cyril amarchand mangaldas
ahead of the curve

Cyber Incident Response

A Cyril Amarchand Mangaldas Thought Leadership Publication

Cyber Incident Response
published by Cyril Amarchand Mangaldas.

This handbook has been updated till September 11, 2025.

Index

Summary Overview

This handbook highlights key considerations for cybersecurity and cyber resilience practices to be taken up by entities in India, including entities operating in the Banking, Financial Services and Insurance (**BFSI**) sector. It outlines the best practices to be followed by such entities for cybersecurity and cyber resilience.

In India, while there are primary laws governing data privacy, and guidelines issued by the nodal agency for cyber security and cyber resilience, sector-specific regulators, too, mandate certain requirements and standards to be maintained by their respective regulated entities. This handbook provides a comprehensive overview of cybersecurity measures and checks, broadly encompassing the obligations prescribed by the sector-specific regulators.

An entity must check several vital areas to ensure robust cybersecurity across its operations, which includes:

a. Technical controls;

b. Employee training;

c. Monitoring mechanisms;

d. Internal security measures; and

e. Resilience factors.

Entities must carefully consider obligations set out under law, including reporting obligations to regulators, persons impacted by the cybersecurity incident while dealing with a cybersecurity incident. Presenting a consistent picture while addressing concerns and informing regulators and stakeholders of remedial measures, is key to safeguarding reputation and building client confidence, while dealing with a cybersecurity incident.

5 things to do, upon becoming aware of a cyber incident taking place:

a. Activate containment measures to reduce immediate damage and prevent infiltration to connected systems;

b. Report to CERT-In and respective Regulators (defined herein) within 6 hours of detection;

c. Conduct forensic and root-cause analysis to reconstruct the sequence of events and capture attack vectors;

d. Prepare Impact Assessment Report to document the direct and indirect effects of the cyber incident; and

e. Maintain evidence and securely preserve system logs, network traffic records, access logs, and audit trails.

A checklist which provides a comprehensive step-by-step guide for implementing cybersecurity measures as outlined in this handbook has been attached as **Appendix A**.

Introduction

Cybersecurity refers to the practice of safeguarding hardware and software, utilised by entities, from malicious attacks by implementing technologies and strategies that prevent such attacks. The threat may include infiltration of viruses and malware, unauthorised access, hacking attempts or data breaches.

Entities across sectors handle vast volumes of sensitive customer and transactional data, making them highly valuable targets for threat actors. Cybersecurity incidents can result in financial losses, legal reporting obligations and liabilities, reputational damage and erosion of customer confidence.

A

Landscape

1. Law

Cybersecurity in the Indian BFSI sector is governed by a comprehensive set of laws – starting with overarching primary laws that apply to all entities across sectors, followed by sectoral guidelines and regulatory mandates specific to the BFSI sector. The framework operates on two levels: (a) primary laws that establish the foundational cybersecurity obligations for all entities in India; and (b) sectoral laws and regulations issued by the Reserve Bank of India (**RBI**), Securities and Exchange Board of India (**SEBI**) and the Insurance Regulatory and Development Authority of India (**IRDAI**) (collectively referred to as **Regulators**), which impose additional requirements specific to their respective regulated entities.

The Information Technology Act, 2000 (**IT Act**), is the foundational legislation in India, which applies to all entities in India that handle electronic records and digital transactions. Section 43A states that body corporates that possess and handle sensitive personal data or information, and fail to protect such data or information due to negligence in implementing and maintaining reasonable security practices and procedures, will be liable to pay damages as compensation to the affected person.

As per Section 70B of the IT Act, the Indian Computer Emergency Response Team (**CERT-In**) shall serve as the nodal agency for performing the following functions with respect to cyber security incidents:

a. Collection, analysis and dissemination of information;

b. Forecast and alerts;

c. Emergency measures for handing such incidents;

d. Coordination of response activities;

e. Issue guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, prevention, response and reporting; and

f. Such other functions.

Key compliances laid down by CERT-In are:

a. All systems must synchronise their clocks with Network Time Protocol (**NTP**) servers;

b. Cyber incidents (like data breaches, attacks, ransomware, etc.) must be reported to CERT-in within six hours of noticing the incident;

c. Entities must maintain logs of all Information and Communication Technology (**ICT**) systems for 180 days; and

d. Appointing a point of contact to liaise with CERT-in.

As per Section 70A of the IT Act, the Central Government shall designate an organisation of the Government as the national nodal agency for Critical Information Infrastructure (**CII**) Protection, which is the National Critical Information Infrastructure Protection Centre (**NCIIPC**). CIIs are those computer resources, the incapacitation or destruction of which, will have a debilitating impact on national security, economy, public health or safety. The Government shall notify any computer resource that directly or indirectly affects the facility of CII, to be a protected system. Some additional key compliances are:

a. Establish a Cyber Securities Operation Centre (**C-SOC**);

b. Establish a Cyber Crisis Management Plan (**CCMP**);

c. Conduct Vulnerability/ Threat/ Risk (V/T/R) analysis of the cyber security architecture at least once a year;

d. Nominate an officer as Chief Information Security Officer (**CISO**); and

e. Constitute an Information Security Steering Committee (**ISSC**).

