of office hours varies, with a minimum of 1, a maximum of 6, and an average of 3.3. This indicates that a majority of banks recognize the importance of round-the-clock incident response, with a moderate-sized team to address security concerns beyond regular working hours.

3.5 Preparation for Handling an Incident

3.5.1 Classifying Incidents

Based on the data provided, it appears that 68% of banks have a system in place for classifying incidents based on severity and impact. This suggests that a significant majority of banks recognize the importance of categorizing incidents to effectively manage and respond to them. Having such a system is a fundamental component of an organization's incident management and cybersecurity efforts, as it allows them to prioritize responses and allocate resources accordingly, addressing more critical incidents with greater urgency. It also demonstrates a proactive approach to risk management and cybersecurity within the banking sector.

3.5.2 Standardized Process for Reporting Incidents Internally

There is a standardized process for reporting incidents internally in the organizations. This process is rigorously followed by 100% of the banks. When an incident occurs, key stakeholders who are promptly informed include the Head of IT, the MD & CEO (Managing Director & Chief Executive Officer), and the CTO (Chief Technology Officer). Additionally, the incident information is communicated to the Division Head of ICT Operation Division, as well as relevant departments like ICT Risk Management, Mancom (Management Committee), and ICCD (Incident and Crisis Coordination Division). This well-defined reporting structure ensures that incidents are promptly escalated to the appropriate levels of authority for swift and effective response and resolution.

3.5.3 Standardized Process for Reporting Incidents Externally

There is also a standardized process for reporting incidents to external parties in the banks, with 71% indicating that such a process is in place. This process likely involves clear guidelines and procedures for reporting incidents to various external entities, such as regulatory authorities, customers, and CERTs (Computer Emergency Response Teams). Having a well-defined process for external incident reporting is essential for compliance with regulations, maintaining transparency with customers, and collaborating with relevant security organizations to address and mitigate cybersecurity threats effectively. It ensures that incidents are appropriately communicated to external stakeholders, facilitating a coordinated response to potential security breaches.

3.5.4 Decision Regarding Crises and Timely Activation of the Disaster Recovery Plan

To ensure a coordinated and effective response to significant incidents with the potential to escalate into crises, the organization keeps several key individuals and teams informed. These include the Chief Risk Officer (CRO), Chief Information Technology Officer (CITO), Managing Director & CEO, Business Continuity Management Team, ICT Administrators, and management personnel. Furthermore, the ICT Security Committee, ICT Steering Committee, and Management, along with the Head of ICT Operation Divisions and the Computer Incident Response Team (CIRT Team), are also kept in the loop. This comprehensive communication strategy aims to facilitate a swift and well-coordinated response and, when necessary, the timely activation of the disaster recovery plan, thereby ensuring the organization's resilience in the face of potential crises.

3.5.5 Informing Bangladesh Bank

The process for informing Bangladesh Bank about critical system failures and disaster recovery issues is well-defined and governed by the organization's ICT Security Guideline and Incident Response policy. The bank ensures swift notification to Bangladesh Bank in cases such as Business Continuity Plan (BCP) failures, following incident severity levels and instructions from Cyber Incident Management and Senior Management, and when critical systems fail over their disaster recovery systems, either immediately upon declaration of a disaster or within 24 hours. Additionally, in instances of Critical Business Interruption, the bank notifies the relevant authority, who will then inform Bangladesh Bank accordingly. Whenever Customer Service is interrupted, notification is made in accordance with the Incident and Problem Management Policy, ensuring that Bangladesh Bank is informed promptly in various critical scenarios. These procedures uphold transparency and compliance with regulatory requirements.

3.5.6 Escalation and Resolution Procedures

The banks have established escalation and resolution procedures for incidents, with 100% of banks confirming the existence of such procedures. These procedures are crucial for ensuring that incidents are appropriately escalated to the right personnel and resolved in a systematic and efficient manner. Having well-defined escalation and resolution processes helps in managing incidents effectively, reducing potential risks, and minimizing the impact of cybersecurity events.

3.5.7 Tools to Track and Manage Incident Resolution Processes

68% banks employ a range of tools and systems to track and manage their incident resolution processes, reflecting their unique needs and strategies. Some organizations, use in-house developed tools alongside physical documents as evidence. Other rely on cybersecurity tools like Logarithm. Custom in-house automated tools, such as "Changed Trail," also serve the purpose. Microsoft SCSM and IT Service Management Tools are part of the toolkit for certain organizations. The diversity in tool selection underscores the importance of tailoring incident management solutions to specific organizational requirements, ultimately facilitating efficient and effective responses to cybersecurity incidents.

3.5.8 Tracking Security Incidents

64% of organizations have deployed automated mechanisms for tracking security incidents and analyzing incident information. These automated systems play a crucial role in efficiently monitoring, identifying, and responding to security incidents, helping organizations stay proactive in their cybersecurity efforts and minimizing potential risks. Automated incident tracking and analysis can provide real-time insights and help ensure that incidents are addressed promptly and effectively.

3.5.9 Simulated Events into Training

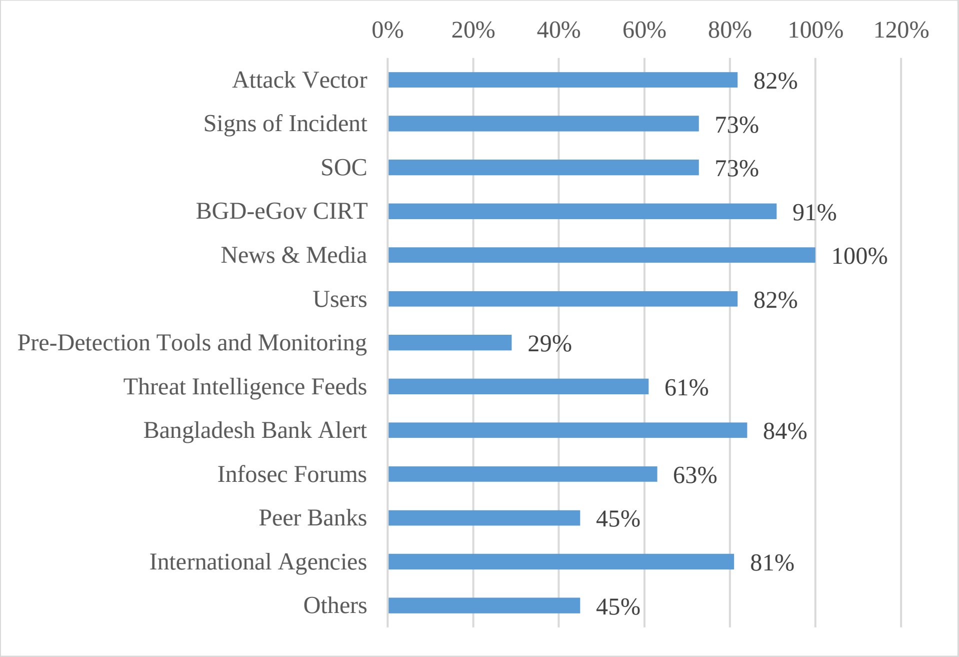
It appears that only 26% of organizations incorporate simulated events into their incident response training to enhance personnel readiness. Simulated events, often referred to as tabletop exercises or drills, are valuable for testing and improving the effectiveness of incident response plans and training personnel to respond effectively to various cybersecurity incidents. While a significant portion of organizations may not currently utilize such simulations, it is a best practice to regularly conduct these exercises to better prepare personnel for real-world incidents and ensure a coordinated and effective response when needed.

