Key Takeaways/Learnings

1. The importance of having a robust Cyber Crisis Management Plan (CCMP) was emphasized. Alongside this, moving towards risk-based assessments, conducting threat intelligence–driven red-teaming exercises, and on boarding to CERT-In's Cyber Swachhta Kendra (CSK) were highlighted as critical preparedness measures.

2. It was agreed that organizations must revisit their checklists and technical/administrative controls regularly to identify gaps and mitigate risks before they are exploited.

3. It was suggested that engaging with experienced Public Relations (PR) agencies is a good practice, so that, during a crisis, communication to stakeholders and the public is timely, consistent, and fact-based, thereby protecting trust and reputation.

4. The need for conducting regular spear-phishing simulation exercises was emphasized. Such drills help test awareness, validate existing controls, and strengthen the organization's resilience against targeted phishing campaigns.

5. It was highlighted that employee data are also important and must be treated with the same priority as investor and customer data. This should be explicitly reflected in the data protection and privacy policies of the organization.

6. Participants understood the importance of moving from compliance based to risk-based assessments, focusing on real threats instead of just box-ticking.

7. Incident reporting to CERT-In within six hours is non-negotiable under April 28, 2022 directions; log retention for 180 days and clock synchronization are essential for forensic accuracy.

8. Contracts with third-party service providers must enforce timely closure of VAPT observations and security responsibilities.

9. Threat-intelligence–based red-teaming exercises were emphasized as a proactive way to test defences against evolving threats.

10. It was agreed that maintaining cybersecurity hygiene among employees is critical, including training on identifying spam, understanding whitelisting practices, and verifying email gateways.

11. CERT-In also suggested about subscribing/ on boarding to its various initiatives such as regular alerts & advisories, Cyber Threat Intel Exchange Platform, Cyber Swachhta Kendra (Botnet Cleaning & Malware Analysis Centre), Empanelment of Cyber security auditors, Cyber security exercises and drills, assistance in development and implementation of sectoral Crisis Management Plans, National Cyber Coordination Centre (NCCC) for generating necessary situational awareness of existing & potential

cyber security threats to create a robust & resilient cyber secure environment over Indian cyberspace.

12. Early detection of anomalies through SIEM thresholds, EDR, and layered monitoring was acknowledged as crucial to effective containment. The importance of preserving the volatile evidence, using the order of volatility in forensics, and avoiding outdated practices like “pulling the plug.”

13. Network micro-segmentation was recognized as a key strategy to limit lateral movement and preserve logs for forensics.

14. Regular Vulnerability Assessment and Penetration Testing (VAPT) and Systems /Cybersecurity Audit help in performing risk assessment of the organization and also help in improving the cybersecurity posture of the organization by discovering the vulnerabilities within the network/ systems of the organization.

15. Snapshots and rollback mechanisms should be tested in staging environments before production deployments.

16. It was stressed that maintaining offline immutable backups (air gapped solutions) is necessary to ensure quick restoration of services and minimize operational downtime after a cybersecurity incident.

17. Organization should ensure that third-party/vendor organizations meet cybersecurity standards, which includes assessing and monitoring their cybersecurity practices to prevent the introduction of additional risks.

18. It was pointed out that a public response plan, including templates for media communication, should be pre-documented in an organization's Cyber Crisis Management Plan (CCMP) to ensure controlled messaging during incidents.

19. Segregation of duties (developers ≠ testers; IT staff ≠ security professionals) was strongly emphasized to avoid conflicts and ensure accountability.

20. A cybersecurity-conscious culture should be promoted within the organization, starting at the board level and regular training, awareness, and exercise programs should be encouraged for employees, executives, and board members.

21. It was concluded that organizations must operate under the mind set that cybersecurity breaches are inevitable, and hence, should invest equally in preventive controls (like MFA, RBAC, PAM, SIEM) and resilience measures such as RCA (Root Cause Analysis), regular self assessments, and active collaboration with SEBI and CERT-In initiatives.

22. Premature service restoration from backups without mitigation may result in reinfection and loss of forensic artefacts; mitigation must come first. Containment and security validation must precede BCP activation to avoid repeating failures.