S.No	Regulator	Guidelines
1.	RBI	Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices
2.	SEBI	Cybersecurity and Cyber Resilience Framework (CSCRF), 2024
3.	IRDAI	Information and Cybersecurity Guidelines, 2023

If an entity is regulated by multiple Regulators, it is prudent to ensure that the compliances mandated by the primary regulator are adhered to. Certain systems/ applications/ infrastructure/ processes that are exclusively used for specific regulated activities must comply with the guidelines/ compliances prescribed by the corresponding Regulator.

Chapter Summary:

a. *India's cybersecurity framework operates on two distinct levels: primary laws like the IT Act 2000 that establish foundational obligations for all entities, and sector-specific regulations by RBI, SEBI, and IRDAI that impose additional requirements on their respective regulated entities.*

b. *CERT-In serves as the national nodal agency requiring all cyber incidents to be reported within six hours of detection, mandating 180-day log retention, NTP server synchronization, and appointment of liaison contacts.*

c. *Multi-regulator entities must ensure compliance with their primary regulator's requirements while also adhering to sector-specific guidelines, with CII entities facing additional obligations including C-SOC establishment and annual V/T/R analysis.*

2. Customer Verification

Know Your Customer (**KYC**) is a critical cornerstone of operational security, regulatory compliance and risk management in the BFSI sector. By accurately verifying and continually updating customer identities, entities can comply with anti-money laundering and counter terrorism requirements, as well as mitigate the risk of fraud, impersonation and unauthorised transactions.

Accurate logging of customer information flow and touchpoints, both internal and external, is vital for proactively identifying potential threats and managing risks across the chain of transactions.

Customer due diligence, facilitated by enhanced processes and advanced technologies such as Artificial Intelligence (**AI**) and Machine Learning (**ML**), enables real time analysis of the submitted documents and helps prevent misconduct.

Chapter Summary:

a. *KYC is critical for operational security, regulatory compliance, and fraud prevention.*

b. *Enhanced processes using AI/ML enable real-time document analysis.*

c. *Accurate logging of customer information flow and touchpoints vital for threat identification.*

3. Vendor management

As digital ecosystems expand in the financial sector, vendor relationships and outsourced partnerships have become indispensable to operations. However, third-party vendors and outsourced partnerships represent critical vulnerable points as cyberattacks typically target weaker links in the supply chain to access sensitive financial infrastructure.

Outsourcing of activities to vendors does not diminish the entity's obligations. The entity shall remain responsible for the outsourced activity. The entity must ensure that the vendor employs a standard of care equivalent to what the entity itself would, had the activity not been outsourced. The entity shall further ensure that the outsourcing of the activity to vendors does not impede its ability to carry out supervisory functions and objectives.

Prior to engaging vendors, the entity must conduct a comprehensive assessment of the need for outsourcing, including its potential benefits and risks.

An entity seeking to outsource an activity to a vendor must put in place a comprehensive outsourcing policy, specific for IT assets. Such policy shall incorporate oversight responsibilities, guidelines for selection and delegation of authority based on risks and materiality, business continuity and disaster recovery process, monitoring mechanisms of operations, termination process and exit strategies.

Before entering into an outsourcing arrangement with a vendor, appropriate vendor due diligence must be conducted to evaluate the vendor's ability to fulfil their duties and obligations as per the arrangement, without disruptions. A risk-based approach must be adopted while conducting the due diligence, taking into consideration the qualitative, quantitative, financial, operational, legal and reputational factors.

Independent reviews and market feedback on the vendor must be gathered during the due diligence.

Entities must ensure that their rights and obligations are crystallised with each of their vendors in clearly defined and legally binding written service agreements. These agreements must *inter-alia* include the following conditions/ clauses:

a. Description of the activity being outsourced;

b. Appropriate service and performance standards for the vendor and any sub-contractor engaged;

c. Provision for regular monitoring and supervision of the vendor by the entity or a Regulator;

d. Confidentiality obligations of the vendor;

e. Transportability of data between the entity, vendors, customers and third parties, if required;

f. Resolution processes in the event of default or indemnity, outlining the specific remedies and recourse available to the respective parties;

g. Business contingency and disaster recovery plans;

h. Right to conduct audit and seek information by the entity; and

i. Contractual liability of the vendor for performance and risk management practices by it and it's engaged sub-contractors.

Chapter Summary:

a. Third-party vendors and outsourced partnerships represent critical vulnerable points in the supply chain as cyberattacks typically target weaker links to access sensitive financial infrastructure, making vendor security a systemic risk.

b. Entities remain fully responsible for outsourced activities and must ensure vendors employ equivalent standards of care, conduct comprehensive risk-based due diligence, and maintain ability to carry out supervisory functions .

c. Comprehensive outsourcing policies must include oversight responsibilities, selection guidelines, business continuity processes, monitoring mechanisms, termination procedures, and legally binding service agreements with specific performance standards and security obligations.

4. Organisational Preparedness

Implementing technical measures is foundational for effective protection of the sectors' integrity, operational continuity and reputation. Entities should implement comprehensive policies and other technical measures such as access control, real-time monitoring, and incident response protocols to reduce the risk of breaches and also ensure swift recovery from cyber-attacks, thereby minimising financial losses, regulatory penalties, and erosion of customer trust.

Adopting clearly defined and approved policies ensure that all aspects of cyber risk – prevention, detection, response and recovery – are governed by standardised procedures. Regulatory authorities require entities in the BFSI sector to operationalise certain policies as part of their governance framework. Some policies that are required to be implemented *inter-alia* include:

a. Information security policy;

b. Incident reporting and response policy;

c. Data privacy and protection policy, including regular testing and certification;

d. Business continuity and disaster recovery policy;

e. Risk assessment policy; and

f. Cyber crisis management policy.