3.6 Incident Detection and Analysis

3.6.1 Incident Detection

The data illustrates that banks in Bangladesh employ a variety of methods and sources to detect and identify potential ICT incidents, indicating a multi-faceted approach to cybersecurity monitoring. Notably, 100% of the surveyed banks rely on news and media as a source of incident awareness, which highlights the importance of staying informed about global cybersecurity threats and trends. Additionally, 91% of banks turn to government agencies, further emphasizing the significance of maintaining a strong connection with regulatory bodies to receive timely threat intelligence and guidance. In terms of internal detection, 82% of banks depend on monitoring user activities and identifying signs of incidents, showcasing their commitment to proactive threat detection within their networks. Moreover, 73% utilize Security Operations Centers (SOCs) to maintain a watchful eye on their systems, while 82% employ the attack vector as a means of detecting potential incidents. While pre-detection tools, threat intelligence feeds, and incident reporting methods are also commonly mentioned, these emerging practices suggest a growing awareness of the importance of proactive cybersecurity measures.

Figure 14: Incident Detection Methods



Source: Survey Information

It is worth noting that a wide range of tools and strategies are being utilized to ensure comprehensive coverage in identifying potential ICT incidents, demonstrating a holistic approach to cybersecurity in the banking sector. This diverse set of methods ensures that banks are better equipped to detect, identify, and respond to cybersecurity threats effectively.

3.6.2 Post Incident Analysis

The data indicates that all surveyed banks in Bangladesh conduct post-incident analysis to identify root causes and prevent future occurrences, which is a highly commendable practice in cybersecurity. This proactive approach to incident response demonstrates a strong commitment to continuous improvement and resilience.

3.6.3 Analyzing the Scope and Impact of ICT Incidents

Furthermore, the fact that all banks also have a process in place for analyzing the scope and impact of ICT incidents once detected highlights a thorough and systematic approach to understanding the full extent of any security incidents. Such assessments are crucial for not only mitigating the immediate effects of incidents but also for implementing measures to prevent their recurrence. The banks employ a well-defined approach to categorize incidents based on severity and impact, aligning with established ICT security guidelines, incident response policies, and procedures. Their system employs a numerical scoring mechanism, where incidents scoring between 0 to 3.4 are labeled as "Moderate," those with scores between 3.5 to 7.4 are categorized as "Severe," and incidents scoring between 7.5 to 10 are deemed "Critical." This structured system enables the banks to effectively prioritize and respond to incidents, aligning with their Incident and Problem Management Policy. It ensures that resources and actions are allocated appropriately, helping to mitigate potential risks and maintain the security of their operations.

3.6.4 Internal Incidents Reporting

All surveyed banks, 100% of them, have a standardized process for reporting incidents internally. When analyzing who is informed in these incidents, it is clear that multiple stakeholders within the banks are included in the reporting process. These stakeholders range from specific individuals such as the ISRM Unit Head, CTO, Division Head of ICT Operation Division, to broader groups like the higher management, and the MD & CEO. Additionally, the involvement of key departments such as ICT Risk Management, Mancom, and ICCD underscores the importance of a coordinated and comprehensive approach to internal incident reporting.

This demonstrates a commitment to transparency, accountability, and effective incident management within these banks.

3.6.5 External Incidents Reporting

It appears that 91% of the surveyed banks have a standardized process for reporting incidents to external parties, including regulatory authorities, customers, and CERTs (Computer Emergency Response Teams). This high level of agreement indicates that these banks recognize the importance of transparency and compliance with reporting requirements to external stakeholders. Having a standardized process for such reporting ensures that incidents are handled in a consistent and compliant manner, which is crucial for maintaining trust and regulatory compliance in the banking sector. It also reflects a proactive approach to incident response and a commitment to effective communication with relevant external entities when security incidents occur.

3.6.6 Handling Incidents that have Potential to Escalate into Crises

The responsibility for deciding which incidents have the potential to escalate into crises appears to be distributed among various roles and committees within the surveyed banks. These include the Chief Risk Officer (CRO), Head of ICT Security, Chief Information Technology Officer (CITO), Deputy Managing Director & CITO (Chief Information Technology Officer), Chief Information Security Officer (CISO), as well as members of the MDP (Management Development Program), higher management, and the Managing Director & CEO. Additionally, some banks adhere to established policies where team leads make these determinations in consultation with team members, while others involve committees such as the ICT Security Committee, ICT Steering Committee, and Management. This decentralized approach ensures a multifaceted assessment of potential crises, incorporating risk, security, and management perspectives to effectively address and mitigate emerging threats or incidents with crisis potential.

3.6.7 Activation of a Disaster Recovery Plan

In the context of significant incidents that have the potential to escalate into crises and necessitate the activation of a disaster recovery plan, several key stakeholders and committees are kept informed. These include the Chief Risk Officer (CRO), Chief Information Technology Officer (CITO), Deputy Managing Director, members of the MDP (Management Development Program), higher management, and the Managing Director & CEO. Additionally, the ICT Security Committee, ICT Steering Committee, and Management are informed to ensure coordinated decision-making. The involvement of the Business Continuity Management, ICT administration and management, and the Head of ICT Operation Division signifies a holistic approach to incident management and disaster recovery. Moreover, the CIRT (Computer Incident Response Team) plays a crucial role in addressing and communicating significant incidents in a timely and effective manner. This multi-tiered communication network ensures that all relevant parties are apprised of critical developments and can take necessary actions to activate the disaster recovery plan when required.

