Key Takeaways/Learnings

1. Cyber Crisis Management Plan (CCMP): CCMP document outlines a framework for dealing with cyber related incidents for a coordinated, multi-disciplinary and broad-based approach for rapid identification, information exchange, swift response and remedial actions to mitigate and recover from malicious cyber related incidents. Review of CCMP to be done by Boards.

2. Preparedness against “5 must haves”: One of the key requirements of CCMP, “Cyber Security Must Haves” indicates the basic cyber security fundamentals applicable to all the organizations. By deploying these Must Haves, organizations can defend against the most common form of basic cyber-attacks originating from the Internet as well as reduce the initial attack surface. Preparedness against “5 must haves” to be submitted to the Boards.

3. Onboarding to CERT-In services and indicator assessment for the Boards: CERTIn also suggested about subscribing/ onboarding 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.

4. The role of Board in cyber strengthening of the organization is multifaceted and crucial for an organization's overall cyber resilience. Board plays a pivotal role in shaping an organization's cybersecurity posture by providing strategic direction, oversight and accountability.

5. A governance framework that outlines roles, responsibilities and reporting structures related to cybersecurity should be established and maintained.

6. Board’s oversight of cyber risks & cybersecurity is vital for facilitating informed decision-making and ensuring that an organization is adequately prepared to protect itself against evolving cyber threats. It is strategic and governance matter that requires active engagement and commitment from the highest levels of leadership within the

organization. The Board should have proper understanding of organization's technical capabilities and processes.

7. Cybersecurity should be treated as a strategic enterprise risk rather than solely an IT risk. Board-management discussions about cyber risk should involve identifying and assessing the financial exposure to cyber risks, determining which risks to address through acceptance, mitigation, or transfer and developing detailed plans for each approach.

8. The organization should assess and review the current cyber readiness and conduct maturity assessment against a recognized framework.

9. The cybersecurity threat landscape is continuously evolving, and it needs to be ensured that cybersecurity receives the necessary investment, resource allocation, and cyber expertise acquisitions to address current as well as emerging threats adequately.

10. 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.

11. The Board should determine business-critical systems or "Crown Jewels" that need to be protected, conduct Crown Jewel Risk Analysis, training and awareness program for self & employees, conduct regular BCP-DR/ Recovery drills, cyber security resource allocation – funding and staffing and fostering cyber security culture within organization.

12. 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.

13. Organizations should engage with the media/social media regarding incident and crisis as per clearly defined policy of the utility, by nominating a spokesperson and synchronizing the public messaging with CERT-In, SEBI, key stakeholders and vendors to avoid contradictions and misinterpretations.

14. Ransom payment, in the case of ransomware/ data breach attacks, is a business decision and that needs to be made in consultation with National-CERT (CERTIn), regulator, Law Enforcement agencies and other relevant stakeholders.

15. Enterprise-wide risk management may encompass a risk interconnectivity analysis aimed at recognizing related risks, enhanced monitoring, threat intel from trusted partners & threat hunting during an incident may counter ripple effects of an incident and Board should be Co-Responsible along with CISO who should not be the only one accountable in dealing with cyber crisis.

16. As per CERT-In directions issued on 28th April 2022, it is mandatory report cyber incidents to CERT-In within 6 hours of noticing such incidents or being brought to notice about such incidents.

17. 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.

18. Cybersecurity is technology intensive, hence a culture of continuous improvement in cybersecurity practices & policies in response to evolving threats and technologies should be promoted. The Board should continuously reassess and help improve organization’s cyber posture.