Access Controls: Entities must implement stringent access management protocols that are based on a 'need-to-know' or 'least privilege' basis. Role-Based Access Controls (**RBAC**) must be granted as necessary with Multi-Factor Authentication (**MFA**) and periodic audits and reviews of access rights. Upon periodic audits of access rights, if the purpose of providing access has been completed, such access must be revoked. SEBI and IRDAI require their respective regulated entities to implement access control policies, while SEBI also mandates the maintenance of access logs for a minimum two years.

Migration controls and data localisation: Below are the compliances imposed by the Regulators on their respective regulated entities.

S.No	Compliances	RBI	SEBI	IRDAI
1.	**Data Localisation**	Applicable to payment system operators and payment data, to be stored in India only.	Processing and storage within the legal boundaries of India.	Record of policies/ claims made in India will be stored in data center's in India.
2.	**Data Migration**	Requirement of Data Migration Policy, which shall inter-alia include the following provisions: (a) sign-offs from business users and application owners at each stage, (b) maintaining detailed audit trails, etc.	Data migration policy specifying SOPs and processes for data migration while ensuring data integrity, completeness and consistency	Not allowed.

The aforementioned technical measures must be updated and developed regularly, basis the development of new and advance technologies and available cyberattack reports.

Chapter Summary:

a. *Technical measures form the foundation for protecting sector integrity and operational continuity, requiring comprehensive policies – access controls based on 'need-to-know' principles, Multi-Factor Authentication, and periodic access rights audits with prompt revocation when purposes are completed.*

b. Regulatory authorities mandate implementation of specific policies including information security, incident reporting and response, data privacy and protection with regular testing, business continuity and disaster recovery, risk assessment, and cyber crisis management policies.

c. Data localization and migration controls vary by regulator.

5. Learning

Constant learning and development, along with adaptive training and organisational awareness is crucial to tackle the continuously evolving cyber threats. Financial institutions must keep their personnel, processes and technologies up to date.

Constant upskilling of employees will ensure they remain the strongest line of defense against malicious attacks, protect financial data, support uninterrupted operations and sustain customer trust.

Some of the key best practices to propagate continuous learning and awareness include:

a. Regular training and cyber drills like cybersecurity awareness programmes, phishing simulations and incident response drills for staff at all levels;

b. Periodically review and update security policies, access controls, and monitoring protocols in line with global best practices and industry trends, ensuring they address emerging risks such as AI-driven attacks and supply chain intrusions;

c. Conducting organisation-wide awareness initiatives to promote cybersecurity as a shared responsibility; and

d. Creation of internal platforms for sharing real-time threat alerts, security tips and learning from past incidents to stay informed and engaged.

Chapter Summary:

a. Continuous learning and adaptive training programs are crucial for tackling constantly evolving cyber threats, ensuring financial institutions keep personnel, processes, and technologies current with emerging attack vectors and defense mechanisms.

b. *Constant upskilling of employees ensures they remain the strongest line of defense against malicious attacks, protecting financial data, supporting uninterrupted operations, and sustaining customer trust through informed security practices.*

c. *Best practices include regular cybersecurity awareness programs, phishing simulations, incident response drills, periodic policy reviews aligned with global trends, organization-wide awareness initiatives, and internal platforms for real-time threat sharing and learning from past incidents.*

6. Vigilance

Vigilance against cyber threats requires more than certain foundational controls. Financial institutions must implement robust external periodic audits, swift rectification actions and sophisticated technology to detect evolving threat patterns.

Cybersecurity audits are essential for detecting vulnerabilities, assessing risks, and ensuring compliance with security standards. CERT-In mandates that the frequency and the broad scope of audits are included in the annual reports of the entities. Further, entities are required to follow CERT-In issued audit related advisories and directions.

Entities are expected to carry out comprehensive audits, covering all aspects of their ICT systems at least once a year as per CERT-In – the frequency may vary basis the mandates of the relevant Regulator.

Sector regulators require the audits of regulated entities to be conducted at prescribed frequencies — ranging from annual reviews for most entities to biannual audits for select SEBI-regulated organisations. Certified auditors, typically empanelled with CERT-In or those which meet the IRDAI criteria, must assess both critical and non-critical systems. The assessment results serve not just regulatory compliance, but also as forensic evidence in potential dispute resolution.

The regulatory guidelines further mandate structured and timely reporting, for example:

a. RBI requires audit submission within one month of completion;

b. SEBI requires submission within one month of audit, with IT committee approval; and

c. IRDAI expects a signed report with comments within 90 days of the financial year's end or 30 days after completion of audit.

Entities are required to review the audit report and prioritize rapid rectification of identified vulnerabilities. Modern technologies have enabled evolved threat landscapes, which demand proactive solutions capable of identifying anomalies, fraudulent behaviours and emerging attack vectors before they compromise key assets.

AI-driven detection tools are recommended for monitoring large volumes of network and transactional data. These platforms use machine learning to uncover previously unseen attack patterns, flag deviations from baseline activities, and automate incident validation and escalation.