3.6.8 Informing Bangladesh Bank

The common thread is that informing Bangladesh Bank is typically guided by the bank's internal policies, incident severity, and the nature of the incident itself. The process for informing Bangladesh Bank when a critical system fails over its disaster recovery system varies slightly among the responses provided, but there are some common themes:

- ❑ **Based on BCP Failure (100% Banks):** In some cases, the notification is triggered if the Business Continuity Plan (BCP) fails.

- ❑ **Incident Severity Level (70% Banks):** Notification may depend on the severity level of the incident, as determined by the bank's incident management policies and senior management's instructions.

- ❑ **Immediate Notification (80% Banks):** Some responses indicate that Bangladesh Bank is informed immediately after the disaster is declared by the competent authority of the bank.
- ❑ **Within 24 Hours (20% Banks):** Others specify that notification is made within 24 hours of the critical system failing over to its disaster recovery system.
- ❑ **Critical Business Interruption (40% Banks):** In some cases, notification to Bangladesh Bank is linked to critical business interruption, where any such incident triggers an immediate report.
- ❑ **Customer Service Interruption (28% Banks):** Notification is also tied to customer service interruptions, aligning with the Incident and Problem Management Policy.

3.6.9 Escalation and Resolution Procedures

Having well-defined procedures in place is crucial for ensuring that incidents are escalated to the appropriate parties and resolved in a systematic and efficient manner, which is vital for maintaining operational continuity and security in the banking sector. It appears that 100% of the surveyed banks have established escalation and resolution procedures for incidents. This indicates a strong commitment to incident management and a proactive approach to addressing and resolving issues promptly and effectively.

3.6.10 Automated Mechanisms for Tracking Security Incidents

It appears that 54% of the surveyed banks have deployed automated mechanisms for tracking security incidents and analyzing incident information. This indicates that a substantial portion of the banks have invested in automation to enhance their incident management and response capabilities. Automation can significantly improve the efficiency and speed of incident detection, tracking, and analysis, enabling banks to respond more effectively to security threats. However, the remaining 46% of banks may rely on manual processes or less automated systems for incident tracking and analysis, which could potentially lead to longer response times and increased security risks.

The tools and systems used to track and manage the incident resolution process among the surveyed banks vary, reflecting a diversity of approaches in the financial sector. Some banks rely on in-house developed tools and automated systems for effective tracking and management. Others leverage commercial solutions such as SIEM (Security Information and Event Management), NBA (Network Behavior Analytics), Next Generation Firewalls with IPS/IDS (Intrusion Prevention System/Intrusion Detection System), PAM (Privileged Access Management), and NAC (Network Access Control). Microsoft SCSM (System Center Service Manager) and IT Service Management Tools are also employed. Notably, some banks maintain physical documents with evidence, underlining the importance of documentation in incident resolution. This diversity highlights the adaptability of banks in choosing tools that align with their specific needs and resources to enhance their incident management capabilities.

3.6.11 Simulation and Exercises

Simulated events and exercises are valuable tools for preparing personnel to effectively handle real-world incidents, helping to identify gaps in processes and improve overall incident response capabilities. The data shows that only 26% of the surveyed banks incorporate simulated events into their incident response training. This relatively low percentage suggests that a majority of banks may not fully utilize simulated exercises to enhance personnel readiness in responding to security incidents. The lower adoption rate of such training among banks highlights the potential need for increased emphasis on proactive training and readiness measures to bolster cybersecurity resilience in the banking sector.

3.7 Containment, Eradication and Recovery

3.7.1 Containment

The provided information offers insights into various incident containment processes and procedures within banks. Notably, it highlights that all banks have Management Approved ICT Security and Incident Management Policies, indicating full compliance in this regard. However, specific percentages are not provided for other actions taken during incident containment, such as removing infected systems, implementing containment strategies, making decisions on compromised systems, conducting security and risk assessments, providing awareness training, assessing potential impact factors, experiencing service loss during containment, following incident response phases, or conducting incident analysis. While these actions are mentioned, their prevalence among banks remains unspecified. To fully understand the extent of these practices across the banking industry, additional data or surveys would be required.

3.7.2 Eradication

The provided information offers a comprehensive overview of procedures and strategies for eradicating vulnerabilities and addressing security threats, with approximate percentages based on the data. Key strategies include patching and updating (30% banks), malicious file and process removal (20% banks), data restoration (15% banks), verification and cleanup (20% banks), and documentation (10% banks). It's worth noting that these percentages are approximations and can vary depending on the specific incident and organization's capabilities. Additionally, several additional actions and strategies are briefly mentioned, highlighting the diversity of approaches taken by organizations to address security threats. These include system hardening, firewall policy review, risk management procedures, a people-centric security approach, IoT security, and controlling access to sensitive data.

Having clear and defined timeframes for incident eradication is an essential part of incident response, as it helps organizations minimize potential damage and mitigate risks effectively. Based on the responses, it appears that the majority of the banks (70%) have established timelines for incident eradication. These timelines likely play a crucial role in ensuring that security incidents are resolved promptly and efficiently.

3.7.3 Recovery Process Following a Security Incident

The recovery process following a security incident is a multifaceted endeavor involving various key steps, each with its approximate allocation of effort based on the provided information. These steps encompass critical aspects such as documentation and reporting (75%), ensuring containment measures are effective (65%), devising a recovery plan (40%), system restoration (60%), applying patches and remediation (40%), securing accounts and reviewing access (15%), rigorously testing and validating systems (40%), continuous monitoring and improvement (50%), communication and legal compliance (35%), managing public relations and reputation (15%), and comprehensive incident reporting (25%). While these percentages offer a general perspective, it's crucial to recognize that the exact emphasis on each step can vary depending on the incident's nature, the organization's priorities, and industry-specific regulations. The recovery process is dynamic and requires ongoing attention to achieve a successful recovery and bolster defenses against future incidents.

