Guidelines on Cybersecurity Measures

13 MAY 2025

Fintech Association for Consumer Empowerment (FACE)
RBI-recognised Self-regulatory Organisation in the FinTech Sector (SRO-FT)

Version Control: Version 1.1 published with the Board's approval on 13 May 2025.

Table of contents

Context

We are issuing these guidelines[1] in the context of the government's advisory to businesses[2], including the BFSI sector[3] for cyber preparedness. In drafting this, we borrowed from government/regulatory authorities' advisories already issued and members' input.

Potential cyberattacks include ransomware, supply chain intrusions, DDoS[4] attacks, website defacement, data breaches, and malware attacks. They can also involve double extortion, data exfiltration, and the exploitation of unpatched vulnerabilities.

Threat actors particularly leverage supply chain attack vectors and exploit trusted relationships between companies and the value chain of technical service providers (TSPS). This layered structure introduces considerable complexity in detection and mitigation, making attacks challenging and dangerous to defend against.

We urge members and industry stakeholders[5] to implement these guidelines as necessary for their circumstances. For any suggestions/clarification, email to sro@faceofindia.org.

Basics

1. Implement all applicable controls prescribed in advisories issued by the government and regulatory authorities, particularly the Indian Computer Emergency Response Team (CERT-In)[6], as applicable and relevant.
2. Switch to heightened alert mode with operational 24/7 Security Operation Centre (SOC) and the Network Operation Centre to detect, respond to, and recover from cyber threats.
3. Enforce strict identity verification and authorisation for every access request, including from vendors. Restrict and monitor access to the critical systems. Maintain relevant personnel's contact list/call tree, including key IT service providers.
4. Implement a Zero-Trust security model in which no entity, whether inside or outside the company, is trusted by default.
5. Comprehensively document the IT asset inventory along with risk metrics.
6. Monitor and block IP addresses from sensitive geo-locations.
7. Deploy necessary mechanisms for security updates/emergency patches.
8. Put Business Continuity and Disaster Recovery Plans in place for business resilience.

[1] Approved by the FACE Board on 13 May 2025.
[2] https://www.cert-in.org.in/
[3] https://www.pib.gov.in/PressReleseDetailm.aspx?PRID=2127960
4 Distributed Denial-of-Service (DDoS)
[5] FACE has published these guidelines, and we welcome the industry to refer to and adopt with adequate attribution to FACE
[6] https://www.cert-in.org.in/

9. As per CERT-In directions, preserve all logs[7], take containment measures and report all relevant logs to incident@cert-in.org.in immediately.
10. Enhance oversight by the company's top management on cybersecurity and preparedness.
11. Conduct cyber drills to test the effectiveness of the Incident Response Plan (IRP) and Cyber Crisis Management Plan (CCMP), especially against data breach, ransomware, phishing, and DDoS attacks. Use identified gaps to update the CCMP.
12. Develop and implement a robust supply chain incident response plan, ensuring all stakeholders, including third-party vendors, know their roles and responsibilities during a breach.
13. Set up a communication channel with suppliers to promptly report suspected or confirmed security incidents, including data breaches or system compromises.
14. Create a prioritisation matrix and assess vulnerability, especially for public-facing resources. Club reachability tests[8] with vulnerability scanning for prioritisation.

Specifics

Threat Hunting

15. Conduct proactive threat hunting to identify and eliminate any compromise or persistence of threat actors in your systems.
16. Educate employees to be alert and report any phishing attempts, credential theft, or suspicious activities on organisational systems.
17. Use User and Entity Behaviour Analytics (UEBA) to detect deviations from normal behaviour (e.g. unusual login times, data access patterns).

Data Security

18. Encrypt database at file level and field level for regulated and PII data, depending on the sensitivity and criticality of data and infrastructure capability[9].
19. Classify data as critical and PII data to help with prioritisation.
20. Encrypt data in flight/transit.
21. Monitor data repositories for any dark data (e.g. data shared with the analytics department for building models but not being used now and not erased after usage) in the company.

[7] Ensuring NTP sync and log retentions in line with CERT-In advisory https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf

[8] Reachability defines the degree to which a given security vulnerability that is detected can actually be attacked and exploited to gain privileged access and directly or indirectly access critical to systems or data.