Vulnerability Assessment and Penetration Testing (**VAPT**) exposes weaknesses that may be exploited by adversaries, reduces existing risks and is a required regulatory compliance. It directly contributes to the constant improvement of the entity's security controls. Comprehensive VAPT programmes, with broad-level oversight and cross-functional review, position organizations to proactively defend against the latest threats and maintain robust operational continuity in an era of rising cyber risks. The requirements of VAPT by entities may vary, depending on the respective Regulators.

a. **Frequency**: RBI mandates Vulnerability Assessment for critical systems. It must be conducted bi-annually, while penetration testing must be carried out annually. SEBI mandates assessments twice a year for entities designated as 'Protected Systems' under the IT Act. Additional assessment should be carried out for components that have undergone significant changes.

b. **Timelines**: Best practices would be the closure of VAPT findings within three months. High-risk gaps must be closed within one month of report submission and all remaining gaps within the provided window, with exceptions documented and approved by the Information Technology Committee of the entity and addressed before the next scheduled VAPT cycle.

c. **Compliance and Oversight**: VAPT should ideally be performed in production environments. However, tests in environments mirroring the production environment are acceptable, provided the deviations are documented and approved. The closure of the findings of VAPT must be monitored and tracked by the IT committee. A risk register should be maintained and reviewed regularly by the IT committee.

d. **Reporting**: VAPT completion and remediation must be reported to the relevant regulator - RBI, SEBI, or IRDAI, as specified in the relevant sectoral guidelines.

Chapter Summary:

a. *Vigilance requires robust external periodic audits, swift rectification actions, and sophisticated technology to detect evolving threat patterns, with CERT-In mandating annual audit frequency reporting and compliance with issued audit advisories.*

b. *Comprehensive ICT system audits must be conducted at least annually by certified auditors, with sector regulators requiring specific frequencies ranging from annual reviews to biannual audits, serving both regulatory compliance and forensic evidence purposes.*

c. *Vulnerability Assessment and Penetration Testing (**VAPT**) programs expose exploitable weaknesses, with RBI mandating bi-annual vulnerability assessments and annual penetration testing, SEBI requiring twice-yearly assessments for Protected Systems, and best practices calling for closure of findings within three months.*

B

Detection and Analysis

1. Identify

Early identification of threats is imperative for cybersecurity. An undetected breach in one entity can cascade systemically, threatening the stability of the entire financial ecosystem.

IT systems operated by entities are required to operate continuous, real-time monitoring systems across their networks, endpoints and transactional nodes. Typically, security operation centres (**SOCs**) are deployed to detect anomalies, suspicious behaviour, and indicators of compromise at the earliest stage. These systems are integrated with global and domestic threat intelligence feeds for instantaneous updates on new attack vectors.

Some of the operational best practices of SOCs are:

a. **24x7x365 staffing**: SOCs must be staffed round the clock, via well planned shifts, ensuring that skilled analysts are always present.

b. **Flexible operational models**: Entities can staff SOCs with internal talent or outsource functions to managed security service providers with the requisite expertise and resources.

c. **Functional efficacy reviews**: SOC operations are subject to half-yearly functionality reviews, periodic internal audits to validate compliance, operational readiness and continual improvement.

d. **Enterprise-wide incident monitoring**: SOC is responsible for enterprise-wide surveillance of security incidents, with comprehensive record-keeping of every event.

Chapter Summary:

a. *Early identification of threats is imperative as undetected breaches can cascade systemically, threatening the stability of the entire financial ecosystem, requiring continuous real-time monitoring across networks, endpoints, and transactional nodes.*

b. *Security Operation Centers (**SOCs**) must operate 24x7x365 with skilled analysts, flexible operational models allowing internal or outsourced staffing, and integration with global and domestic threat intelligence feeds for instantaneous updates on new attack vectors.*

c. *SOC operations require half-yearly functionality reviews, periodic internal audits for compliance validation, operational readiness assessment, and enterprise-wide incident monitoring with comprehensive record-keeping of every security event.*

2. Activate Containment

Containment of a cyberattack is the highest priority in incident response to reduce immediate damage and prevent infiltration to connected systems. Containment strategy will depend on the type of cyberattack launched on the systems.

The following factors are considered when evaluating the containment strategy:

a. Impact on collection, storage and documentation of evidence of such attack;

b. Duration and extent of the containment process, including resources required and effectiveness; and

c. Any other adverse impact on operations and accessibility to services provided by the entity.

Adversaries may actively monitor such defensive measures and shift their strategies to avoid detection and containment. The cyberattack must be accurately identified and this may involve allowing the adverse activity to persist until the full extent of compromise can be determined. If new signs of compromise are detected after containment, the incident must be re-evaluated by returning to the technical analysis stage. Upon successful containment, evidence collected must be preserved for future reference or investigation by law enforcement agencies. Detection tools can also be evolved and adjusted, threat must be eradicated from the system, followed by a recovery and restoration.

Chapter Summary:

a. *Containment represents the highest priority in incident response to reduce immediate damage and prevent infiltration to connected systems, with strategy dependent on attack type and consideration of evidence preservation, resource requirements, and operational impact.*

b. *Adversaries may actively monitor defensive measures and shift strategies to avoid detection, requiring accurate attack identification that may involve allowing adverse activity to persist until full compromise extent is determined.*

c. *Successful containment requires evidence preservation for future reference or law enforcement investigation, followed by detection tool evolution, threat eradication from systems, and comprehensive recovery and restoration processes.*

3. Analysis

Identifying the root cause and enabling factors of a cyberattack is vital to prevent recurrence of the attack, fortify defenses and ensure compliance. Following the detection of a cyber incident, a thorough forensic analysis is required to be conducted to reconstruct the sequence of events, capture attack vectors, affected systems and identify methods utilised by the adversary. This may include examining logs, system configurations, user activities and network traffic.