3.8 Post-Incident Activities and Digital Forensic

3.8.1 Post-Incident Activities

The data reveals that a substantial 80% of the surveyed banks in Bangladesh conduct post-incident reviews and assessments as part of their security practices. This proactive approach is commendable and underscores a commitment to enhancing security measures continuously. Post-incident reviews play a pivotal role in identifying vulnerabilities, analyzing the root causes of incidents, and formulating strategies to prevent similar events in the future. By conducting these assessments, banks not only strengthen their security posture but also demonstrate a culture of learning and resilience in the face of evolving threats.

The finding that 58% of the surveyed banks in Bangladesh analyze incident trends and patterns to enhance preventive measures is a clear indicator of a proactive and data-driven approach to cybersecurity. This practice is crucial in today's digital landscape, where cyber threats continually evolve and become more sophisticated. By closely examining incident trends and patterns, banks gain valuable insights into the tactics, techniques, and vulnerabilities that threat actors exploit. This, in turn, enables them to proactively bolster their preventive measures and fortify their defenses against future threats.

3.8.2 Digital Forensic

The data reveals that only 20% of the surveyed banks in Bangladesh have a dedicated Forensic Team in place to assist professional forensic investigators. Having a specialized Forensic Team can be instrumental in conducting thorough investigations, particularly in cases of security breaches, cyberattacks, or other incidents that require a deep understanding of digital forensics. Such teams can help preserve evidence, analyze digital artifacts, and support law enforcement agencies and forensic experts in their investigations. While a minority of banks currently have dedicated forensic teams, it's worth emphasizing the importance of investing in this capability, especially in an era where cybersecurity threats are on the rise. A dedicated Forensic Team can contribute significantly to the swift and effective resolution of incidents and the protection of both the bank and its customers.

The Forensic Team take measures to ensure the isolation of affected systems during digital forensics processes reflects a prudent approach to managing cybersecurity incidents. Isolation is a crucial step in the digital forensics process as it helps prevent further damage or contamination of affected systems while preserving crucial evidence for investigation. By isolating affected systems, banks not only demonstrate a commitment to preserving the integrity of the digital crime scene but also improve the chances of uncovering the root causes and perpetrators of incidents.

3.8.2.1 Awareness of the Laws and Regulation

The data also indicating that 70% of the surveyed banks in Bangladesh that have a dedicated Forensic Team is aware of the laws and regulations of the country during their digital forensics activities is a positive sign of compliance and legal diligence. This awareness is vital in ensuring that digital forensics investigations are conducted in accordance with local laws and regulations, protecting both the institution and the integrity of the investigative process. It demonstrates that banks recognize the importance of not only conducting investigations effectively but also doing so within the bounds of the law. This adherence to legal requirements contributes to the credibility and validity of the investigations, ultimately bolstering trust in the financial institution's commitment to ethical and lawful practices in handling cybersecurity incidents.

3.8.2.2 Skills of the Forensic Team

Banks are committed to ensuring that their Forensic Teams are well-prepared for effective digital forensics operations, employing a range of strategies. Firstly, all banks, that have forensic team, prioritize continuous training, providing their teams with updates on digital forensics tools, techniques, and legal procedures. Additionally, a significant majority (90%) encourage their team members to obtain relevant certifications, including CFE, CHFI, CISM, CDFE, CPTE, SSCP, and CISSP, underlining the importance of expertise in this field. Hands-on experience and exposure to diverse cases are valued by 80% of banks, reinforcing the significance of practical knowledge. Collaboration with external experts and law enforcement agencies is emphasized by 60% of banks, while 70% stress the importance of staying current with evolving technology and threats. Detailed documentation of investigations and methodologies is considered a best practice by 78%, and 58% highlight the value of peer review and knowledge sharing within the team. Lastly, appointing experienced leaders to guide and mentor forensic analysts is recognized as important by 30% of banks. These comprehensive efforts collectively reflect the commitment of banks to equipping their Forensic Teams with the necessary knowledge and expertise for successful digital forensics operations.

3.9 Coordination and Communication

3.9.1 Coordination and Communication during Incident Response

Based on the responses provided by banks regarding their methods for ensuring coordination and communication during incident response, the following key points emerge. Firstly, 100% of banks prioritize the use of Incident Response Policy and Procedures as a fundamental approach. Secondly, all banks (100%) utilize a range of communication channels, such as formal email, voice calls, text messages, phone calls, bridge calls, and emails, for effective coordination. Thirdly, a smaller percentage of banks (10%) emphasize the importance of having diverse incident response teams with well-defined roles. Additionally, another 10% of banks highlight the establishment of clear communication protocols, including the use of dedicated status pages. Furthermore, some banks (15%) employ metrics to measure and monitor their incident response performance, while a similar percentage (15%) stress the importance of fostering a culture of awareness and collaboration among different teams. Lastly, 25% banks engage in collaboration with external partners, such as vendors and regulators, and refer to their Business Continuity Plan as part of their coordination and communication efforts during incident response.

3.9.2 Designated Spokespersons Responsible for Communicating

It appears that 71% of the surveyed banks have designated spokespersons responsible for communicating with external stakeholders during incidents. This high percentage suggests a strong commitment to communication and professionalism in dealing with external parties during incidents among the surveyed banks. This practice is crucial for effective incident management and communication, ensuring that external parties receive accurate and timely information about the incident's status, impact, and resolution. Having a designated spokesperson helps maintain transparency, manage public relations, and establish trust with customers, regulatory authorities, and other stakeholders during challenging situations.

3.9.3 Communicating Findings and Recommendations to Stakeholders

It appears that 82% of the surveyed banks have predefined communication channels and templates for notifying stakeholders during incidents. This practice demonstrates a proactive and organized approach to incident response and communication. Having predefined channels and templates streamlines the communication process, ensuring that stakeholders receive consistent and accurate information in a timely manner. It also helps maintain professionalism and clarity in communication during high-stress situations, such as security incidents. This high percentage indicates that the majority of banks recognize the importance of structured and effective communication when dealing with incidents that may impact external stakeholders.

