NABARD

Department of Supervision - Cyber Security and Information Technology Examination (CSITE)

Email Bulletin

Incident Management Awareness - Best Practices for Bank Security

1. In today's fast-evolving digital landscape, ensuring the security of systems and protecting depositors' money has become more critical than ever. As part of our ongoing commitment to cybersecurity, with the beginning of the new financial year 2025-26, DoS-CSITE, NABARD is sharing this important Cyber Incident Management Awareness Bulletin to help everyone understand procedures for identifying, responding to, and recovering from cyber incidents. This bulletin outlines how to align incident response efforts with the Cybersecurity Framework and ensure how to remain resilient against evolving cyber threats.

2. What is a Cyber Incident?

A cyber incident refers to any event that may threaten the confidentiality, integrity, or availability of the bank's information systems.

- Data breaches
- Ransomware and malware attacks
- Phishing and social engineering
- System intrusions or compromises
- Distributed Denial of Service (DDoS) attacks

3. Recognizing a Cyber Incident

It's crucial to be vigilant. An entity might encounter incidents such as:

- Unexpected system behaviour
- Suspicious emails (phishing)
- Unauthorized access attempts
- Slow or unresponsive systems
- *If anything unusual is noticed, please report it immediately!*

4. Immediate Action Steps

If the cyber incident is suspected/occurs:

- **Follow the Golden Hour Rule in Incident Management:** Report incidents immediately to the IT Security team via the designated reporting channel/email. As per the guidelines, incidents must be reported to CERT-In, NABARD, and RBI within **6 hours**, ensuring transparency and accountability.
- **Do not attempt to resolve the issue yourself** unless directed by the IT team.
- **Isolate affected systems** to prevent further spread (e.g., disconnect from the network).

5. Incident Response Process

Banks' response to cyber incidents follows a structured process that aligns with the Cybersecurity Framework:

- **Identification & Logging**: identify and log all incidents.
- **Assessment & Prioritization**: assess the incident to understand its scope and impact.
- **Containment**: isolate affected systems to minimize damage.
- **Eradication & Recovery**: remove threats and restore systems to normal.
- **Resolution & Reporting**: resolve the incident and communicate with stakeholders.

6. Individuals' Role in Cybersecurity

Bank staff's role in ensuring cybersecurity of the bank is critical.

- Report suspicious activities immediately via the designated reporting channels.
- Follow secure practices such as using strong passwords, avoiding clicking on unknown links, and regularly updating software.
- Stay aware of the latest phishing techniques and scam alerts to help identify potential threats.

7. Staying Prepared: Best Practices

To stay prepared for potential cyber incidents:

- **Participate in Cybersecurity Training**: Regular training ensures that updated on the latest threat vectors and the bank's security protocols.
- **Report Security Concerns**: If notice any unusual activity or encounter potential security issues, report them immediately.
- **Ensure Device Security**: Always lock work devices, avoid using public Wi-Fi for sensitive transactions, and follow the bank's security guidelines.

8. Educate Yourself and Others

Stay informed about the latest cyber security threats and trends.

- Attend training sessions and share knowledge with colleagues.
- A well-informed team is the first line of defence against cyber threats.

9. Compliance with RBI & NABARD Guidelines

The bank should follow the Cybersecurity Framework for its Supervised Entities

- Ensure that Cyber Incident Management Policies are regularly updated to align with RBI's/NABARD's/Govt of India's standards.
- Continuous monitoring of systems and proactive threat intelligence is a priority to prevent potential incidents.
- In case of financial fraud or a victim of cyber-crime, report at cybercrime helpline number 1930 or website https://www.cybercrime.gov.in

10. Continuous Improvement

Cyber threats are constantly evolving. To ensure that you stay one step ahead, regularly review and update cybersecurity protocols. An active participation is essential to strengthening defences and minimizing risk.

Remember: Cyber Security is Everyone's Responsibility!

CSITE, DoS, NABARD
HO, Mumbai
csite@nabard.org