A Root Cause Analysis (**RCA**) will examine which of the security controls failed, such as weak authentication, unpatched vulnerabilities, misconfigured APIs or inadequate monitoring, alongside human errors or procedural gaps. RCA also explores systemic enabling conditions, which may be human error, insufficient vendor controls, outdated software or architectural weaknesses that created the opportunity for the adversity to infiltrate or escalate such an attack.

An Impact Assessment Report must be prepared, documenting the direct and indirect effects of the incident, including financial loss, data loss, operational disruption, regulatory non-compliance and customer impact, to understand the severity of the attack.

Impact Assessment Report facilitates transparent communication with regulators and stakeholders, providing an objective and evidence-based summary of the

incident. The Report will also provide targeted remediation efforts, policy updates, risk mitigation strategies, and investment priorities to bolster cyber resilience.

Regulators require entities operating in the BFSI sector to perform an RCA after the incident and submit the Impact Assessment Reports.

Chapter Summary:

a. *Root Cause Analysis (**RCA**) examines failed security controls such as weak authentication, unpatched vulnerabilities, misconfigured APIs, inadequate monitoring, human errors, and procedural gaps, alongside systemic enabling conditions that created infiltration opportunities*

b. *Impact Assessment Reports must document direct and indirect effects including financial loss, data loss, operational disruption, regulatory non-compliance, and customer impact to understand attack severity and facilitate transparent regulator communication*

c. *Thorough forensic analysis reconstructs event sequences, captures attack vectors, identifies affected systems and adversary methods through examination of logs, system configurations, user activities, and network traffic to prevent recurrence and ensure compliance.*

4. Decision Making

Activity	Responsible	Accountable	Consulted	Informed
Detection of Incident	SOC Analysts	Chief Information Security Officer (CISO)	IT Operations, Incident Response Team	Executive Management, Legal Team
Initial Impact Assessment	Incident Response Team	CISO	Risk Management, Compliance Team	Board of Directors, Communications
Determine Severity Level & Classification	Incident Response Team	CISO	Business Unit Heads, Legal Counsel	Relevant Business Units, Regulators (if applicable)
Escalate Incident to Senior Management	Incident Response Lead	CISO	COO, CIO, Risk and Compliance Heads	Entire Leadership Team
Decision on External Notification Trigger	CISO, Legal Counsel	CEO or Chief Risk Officer	Regulatory Affairs, Incident Response Team	Regulators, Customers (if required)
Notification to Regulators and Authorities	CISO, Legal Team	CEO	Incident Response Team	All Relevant Stakeholders
Post-Incident Review and Reporting	Incident Response Team	CISO	Audit, Legal, Risk Management	Board of Directors, Regulators

5. Co-ordination

Cyber incident response cannot succeed if activities are conducted in isolation. Effective coordination between internal and external units of the entity is essential to comprehensively assess impact, make informed decisions and promptly contain threats.

An effective cross-functional internal response group must include:

a. Technical teams;

b. External advisors;

c. Business Units; and

d. Risk and compliance.

Appropriate external cybersecurity consultants, forensic specialists and vendor partners must be integrated into the response process as their expertise can accelerate root cause identification, provide additional resources and fulfil reporting requirements.

Impact assessment reports should be reviewed collaboratively by all stakeholders to incorporate diverse perspectives, verify findings, and align on mitigation strategies. This ensures a holistic understanding of the incident's consequences and facilitates unified communication both internally and externally.

Chapter Summary:

a. *Effective cross-functional internal response groups must include technical teams, external advisors, business units, and risk and compliance functions.*

b. *External cybersecurity consultants, forensic specialists, and vendor partners must be integrated into response processes as their expertise accelerates root cause identification, provides additional resources, and fulfils reporting requirements.*

c. *Impact assessment reports should be reviewed collaboratively by all stakeholders to incorporate diverse perspectives, verify findings, align on mitigation strategies, ensure holistic understanding, and facilitate unified communication, internally and externally.*

C

Responsive Actions – Detection and Response

1. Reporting

All cyber incidents are required to be reported to CERT-In and the respective Regulators within six hours of detection

2. Talking to stakeholders

Effectively communicating with stakeholders during a cyber incident is pivotal to managing reputation and fostering trust. Financial institutions must develop comprehensive public relations (**PR**) and stakeholder communication plans, including:

a. **Pre-Designated Spokespersons**: Identify and train official spokespersons authorised to speak on behalf of the organisation to ensure consistency and credibility.

b. **Tailored Messaging for Diverse Audiences**: Prepare communication scripts targeted at different groups — employees, customers, regulators, investors, media, and partners — with relevant information suitable for the needs and concerns of each group.

c. **Timing and Frequency**: Define optimal timing for disclosures that balance transparency with operational security, avoiding premature or delayed announcements.

d. **Collaborative Approach**: Coordinate with legal, compliance, and technical teams to ensure all statements are factually accurate and legally sound.