Organizations employ various methods and practices to effectively communicate findings and recommendations from post-incident reviews to relevant stakeholders, as outlined by the responses from banks. A substantial portion of banks (55%) adopt a structured approach by generating comprehensive Post-Incident Review Reports, summarizing key information and action items objectively. Around 15% of organizations utilize templates and visual aids like graphs and charts to enhance the clarity and completeness of their reports. Ensuring accessibility to stakeholders from diverse backgrounds, 10% of banks prioritize using clear and simple language. Additionally, a few banks (10%) highlight positive aspects of incident responses and include feedback from stakeholders. Furthermore, 30% of organizations publish these reports on centralized platforms for easy access and transparency, while a similar percentage (30%) prefer email communication for sharing findings and recommendations. A good number of banks (40%) provide incident reports and conduct detailed meetings to convey post-incident review information, and a smaller percentage (15%) maintain Knowledge Databases for documenting and sharing incident-related insights.

3.9.4 Communication Channels and Methods to Keep Customers Informed

Organizations employ various communication channels and methods to keep customers informed during incidents, with different percentages of banks mentioning each approach. Email emerges as a widely adopted method, with 75% of banks using it to provide detailed and formal updates to customers. SMS is another prevalent channel, mentioned by 60% of banks, enabling quick and direct communication. Some organizations (25%) utilize social media platforms for real-time updates and engagement. A smaller percentage of banks (15%) occasionally resort to newspaper publications, while a few (5%) opt for traditional media channels like TV or print media to reach a broader audience and convey incident-related information. These diverse communication methods reflect the effort to ensure that customers stay informed during incidents through channels that suit their preferences and needs. These percentages represent the relative frequency with which each communication channel or method was mentioned by the surveyed banks. The mentioned methods collectively showcase various ways organizations keep customers informed during incidents, with SMS and email being the most commonly used channels.

3.9.5 Addressing Legal and Regulatory Requirements

In addressing legal and regulatory requirements within incident response procedures, organizations typically employ a comprehensive approach. This involves ensuring compliance with applicable laws, regulations, and industry standards (85%), meticulously documenting all actions taken during incident response (75%), promptly reporting incidents to relevant authorities and affected parties (85%), following legal guidelines for preserving digital evidence (60%), seeking guidance from legal experts or departments (30%), safeguarding sensitive data in accordance with privacy laws (50%), maintaining a clear chain of custody for collected evidence (80%), adhering to regulatory reporting timelines (70%), retaining incident-related records (65%), and assessing compliance with legal obligations in post-incident reviews (65%). These measures collectively address legal and regulatory considerations, playing a pivotal role in minimizing legal risks and upholding compliance with pertinent laws and regulations.

3.10 Incident Documentation

3.10.1 Standardized Format for Documenting Incident

The findings indicate that a significant majority, approximately 90%, of banks in Bangladesh have adopted some sort of format for documenting incident details and response actions for future reference. This high level of adoption suggests a proactive approach to incident management within the banking sector in Bangladesh. The use of standardized documentation formats is a best practice in incident management, as it helps ensure consistency and clarity in recording incident information and response actions. It also facilitates post-incident analysis and review, which can be crucial for learning from past incidents and continuously improving incident response procedures. The fact that such a large proportion of banks in the country have embraced this approach emphasizes the importance placed on robust incident management practices in the financial sector and highlights a commitment to enhancing cybersecurity and risk management efforts.

3.10.2 Software for Documenting Incident

On the other hand, the statistic that only 27% of banks use software for documenting incident details and response actions for future reference indicates a relatively low adoption rate of specialized incident management software within the banking sector. This suggests that a majority of banks may still rely on manual or less automated methods for recording and tracking incidents. It's worth noting that using dedicated incident management software can offer several advantages, such as streamlining the documentation process, enhancing data security, providing real-time incident tracking, and facilitating more efficient incident analysis. Banks that have not yet adopted such software may want to consider its implementation to improve their incident management capabilities, enhance compliance with regulatory requirements, and ultimately bolster their overall cybersecurity posture.

In the context of incident documentation practices, a comprehensive range of information is typically included by a varying percentage of banks. Incident details and descriptions are universally documented by all banks, representing 100% of the institutions surveyed. Meanwhile, 75% of banks detail actions taken during response. However, affected assets and vulnerabilities, as well as the timeline of events and threat actor details if known, are documented by only 25% of the banks. The majority, 86%, focus on capturing lessons learned and recommendations. Legal and regulatory compliance efforts, along with final incident status and review details, are also reported by a quarter of the banks. Incident time, date, and methods used in detection and response are noted by 25% of the institutions. Additionally, certain aspects such as impact and business impact, root cause analysis, scope and impact, immediate action, detailed investigation and findings, business unit affected by the event, controls that failed or did not exist, recommendation for future recurrence, and incident resolution time, are reported to varying degrees, ranging from 14% to 29%. This diversity in documentation practices underscores the importance of tailoring incident reports to meet the specific needs and priorities of each institution.

3.10.3 Retention Periods for Incident Records

The retention periods for incident records among the surveyed banks vary considerably, with different institutions adopting distinct approaches.

A notable portion of banks, constituting 10%, opt for perpetual or permanent retention of incident records, emphasizing their long-term significance. Another 10% retain these records specifically for learning and audit purposes, subject to a maximum retention period of up to 20 years. Meanwhile, 10% have not specified a defined retention period, while the same percentage ensures that incident records are never erased. Additionally, 10% of banks follow their data retention policies to determine retention periods, and 10% retain incident records for one year before archiving them. Notably, no banks fall into the category of having a variable retention period, and none have specified no retention period, as they are either in the process of formulating data retention policies or awaiting external regulatory guidance.

3.11 Continuous Improvement of Incident Management Process

The survey findings demonstrate a strong commitment to continuous improvement and learning within the surveyed banks in Bangladesh regarding incident management practices. Some 61% of the banks indicated that they regularly review and update their incident management processes in response to evolving threats and technology. This proactive approach is crucial in the ever-changing landscape of cybersecurity, ensuring that banks stay well-prepared to mitigate new and emerging threats effectively. Additionally, an equally impressive 61% of banks stated that they leverage lessons learned from past incidents to enhance their incident response processes. This indicates a mature incident management culture where the banks not only react to incidents but also take a proactive stance in learning from them to strengthen their defenses. A majority of the surveyed banks, constituting 70%, employ a multi-faceted approach to ensure the continuous improvement of their incident management practices. This includes measures such as regularly reviewing and updating incident response procedures, conducting post-incident reviews to identify areas for improvement, providing ongoing training to staff on emerging threats and response techniques, implementing lessons learned from previous incidents, and engaging in tabletop exercises and simulations to refine response plans. Additionally, these banks stay informed about industry-based practices and regulatory changes, collaborate with industry peers and security experts for insights and benchmarks, and actively participate in national cyber activities. These collective efforts underscore their commitment to enhancing their incident management capabilities and bolstering cybersecurity resilience in a rapidly evolving threat landscape.