[9] In line with applicable industry standards e.g. PCI DSS

22. Leverage Data Loss Prevention (DLP)[10] tools for avoiding any sensitive data exposure.

Phishing

23. Monitor emails for phishing attacks. Report all phishing emails and ensure vigilance/reporting of phishing websites.
24. Ask employees to verify the sender's email address and domain for authenticity, hover over hyperlinks to ensure the URL matches the intended destination, and be cautious of emails that invoke urgency, fear, or seek sensitive information.
25. Educate employees to be alert and report any phishing attempts, credential theft, or suspicious activities on company systems.

Geo & Threat-Based IP Blocking

26. Monitor and block IP addresses and incoming traffic from high-risk countries[11] using a firewall or CDN geo filters, and implementing geo-fencing based on business requirements.
27. If the users/customers are all in India, then geo fence to the India region, so that nobody outside India can access.
28. Apply rate limiting and behavioural filtering to protect against IP spoofing or evasion techniques to bypass geo-filters.

Endpoint Protection

29. Enforce full-disk encryption on all employee laptops and desktops to protect data at rest (e.g. BitLocker, FileVault).
30. Mandate strong passwords and implement Multi-Factor Authentication (MFA) for device logins and critical applications.
31. Deploy Endpoint Detection & Response (EDR) solutions to monitor and respond to suspicious activity on employee devices.
32. Restrict administrative privileges and provide users with only the minimum access required to perform their tasks.
33. Automatically lock screens after a short inactivity and enforce secure lock screen settings.
34. Install and centrally manage up-to-date antivirus/anti-malware software.
35. Disable USB ports or enforce read-only mode unless required explicitly for work.
36. Use a centralised patch management system to regularly apply OS and software patches.
37. Prohibit installation of unauthorised software through application whitelisting or endpoint protection platforms.
38. Monitor endpoint logs regularly for abnormal behaviour or indicators of compromise.

---

[10] Data loss prevention is a security solution that identifies and helps prevent unsafe or inappropriate sharing, transfer, or use of sensitive data.

[11] If not critical to business

39. Implement mobile device management (MDM) for company-issued smartphones or BYOD devices.
40. Provide employees with VPN access for secure communication while working remotely.
41. Restrict access to high-risk websites using endpoint DNS filtering or secure web gateways.
42. Educate employees on phishing and social engineering through ongoing awareness training and simulations.
43. Maintain regular backups of important user data and configurations, stored securely and tested for recovery.

Web Server & Infrastructure Hardening

44. Protect web-facing information infrastructure, including web portals and websites, against DDoS attacks by implementing proper mitigation tools and considering clean pipe solutions from ISPs. If a patch is not possible, protect exposed systems using custom WAF or firewall rules.
45. Regularly examine logs of web servers and perimeter devices (e.g. WAF, firewall, DNS) to detect malicious requests or traffic.
46. Block all unused ports (e.g. 23, 445, 3389) on servers, firewalls, and cloud instances.
47. Disable RDP/SSH from the internet and only allow access via VPN or internal IPs.
48. Scan all web servers and infrastructure for open ports and known vulnerabilities (eg: use tools like Nmap, OpenVAS).
49. Remove or isolate unmaintained, old, or unused web applications and systems.
50. Apply the latest OS, software, and firmware updates across all systems.
51. Secure any servers in the company sitting outside the firewall and/or perimeter security.

Access Control, Network & System Protection

52. Enforce strong passwords (minimum 12 characters; no reuse).
53. Enable Multi-Factor Authentication (MFA) on email, VPN, admin panels, and cloud platforms.
54. Remove ex-employee access and disable all unused accounts.
55. Restrict admin privileges to essential personnel only.
56. Use VPNs or any other secure access methods for all remote access.
57. Segregate critical internal systems from vendor access via network segmentation.
58. Consider isolating third-party vendor networks from the company’s core infrastructure using dedicated VLANs or separate subnets, preventing lateral movement if a vendor's system is compromised.

Monitoring & Alerts

59. Enable login attempt alerts on sensitive systems (e.g. VPN, admin panels).
60. Monitor logs for failed login attempts, configure changes, and new device connections.

