Key Takeaways/Learnings

1) Participants understood that cybersecurity incidents must no longer be viewed as isolated technical events, but as enterprise-wide crises capable of simultaneously impacting operations, regulatory compliance, customer trust, financial stability, and organizational reputation.

2) Participants understood that cybersecurity incidents must no longer be viewed as isolated technical events, but as enterprise-wide crises capable of simultaneously impacting operations, regulatory compliance, customer trust, financial stability, and organizational reputation.

3) It was repeatedly highlighted that organizations must transition from a purely preventive cybersecurity mindset to an “assume breach” approach, where preparedness for detection, containment, response, and recovery becomes equally important as preventive controls.

4) Participants acknowledged that Cyber Crisis Management Plans (CCMPs) must remain actionable, operationally tested, and aligned to real-world attack scenarios rather than existing merely as compliance documents.

5) The need for regular table top exercises, ransomware simulations, and scenario-driven drills was strongly reinforced, as such exercises help build institutional “muscle memory” and improve decision-making during high-pressure incidents.

6) Participants recognized that governance and Board-level oversight are critical during high-risk cybersecurity decisions, particularly when business urgency conflicts with security assurance requirements.

7) It was underscored that the CISO function should act as a strategic risk advisor by ensuring proper risk visibility, structured escalation, and documented risk acceptance mechanisms instead of functioning only as a technical control owner.

8) Participants acknowledged that inadequate software and asset visibility significantly weakens an organization’s ability to respond effectively to emerging vulnerabilities and regulatory advisories.

9) The importance of implementing and maintaining an up-to-date Software Bill of Materials (SBOM) was strongly recognized, particularly for managing supply chain and third-party software risks.

10) It was observed that threat intelligence advisories from CERT-In and SEBI deliver value only when operationalized through predefined workflows, threat hunting activities, detection engineering, and incident response procedures.

11) 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.

12) Participants understood that proactive threat hunting aligned to adversary tactics, techniques, and procedures (TTPs) is essential for early identification of hidden compromise and lateral movement activity.

13) It was highlighted that phishing and credential compromise continue to remain among the most effective initial attack vectors against financial sector organizations.

14) Participants acknowledged that rapid reporting of suspicious activity by employees significantly improves containment effectiveness and reduces the overall impact of cyber incidents.

15) The need for continuous employee awareness initiatives, behavioural monitoring, and advanced phishing simulation exercises was repeatedly emphasized to strengthen organizational cyber resilience.

16) Participants recognized that privileged accounts represent critical risk concentration points and therefore require enhanced governance, least privilege enforcement, strong authentication controls, and continuous monitoring.

17) It was observed that incident classification should not be delayed until full business impact is confirmed; credible indicators of compromise should be sufficient to trigger formal incident management processes.

18) Participants acknowledged that containment actions during cyber incidents must carefully balance operational continuity with the preservation of forensic evidence and investigation integrity.

19) It was reinforced that ransomware response requires coordinated execution across technical, legal, compliance, communications, business continuity, and leadership functions rather than isolated IT response actions.

20) Participants understood that backup strategies must incorporate isolation, immutability, periodic validation, and restoration testing to ensure recovery readiness during ransomware incidents.

21) It was highlighted that restoring systems from unverified or compromised backups can significantly increase the risk of reinfection and prolonged operational disruption.

22) Participants recognized the importance of phased and security-validated Disaster Recovery (DR) and Business Continuity Plan (BCP) invocation instead of rushed failover decisions driven by operational pressure.

23) It was observed that customer data breaches introduce not only technical and operational concerns, but also significant privacy, legal, reputational, and regulatory implications.

24) Participants acknowledged that communication strategies during cyber incidents must remain synchronized, fact-based, and coordinated with regulators, CERT-In, and other stakeholders to avoid misinformation and public panic.

25) The growing role of misinformation campaigns, deepfake content, and coordinated disinformation during cyber crises was recognized as a significant emerging threat to institutional credibility and customer confidence.

26) Participants understood the importance of maintaining alternate communication channels during outages and DDoS attacks to ensure continuity of trusted communication with customers and stakeholders.

27) It was emphasized that ransom payment decisions involve complex legal, regulatory, operational, insurance, and reputational considerations and therefore require multi-stakeholder consultation and careful deliberation.

28) Participants recognized that payment of ransom does not guarantee successful recovery, prevention of data leakage, or removal of attacker persistence from the environment.

29) The importance of conducting comprehensive forensic investigations to determine attack origin, persistence mechanisms, lateral movement, and overall impact scope was repeatedly reinforced.

30) Participants acknowledged that supply chain compromise and third-party vendor weaknesses remain among the most significant systemic cybersecurity risks for financial sector entities.

31) It was highlighted that reliance solely on vendor certifications or compliance attestations is insufficient without continuous oversight, contractual security obligations, and independent validation mechanisms.

32) Participants recognized the importance of validating all third-party remediation tools, scripts, and updates within controlled environments before deployment into production systems.

33) The need for enhanced governance around change management, secure development practices, release assurance, and third-party software integration was strongly emphasized.

34) Participants acknowledged that pressure-driven recovery decisions may undermine long-term resilience if security validation and forensic scoping are bypassed for operational expediency.

35) It was reinforced that regulatory reporting under SEBI CSCRF should remain timely, factual, evidence-based, and aligned with prescribed reporting milestones including interim reports, mitigation updates, RCA submissions, and closure reports.

36) Participants understood that post-incident VAPT and assurance activities must extend beyond affected systems to include critical dependencies and adjacent exposure areas.

37) It was emphasized that Root Cause Analysis (RCA) should examine not only technical failures but also governance weaknesses, process gaps, delayed decision-making, inadequate monitoring, and third-party oversight failures.

38) Participants acknowledged that cyber resilience must be treated as a continuous improvement lifecycle involving periodic governance reviews, maturity assessments, resilience drills, capability enhancement programs, and lessons learned implementation.

39) It was underlined that organizations must operate under the mindset 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.

40) It was concluded that effective cyber resilience requires sustained alignment between people, processes, technology, governance, regulatory compliance, and communication capabilities across the organization.