Chapter Summary:

a. Comprehensive public relations and stakeholder communication plans must include pre-designated trained spokespersons, tailored messaging for diverse audiences (employees, customers, regulators, investors, media, partners), and optimal timing that balances transparency with operational security.

b. *Communication strategies require collaborative approaches with legal, compliance, and technical teams to ensure factual accuracy and legal soundness, while avoiding premature or delayed announcements that could compromise response efforts.*

c. *Effective stakeholder communication during cyber incidents is pivotal to managing reputation and fostering trust, requiring consistency, credibility, and audience-appropriate information that addresses specific needs and concerns of each stakeholder group*

3. Maintain evidence

Proper evidence maintenance is critical for post-incident investigations, regulatory audits and potential legal proceedings. Entities must securely maintain system logs, network traffic records, access logs and audit trails generated during the incident.

Documented procedures must be implemented to maintain the integrity and authenticity of evidence from collection through analysis and storage.

Qualified cybersecurity forensic experts must be engaged to collect and handle digital evidence using tools and techniques that prevent data alteration or contamination. Evidence must be stored in controlled, access-restricted environments with proper encryption and backups to prevent tampering or loss.

Document evidence handling processes must be in accordance with the guidelines laid down by regulatory authorities, ensuring evidentiary standards are met for investigations and potential litigation.

Evidence must be promptly made available to regulators, law enforcement, or internal audit teams upon request, while maintaining confidentiality and privacy controls.

Chapter Summary:

a. *Proper evidence maintenance is critical for post-incident investigations, regulatory audits, and potential legal proceedings, requiring secure maintenance of system logs, network traffic records, access logs, and audit trails generated during incidents.*

b. *Qualified cybersecurity forensic experts must collect and handle digital evidence using specialized tools and techniques that prevent data alteration or contamination, with storage in controlled, access-restricted environments using proper encryption and backups.*

c. *Evidence handling processes must comply with regulatory authority guidelines, ensuring evidentiary standards are met for investigations and litigation, while maintaining confidentiality and privacy controls when making evidence available to regulators, law enforcement, or internal audit teams.*

D

Post-Attack Actions – Fortification

1. Business Continuity and Disaster Recovery Policy/ Framework

Business Continuity Plan (**BCP**) and Disaster Recovery Plan (**DRP**) are critical regulatory and operational requirements for the BFSI sector. These plans ensure rapid restoration of essential services and systems in the aftermath of cyber incidents, natural disasters, or other disruptive events. The Regulators mandate comprehensive, formalised policies that address every facet of continuity and recovery.

Effective BCP and DRP are indispensable in the BFSI, where downtime and data loss have far-reaching impacts on customers, partners, and market stability. These plans define not only how to recover from crises, but also how to minimise their likelihood and consequences. By aligning with the regulatory mandates and routinely testing response readiness, BFSI organisations can demonstrate resilience, protect reputational value, and assure regulators and clients of their commitment to safeguarding essential financial services under all conditions.

Chapter Summary:

a. *Business Continuity Plans (**BCP**) and Disaster Recovery Plans (**DRP**) are critical regulatory and operational requirements ensuring rapid restoration of essential services and systems following cyber incidents, natural disasters, or other disruptive events.*

b. *Effective BCP and DRP are indispensable in BFSI where downtime and data loss have far-reaching impacts on customers, partners, and market stability, defining not only crisis recovery but also minimizing likelihood and consequences of disruptions.*

c. *Plans must align with regulatory mandates and undergo routine testing to demonstrate resilience, protect reputational value, and assure regulators and clients of commitment to safeguarding essential financial services under all conditions.*

2. Systemic review and enhancement of cybersecurity

Regulators issue guidelines that mandate regular reviews and continuous improvement of cybersecurity and incident management policies as essential compliance measures. Regulators require organisations to establish comprehensive, robust documented policies and to periodically review and update these policies following events such as cybersecurity incident, significant system upgrades or regulatory updates.

After every cybersecurity incident or detection, entities are required to conduct a formal post-incident review. This should include a detailed analysis of what happened, an assessment of policy effectiveness, and clear identification of any gaps in detection, response, or recovery processes. Insights gained from these reviews must directly be incorporated as policy revisions, ensuring that new threats, vulnerabilities, and attack methods are accounted for.

Regulators require these reviews to be periodic and event driven. For example, entities must ensure that incident response plans, escalation protocols, log management procedures, and communication strategies reflect the insights gained from internal cases or sector-wide advisories. Such reviews often involve cross-functional participation from the IT, compliance, risk management, and business units, further enriching the process.

A continuous improvement cycle based on lessons learnt enhances organisational resilience, enables quicker recovery from future events, and demonstrates compliance with regulatory expectations for proactive risk management. By embedding this systematic review and policy enhancement process into their governance structure, entities ensure that their cyber defence posture remains adaptive, effective, and always audit-ready.

Chapter Summary:

a. *Regulators mandate regular reviews and continuous improvement of cybersecurity and incident management policies as essential compliance measures, requiring comprehensive documented policies with periodic updates following cybersecurity incidents, system upgrades, or regulatory changes*

b. *Post-incident reviews must include detailed analysis of events, policy effectiveness assessment, gap identification in detection/response/ recovery processes, with insights directly incorporated into policy revisions addressing new threats, vulnerabilities, and attack methods*

c. *Continuous improvement cycles based on lessons learned enhance organizational resilience, enable quicker recovery from future events, demonstrate regulatory compliance, and require cross-functional participation from IT, compliance, risk management, and business units for enriched processes*

3. Engaging experts

Engaging experts at the outset is pivotal for effectively managing cyber threats in the BFSI sector. Experts should be immediately looped in when any cyber incident is detected. They play a central role in assessing regulatory obligations, guiding communications, and shaping the response strategy to minimise exposure and reputational damage.