61. Block IPs showing brute-force activity using firewall or endpoint rules.
62. Watch for abnormal traffic spikes from foreign or domestic IPs, investigate and isolate if needed.
63. Implement External Attack Surface Management (EASM) Solutions, maintain up-to-date inventory of public-facing assets
64. Actively monitor for credentials, API tokens, and key leaks in the public domain and take immediate actions to rotate and protect them.
65. Implement an automated fraud detection mechanism for every transaction/sensitive database entry, if applicable.

Software Integrity & Code Review

66. Implement code signing for software and updates to ensure the integrity of the code provided by third-party vendors. Any unsigned code should be flagged as potentially malicious.
67. Perform regular code reviews and static analysis of third-party applications and components integrated into internal systems to detect potential vulnerabilities or malicious code.

Backup & Recovery

68. Regularly back up critical data and store in separate locations (offline[12] or cloud) with strong encryption. Implement necessary data backup mechanisms to restore operations in case of compromise or data loss.
69. Test backup recovery procedures periodically to ensure rapid restoration in case of a supply chain attack.
70. Ensure that backup systems are disconnected from the main network

Technology Providers[13]

71. Sensitise technology providers to adhere to cybersecurity practices and deploy high-quality manpower and standby teams for response.
72. Conduct regular due diligence for their cybersecurity posture, data handling practices, and compliance with industry standards (e.g. ISO 27001, SOC 2)
73. Implement a risk management program to continuously monitor and assess their security maturity, including subcontracted suppliers.
74. Enforce contract for security clauses requiring service providers to maintain robust cybersecurity measures, including incident reporting, access controls, and regular audits.
75. Implement strict access controls to limit vendors' access and use segmentation within internal networks to isolate third-party access from critical systems. Restrict vendors'

[12] Store geographically dispersed copies
[13] All technology providers like IT vendors/supplies, Managed Service Providers and their sub-contractors

access to sensitive data and infrastructure through secure channels (e.g. VPNs, Zero Trust networks).

76. Use multi-factor authentication and least privilege access principles to minimise exposure.
77. Monitor activities for anomalies in software updates or system configurations
78. Conduct simulated supply chain attack exercises to assess vulnerabilities in supply chain defence mechanisms.
79. Regularly test response plans and train staff to recognise suspicious behaviour from the service provider.
80. Perform penetration testing that mimics supply chain compromise scenarios, particularly focusing on the weakest links in service providers' integrations and third-party software components.
81. Mandate comprehensive, regularly updated SBOMs (Software Bill of Materials) and automatically analyse them for known vulnerabilities using trusted databases.
82. Establish a patch management program that prioritises patches based on risk assessment and works for the timely deployment of patches and security updates.
83. Monitor tech providers' updates for any signs of compromise (e.g., trojanised updates) before deployment to internal systems.

References

Key CERT-In advisories[14]

84. Technical Guidelines on SOFTWARE BILL OF MATERIALS.
85. CIAD-2025-18 on Essential Measures for MSME for Safeguarding Business Operations against cybersecurity threats, 9 May 2025.
86. CIAD-2025-19 on Essential Measures for Business for Safeguarding Business Operations against cybersecurity threats, 9 May 2029.
87. CIAD-2023-0036 on Cyber-attack campaigns against Indian websites and ICT infrastructure.
88. CIAD-2022-0023 on Responding to Ransomware Attacks.
89. CIAD-2021-0004 on Preventing Data Breaches/Data leaks.
90. Indian Computer Emergency Response Team (CERT-In)
    https://www.cert-in.org.in/
    Info@cert-in.org.in; +91 11-22902675
    Electronics Niketan 6, CGO Complex, Lodhi Road, New Delhi 110003 India

Others

National Critical Information Infrastructure Protection Centre (NCIIPC)

[14] These are available at: https://cert-in.org.in/

Fintech Association for Consumer Empowerment (FACE) is an RBI-recognised Self-regulatory Organisation in the FinTech sector (SRO-FT). FinTech companies of all kinds come together at FACE to build an industry that enables customer-centric financial services that are safe, suitable, and transparent, delivering positive impacts on society and the economy.