3.12 Problems and Challenges Identified by Banks for Incident Management

The survey highlights several key problems, challenges, and obstacles faced by the banks, along with possible remedies. These remedies address the identified problems, aiming to enhance incident management, cybersecurity, resource allocation, and overall operational efficiency within the banks.

Table 4: Problems and Challenges Identified by Banks

Sl. No.	Problems and Challenges	% of Banks	Remedies
1.	Building Digital Competency within Organizations and Lack of Skilled Personnel	89%	Create a positive work environment and invest in training programs for employees to enhance their skills, facilitate digital adoption with a comprehensive training program, and allocate resources appropriately for ICT staff's training and knowledge sharing. An Institute like IDRBT, India, can be built in this regard.
2.	Vendor Relationship Management and Training Challenges	82%	Optimizing vendor relationships through effective communication, SLAs, training, and resource allocation. Vendors should make sure their resources receive training and stay updated on evolving ICT technologies.
3.	Digital Transformation and Change Management	78%	Ignorance, Improper Implementation, and Lack of Communication is a challenge. Stay informed about the latest technology trends through industry conferences and

Sl. No.	Problems and Challenges	% of Banks	Remedies
			seminars. Establish a communication matrix, and adhere to regulatory instructions and industry standards.
4.	Lack of Communication with Other Departments or Stakeholders for Incident Management	72%	Establish and document incident management processes, automating where possible. Hold regular meetings to facilitate communication and alignment; prioritize communication efforts; promote a positive learning culture; and involve staff in improvement across departments.
5.	Cyber Security Threats	74%	Invest in cybersecurity training and conduct regular security audits to identify vulnerabilities.
6.	Resource and Budget Constraints	52%	Carefully prioritize spending and focus on investments that provide the greatest Return on Investment (ROI).
7.	Existence of Legacy Systems	46%	Develop a plan to phase out legacy systems gradually and prioritize investments in compatible technology solutions.

Source: BIBM Survey

3.13 Expected Roles of BIBM for Incident Management

BIBM's close collaboration with banking professionals, its role in research and education, and its ability to facilitate knowledge sharing make it a key player in improving incident management practices in the banking sector. The percentage allocations represent the relative importance of each role in enhancing ICT emergency response and incident management practices. Here's a summary of the key roles and actions that BIBM can undertake (Table-5).

Table 5: Expected Roles of BIBM

Sl. No.	Roles of BIBM	% of Banks
1.	**Education:** BIBM can develop educational programs and curricula that cover both theoretical and practical aspects of ICT and security risk management. This includes offering courses and training that empower bank professionals with the knowledge and skills necessary for effective incident management. Organizing seminars and round-table meetings addressing non-technical decision-makers and inviting higher management personnel from banks can facilitate greater understanding of technology risk management and incident management practices. Offering specialized training programs on ICT emergency response and incident management can help standardize approaches and ensure that bank professionals are well-prepared to handle incidents.	92%
2.	**Research, Analysis and Publications**: Conducting more research and analysis on incident response and management can contribute to a deeper understanding of emerging threats and best practices. Publishing reports, books, and resources related to ICT emergency response and incident management can serve as valuable references for banks.	84%
3.	**Certification Programs**: Introducing need based certification programs ensuring international standard that validate the expertise of bank professionals in ICT emergency response and incident management can encourage continuous learning and adherence to best practices.	87%
4.	**Consultation and Advisory Services**: BIBM can provide consulting services to banks, including conducting assessments, audits, reviews, and offering recommendations to improve their ICT and security risk management policies, procedures, systems, and capabilities.	74%

Source: BIBM Survey

3.14 Expectation from Bangladesh Bank

The central bank's active involvement and leadership in these areas can contribute significantly to a more resilient and secure banking sector. The percentage allocations represent the relative importance of each role in strengthening ICT emergency response and incident management practices in banks. Here's a summary of the key roles and actions the central bank can take (Table-6).

Table 6: Expectation from Bangladesh Bank

Sl. No.	Roles of Bangladesh Bank	% of Banks
1.	**Setting Standards and Regulatory Oversight:** The central bank can establish Incident Management Guidelines and enforce standards for ICT and security risk management in banks. This includes maintaining regulatory oversight, conducting regular audits and assessments, and ensuring compliance with cybersecurity standards and regulations to uphold banks' policies, procedures, systems, and capabilities.	89%
2	**Information Sharing Hub and Collaboration:** Facilitating information sharing and collaboration among banks, regulators, law enforcement agencies, industry associations, and cybersecurity experts is crucial. This collaborative approach enhances awareness, prevention, detection, and response to ICT and security incidents. Establishing a dedicated hub for incident information sharing and forming a specialized incident management team to assist banks during incidents can greatly enhance response and recovery efforts.	86%
3	**Capacity Building and Contingency Planning**: The central bank can bolster its capacity for better regulatory oversight and develop contingency plans to address potential disruptions to its own/banking services or functions, with the aim of safeguarding the stability of the banking system.	81%

Source: BIBM Survey

3.15 Roles of the Government

The government's proactive involvement in these areas can significantly contribute to a more resilient and secure banking sector. The percentage allocations represent the relative importance of each role in enhancing ICT emergency response and incident management practices. Here's a summary of the key roles and actions that the government can undertake (Table-7).