If engagement with ransomware attackers is contemplated — such as negotiations or payments - it is imperative to first consult legal and compliance advisors. This ensures that actions taken do not violate anti-money laundering or anti-terrorist funding laws, and that the organisation remains within regulatory and ethical boundaries. Legal teams may also advise on required notifications to regulators or law enforcement and help evaluate the risks and long-term consequences of any engagement.

By integrating experts into incident response and decision-making, BFSI organisations can confidently navigate complex threats, maintain compliance with financial crime regulations, and communicate effectively with regulators, stakeholders, and the public. This multidisciplinary approach offers protection, strategic clarity, and stability during periods of crisis — positioning experts as important contributors to cyber vigilance and response planning.

Chapter Summary:

a. *Immediate expert engagement is pivotal for effectively managing cyber threats, with experts playing central roles in assessing regulatory obligations, guiding communications, and shaping response strategies to minimize exposure and reputational damage.*

b. *Legal and compliance consultation is imperative before any ransomware engagement such as negotiations or payments, ensuring actions don't violate anti-money laundering or anti-terrorist funding laws while maintaining regulatory and ethical boundaries.*

c. *Multidisciplinary expert integration into incident response and decision-making enables confident navigation of complex threats, maintains compliance with financial crime regulations, facilitates effective stakeholder communication, and provides protection, strategic clarity, and stability during crisis periods.*

E

Conclusion

Hence, a cybersecurity management plan that includes proactive measures to mitigate incidents, regular updates and upgrades, and an effective response protocol can help organisations maintain a secure and reliable digital environment for business operations. As threat actors grow more sophisticated, a coordinated approach becomes critical to enable effective monitoring and response management. The approach will require several business functions to come together and prepare a comprehensive digital management system, where businesses can operate in today's times.

Based on industry best practices, the following are key actions that entities operating in the BFSI sector must implement to maintain robust cybersecurity:

a. Conduct proper KYC procedures;

b. Implement comprehensive cybersecurity and outsourcing policies;

c. Technical controls on security systems should be robustly implemented;

d. Constant learning and updating to ensure preparedness;

e. Vigilance initiatives through regular audits and reporting;

f. Setting up continuous monitoring facilities;

g. Periodic review and enhancement of cybersecurity; and

h. Engagement of experts.

F

Appendix A

Cybersecurity Implementation Checklist for BFSI Entities

This checklist provides BFSI entities with a comprehensive step-by-step guide for implementing cybersecurity measures as outlined in this handbook. Use this checklist to assess your current cybersecurity posture, identify gaps, and ensure compliance with regulatory requirements.

Legal and Regulatory Framework

a. Register with CERT-In and establish point of contact
b. Determine if entity qualifies as Critical Information Infrastructure (**CII**)
c. Review applicable Regulator guidelines (**RBI/SEBI/IRDAI**)
d. Establish compliance calendar for regulatory reporting requirements

Governance and Policy Framework

a. Appoint Chief Information Security Officer (**CISO**)
b. Constitute Information Security Steering Committee (**ISSC**)
c. Develop and approve Information Security Policy
d. Establish Incident Reporting and Response Policy
e. Create Data Privacy and Protection Policy
f. Implement Business Continuity and Disaster Recovery Policy
g. Establish Risk Assessment Policy
h. Develop Cyber Crisis Management Policy
i. Create comprehensive Outsourcing Policy for IT assets

Technical Controls and Infrastructure

a. Implement Role-Based Access Controls (**RBAC**) on 'least privilege' basis
b. Deploy Multi-Factor Authentication (**MFA**) for all critical systems

c. Synchronize all systems with Network Time Protocol (**NTP**) servers
d. Maintain ICT system logs for minimum 180 days
e. Establish data localization compliance as per Regulator requirements
f. Implement Data Migration Policy with proper sign-offs and audit trails
g. Conduct periodic access rights audits and revoke unnecessary access
h. Maintain access logs for minimum period as per regulator requirements

Monitoring and Detection

a. Establish Security Operations Centre (**SOC**) with 24x7x365 monitoring
b. Implement real-time monitoring across networks, endpoints and transactions
c. Integrate global and domestic threat intelligence feeds
d. Deploy AI-driven detection tools for anomaly identification
e. Conduct half-yearly SOC functionality reviews
f. Maintain comprehensive incident monitoring records

Customer Verification and Vendor Management

a. Implement robust KYC procedures with AI/ML enhancement
b. Establish accurate logging of customer information flow and touchpoints
c. Conduct comprehensive vendor due diligence before outsourcing
d. Execute legally binding service agreements with all vendors
e. Include mandatory clauses in vendor agreements (confidentiality, audit rights, liability, etc.)
f. Establish regular vendor monitoring and supervision mechanisms
g. Ensure vendor business continuity and disaster recovery plans

Training and Awareness

a. Conduct regular cybersecurity awareness programmes for all staff levels
b. Implement phishing simulations and incident response drills

c. Establish organisation-wide cybersecurity awareness initiatives
d. Create internal platforms for sharing threat alerts and security tips
e. Provide continuous upskilling opportunities for cybersecurity personnel