Table 7: Expectation from Bangladesh Government

Sl. No.	Roles of the Government	% of Banks
1.	**Legal Framework**: The government can enhance and enforce legal frameworks governing ICT and security risk management in banks. This involves formulating and implementing standards, guidelines, best practices, and tools to assist banks in effectively preventing, detecting, and responding to ICT and security incidents.	69%
2.	**Coordination and Cooperation**: It is crucial to enhance coordination and cooperation among banks and various stakeholders, including the central bank, regulators, law enforcement agencies, industry associations, and cybersecurity experts. Information sharing, knowledge exchange, and collaborative efforts can collectively strengthen overall incident management capabilities.	86%
3.	**Training and Capacity Building:** Encouraging and facilitating capacity building initiatives, such as training and awareness programs for banks and their customers on cybersecurity can significantly improve preparedness and response capabilities.	81%
4.	**Research and Development Funding:** Allocating resources for cybersecurity research and development can foster the creation of innovative solutions and technologies, ultimately enhancing incident management.	64%
5.	**International Cooperation**: Collaboration with international organizations and governments can facilitate information sharing and the adoption of global best practices in incident management.	52%
6.	**Cyber Insurance Regulation**: The government may develop and regulate the cyber insurance industry to ensure that it aligns with the needs of banks and incentivizes proactive risk management.	42%
7.	**Awareness Building**: Issuing circulars and awareness messages to banks and the customers can help disseminate important information about emerging cyber threats and incident management practices.	71%

Source: BIBM Survey

3.16 Recommendations

ICT Incident Response Management in Bangladeshi banks is a critical concern given the increasing frequency and sophistication of cyber threats. Though the ICT Incident Response Management landscape in Bangladeshi banks has seen notable progress in recent years, with technological advancements and regulatory initiatives driving improvements, there is a pressing need for banks in Bangladesh to develop robust and coordinated incident response mechanisms to safeguard their operations and customer data. The challenges identified in the study underline the importance of continued proactive measures to enhance ICT incident response capabilities in the banking sector of Bangladesh.

The study raises various issues in the roundtable for discussion. Based on the observations and findings of the survey, secondary data analysis and accommodating the comments of roundtable participants, the study recommends the following:

1. **Addressing the Cybersecurity Awareness Gap:** Despite regulatory efforts, a significant lack of awareness regarding the importance of cybersecurity persists at all levels within banks, including both employees and board members. To bridge this gap and enhance the effectiveness of incident response, banks must foster a strong cybersecurity culture across the organization.

2. **Navigating the Rapidly Evolving Threat Landscape:** As cyber threats grow increasingly complex and elusive, Bangladeshi banks must remain agile to stay ahead of cybercriminals. This necessitates a steadfast commitment to continuous investment in advanced technology and comprehensive training programs.

3. **Enhancing Policy Quality and Ensuring Continuous Evolution:** While 58% of banks rate their incident management policies as "Good," the fact that 16% consider them "Poor" highlights the critical need for ongoing improvement. Alarmingly, 28% of banks update their policies only every three years, with some neglecting updates altogether. To strengthen their resilience against disruptions, banks must not only develop robust policies but also commit to their regular evaluation and refinement.

4. **Talent Shortage:** One of the significant challenges faced by Bangladeshi banks is the shortage of skilled professionals. The demand for such talent is high, and many banks struggle to attract and retain experts in the field. This shortage hampers the effective handling of incidents. Banks should invest in comprehensive training programs to upskill their existing workforce, focusing on cutting-edge technologies and incident response protocols. Collaborations with universities and professional institutes can help create specialized courses and certifications tailored to banking ICT needs. Offering competitive salaries and benefits packages is crucial to attract top talent and reduce turnover rates. Banks should also establish clear career progression paths to motivate employees and retain skilled professionals. Additionally, partnerships with global and local ICT firms can enable knowledge transfer and temporary deployment of experts for critical projects.

5. **Incident Reporting and Communication:** Bangladeshi banks have made progress in developing incident reporting mechanisms. Many banks have established dedicated teams to monitor and respond to security incidents. Moreover, they are required to report significant incidents to the Bangladesh Bank. However, the communication of incidents, especially breaches, to the public and customers, remains an area that requires improvement. Transparency in this regard is crucial to maintaining customer trust.

6. **Collaboration and Information Sharing:** Collaboration among banks, industry stakeholders, and government agencies is vital for an effective incident response ecosystem. Some banks have taken steps to foster collaboration by participating in industry-wide forums and sharing threat intelligence. However, there is room for improvement in information sharing to collectively defend against cyber threats.

7. **Regular Drills or Exercises of CIRT:** It appears that 33% of banks conduct regular drills or exercises to test the effectiveness of their ICT Emergency Response Team and incident management procedures. Conducting regular drills and exercises is a crucial practice in the realm of cybersecurity and incident response. Banks may enhance their incident response preparedness through regular drills and exercises.

8. **Alignment with the ICT Security Guidelines of Bangladesh Bank:** It is clear that there are several challenges facing banks in Bangladesh in fully complying with the ICT Security Guidelines Version 4 (2023), particularly in the context of incident management. About 16% of respondents rate their practices as "Fully Aligned," and 27% of banks consider themselves "Mostly Aligned." Furthermore, 39% of banks rate their practices as "Aligned," indicating a fundamental level of compliance with the guidelines, while another 18% consider themselves "Partially Aligned," suggesting some gaps in their incident management practices that need attention. While the bank has recognized the need to comply with the new ICT Security Guidelines Version 4, there are significant challenges related to time constraints, awareness among higher management, strategic alignment, and effective implementation. Banks may adopt appropriate strategies to align more closely with the new ICT Security Guidelines.

9. **Vendor Dependency:** It appears that all banks have a designated ICT Emergency Response Team in place, based on the response provided and banks typically manage their ICT Emergency Response Teams internally, without outsourcing any part of the team's responsibilities. But the level of reliance on service providers or vendors to handle security incidents varied among organizations. The majority, comprising 71%, reported a "Moderate" level of reliance on these external entities, 14% stated that they relied on

vendors "Slightly." Ten percent indicated a "High" level of reliance, while 5% reported relying on them "Extremely," signifying a very strong dependence on external support. Banks may maintain the right balance between internal and external resources for incident response.

10. **Proper Preparation to Follow Incident Response Process:** According to the data provided, the CIRT follows a well-structured incident response process, with varying levels of completion for each step. "Containment, Eradication & Recovery" phase is followed by 100% banks properly. The "Detection & Analysis" phase accurately followed closely, with 73% of the banks. This suggests that 27% banks do not give emphasis on detecting and analyzing incidents, which is fundamental for identifying the nature and scope of the issue. The "Preparation" and "Post-Incident Activity" phases each perfectly followed by 72% of banks. Adequate preparation is essential to have the necessary resources, procedures, and communication channels in place, while post-incident activities help organizations learn from their experiences and improve their incident response capabilities over time.

11. **Establishing SOC:** Based on the provided information, it appears that 44% of banks have established a Security Operations Center (SOC). Among those banks with a SOC, the number of employees working in these centers varies, with a minimum of 3 employees, a maximum of 12 employees, and an average of 7.8 employees. Averaging 7.8 employees suggests that many banks maintain moderately sized SOCs to address cybersecurity concerns effectively. Necessary actions may be taken for the establishment and operation of Security Operations Centers (SOCs) to address cybersecurity concerns effectively.

12. **Analyzing Incident Trends and Patterns:** The finding that 58% of the surveyed banks in Bangladesh analyze incident trends and patterns to enhance preventive measures is a clear indicator of a proactive and data-driven approach to cybersecurity. This practice is crucial for all banks in today's digital landscape, where cyber threats continually evolve and become more sophisticated.

13. **Digital Forensic**: The data reveals that only 20% of the surveyed banks in Bangladesh have a dedicated Forensic Team in place to assist professional forensic investigators. While a minority of banks currently have dedicated forensic teams, it's worth emphasizing the importance of investing in this capability, especially in an era where cybersecurity threats are on the rise. A dedicated Forensic Team can contribute significantly to the swift and effective resolution of incidents and the protection of both the bank and its customers. Banks may expand their digital forensic capabilities to improve their incident response.

14. **Incident Documentation Process and Retention Periods for Incident Records:** Only 27% of banks use software for documenting incident details and response actions for future reference indicates a relatively low adoption rate of specialized incident management software within the banking sector. This suggests that a majority of banks may still rely on manual or less automated methods for recording and tracking incidents. It's worth noting that using dedicated incident management software can offer several advantages, such as streamlining the documentation process, enhancing data security, providing real-time incident tracking, and facilitating more efficient incident analysis. Moreover, the retention periods for incident records among the surveyed banks vary considerably, with different institutions adopting distinct approaches. A notable portion of banks opt for perpetual or permanent retention of incident records, emphasizing their long-

term significance. Some banks retain these records specifically for learning and audit purposes, subject to a maximum retention period of up to 20 years. Few banks follow their data retention policies to determine retention periods, and some retain incident records for one year before archiving them. Banks may determine appropriate retention periods for incident records, considering the diverse approaches mentioned, streamline their incident documentation processes and enhance IT security.

References

Ahmed, S., & Salim, A. (2020). ICT Security Issues in the Financial Sector of Bangladesh: A Review.

Cooke, 2003. Learning from incidents. ResearchGate

Grance, T., Kent, K. & Kim, B. 2004. Computer Security Incident Handling Guide – Recommendations of the National Institute of Standards and Technology. Technology Administration, US Department of Commerce

Haque, A., & Mannan, M. (2020). Cyber Threats and Cybersecurity in Bangladesh: A Review on Banking Sector.

Hossain, M., & Rahman, S. (2019). Enhancing Cybersecurity in the Banking Sector of Bangladesh: A Policy Perspective.

Hossain, S., et al. (2022). Ransomware Attack on a Major Bangladeshi Bank: Lessons Learned and Future Implications. International Journal of Cybersecurity and Digital Forensics, 11(3), 32-44.

Islam, M. S., & Ahmed, F. (2019). Information Security Practices in Banking Sector: A Case Study on Bangladesh.

Jaikumar, V, 2002, “Organisations should build an incident response team”, ComputerWorld Canada, vol.9, no.16.

Kayworth and Whitten, 2010. Effective Information Security Requires a Balance of Social and Technology Factors. ResearchGate, MIS Quarterly.

Khan, S. M. (2018). Cybersecurity in Banking Sector of Bangladesh: Challenges and Policy Measures

Knight & Pretty (1996). The Impact of Catastrophes on Shareholder Value. The Oxford Executive Research Briefings

Kurowski and Fring (2011). https://www.researchgate.net/ publication/ 3361 33 279_ Information_Security_Incident_Response_Management_ in_an_ Ethiopian_Bank_A_Gap_Analysis_Completed_Research_Paper

Mitropolous, S., Patsos, D. & Douligeris, C. (2006). 'On Incident Handling and Response: A state-of-the-art approach', Computers & Security, vol.25, pp.351-370.

Murray, J. (2007). Analysis of the Incident Handling Six-Step Process. SANS Reading Room.

Northcutt, S. (1998). Computer Security Incident Handling, Step-by-Step. The SANS Institute

Rahman, M. H., & Bhuiyan, M. Z. A. (2017). A Study on the Impact of ICT in the Banking Sector of Bangladesh.

Saha, D. K., & Khan, M. J. H. (2019). Cybersecurity Threats in Banking Sector: A Comprehensive Study on Bangladesh Perspective.

Sikder, S. S., & Rahman, M. S. (2018). Strengthening Cybersecurity in Bangladeshi Banking Sector: Challenges and Way Forward.

Smith, S., & Jamieson, R. (2006). Determining Key Factors in E-Government Information System Security. Information Systems Management, 23, 23-32. https://doi.org/10.1201/1078.10580530/45925.23.2.20060301/92671.4

Turner, P. (2007). 'Applying a forensic approach to incident response, network investigation and system administration using Digital Evidence Bags'. Digital Investigation, vol.4, no.1, pp.30-35

Van Wyk, K. & Forno, R. (2001) Incident response. New York. O'Reilly.

West-Brown, M.J., Stikvoort, D. et al. (2003). Handbook of Computer Security Incident Response Teams (CSIRTs), Second Edition. Pittsburgh, PA, Carnegie-Mellon Software Engineering Institute.

Wiik, J., Gonzales, J.J., & Kossakowski, K-P. (2005). 'Limits to Effectiveness in Computer Security Incident Response Teams'. Twenty-Third International Conference of the System Dynamics Society. The System Dynamics Society, Boston, MA.

Whitman & Mattord, 2005. Principles of Information Security, https://www.researchgate.net/publication/200446660_Principles_of_Information_Security

Zhang et al, 2009. Are Incident Durations and Secondary Incidents Interdependent? Sage Journals, https://doi.org/10.3141/2099-05

www.bb.org.bd

Bangladesh Institute of Bank Management (BIBM)
Plot No.4, Main Road No. 1 (South), Section No. 2, Mirpur, Dhaka-1216
Tel: 48032091-4; 48032097-8, 48032104, E-mail: bibmresearch@bibm.org.bd; Web: www.bibm.org.bd

Price: BDT 300.00
USD 8.00