Audits and Assessments

a. Conduct comprehensive ICT system audits at least annually
b. Engage CERT-In empanelled or regulator-approved auditors
c. Submit audit reports within prescribed timelines to regulators
d. Conduct Vulnerability Assessment and Penetration Testing (**VAPT**) as per regulator frequency
e. Close high-risk VAPT findings within one month
f. Maintain and regularly review risk register
g. Conduct annual Vulnerability/Threat/Risk (**V/T/R**) analysis for CII entitie

Incident Response and Reporting

a. Establish Incident Response Team with defined roles and responsibilities
b. Report cyber incidents to CERT-In within 6 hours of detection
c. Report incidents to respective regulators within prescribed timelines
d. Develop containment strategies for different types of cyber attacks
e. Establish evidence preservation and forensic analysis procedures
f. Conduct Root Cause Analysis (**RCA**) for all incidents
g. Prepare Impact Assessment Reports for regulatory submission
h. Establish stakeholder communication plans and designated spokespersons

Business Continuity and Recovery

a. Develop comprehensive Business Continuity Plan (**BCP**)
b. Implement Disaster Recovery Plan (**DRP**)
c. Conduct regular BCP/DRP testing and validation exercises

d. Establish alternate processing sites and backup systems
e. Ensure vendor business continuity alignment with entity requirements

Continuous Improvement

a. Conduct formal post-incident reviews after every cybersecurity incident
b. Update policies and procedures based on lessons learned
c. Periodically review and enhance cybersecurity measures
d. Stay updated with emerging threats and attack vectors
e. Engage cybersecurity experts and forensic specialists as needed
f. Maintain compliance with evolving regulatory requirements

Critical Information Infrastructure (CII) Additional Requirements

a. Establish Cyber Securities Operation Centre (**C-SOC**)
b. Develop Cyber Crisis Management Plan (**CCMP**)
c. Conduct annual V/T/R analysis of cyber security architecture
d. Nominate officer as Chief Information Security Officer (**CISO**)

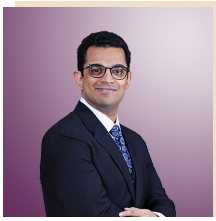
Gap Analysis and Action Planning

a. Conduct comprehensive gap analysis against this checklist
b. Prioritize gaps based on risk assessment and regulatory requirements
c. Develop implementation timeline with clear milestones
d. Assign responsible personnel for each action item
e. Establish regular review and monitoring mechanisms
f. Engage external cybersecurity experts for complex implementations

Note: This checklist is indicative and should be customized based on each entity's specific regulatory requirements, business model, and risk profile. Regular updates to this checklist may be necessary as regulations evolve and new threats emerge.

G

Contact Details



Arun S. Prabhu
Partner (Co-Head – Digital | TMT)
+91 99400 04080
arun.prabhu@cyrilshroff.com

Anirban Mohapatra
Partner
+91 87544 51778
anirban.mohapatra@cyrilshroff.com

Manmeet Singh
Partner
+91 98100 08779
manmeet.singh@cyrilshroff.com

Aditya Mehta
Partner
+91 98203 13945
aditya.mehta@cyrilshroff.com

Notes

Notes


24
AI
LOGIN

Offices of Cyril Amarchand Mangaldas

mumbai

Peninsula Chambers,
Peninsula Corporate Park,
GK Marg, Lower Parel,
Mumbai – 400 013, India
T: +91 22 6660 4455
E cam.mumbai@cyrilshroff.com

bengaluru

3rd Floor, Prestige Falcon Tower,
19, Brunton Road, Off M G Road,
Bengaluru – 560 025, India
T: +91 80 6792 2000
E cam.bengaluru@cyrilshroff.com

chennai

11th Floor, Awfis, Prestige Palladium Bayan,
No.43/1 (Door No.129 to 140), Greams Road, Egmore,
Chennai – 600 006
T: +91 44 4904 2874
E: cam.chennai@cyrilshroff.com

gift city

Office No. 501, 5th Floor, PRAGYA 2 Tower,
Road No. 11, GIFT SEZ area, GIFT City,
Gandhinagar – 382 355, Gujarat.
T: +91 79 6959 3500
E: cam.ahmedabad@cyrilshroff.com

abu dhabi

2459, Al Sila Tower, Abu Dhabi Global Market Square,
Al Maryah Island, Abu Dhabi, United Arab Emirates
(CAM Middle East)
E: cam.abudhabi@cyrilshroff.com

delhi-ncr

Level 1 & 2, Max Towers,
C-001/A,Sector 16 B,
Noida – 201 301,
Uttar Pradesh, India
T: +91 120 669 9000
E cam.delhi@cyrilshroff.com

ahmedabad

Block A-1512, 15th Floor, Navratna Corporate Park,
Ambli Bopal Road, Bodakdev,
Ahmedabad – 380 058, India
T: +91 79 3503 9999
E: cam.ahmedabad@cyrilshroff.com

hyderabad

Ground Floor, AWFIS Ohris Tech Park, Plot No.13,
Survey 64/2, (New) Software Units Layout, Madhapur,
HiTech City, Hyderabad – 500 081, India
T: +91 40 4433 4323
E cam.delhi@cyrilshroff.com

singapore

61 Robinson Road,
#11-03, Singapore – 068 893
T: +65 6329 2260
E cam.singapore@cyrilshroff.com
(CAM Singapore Pte Ltd., UEN: 202137213R)

www.cyrilshroff.com

www.cyrilshroff.com/blogs

cyril amarchand mangaldas

ahead of the curve