sHeadline: A cyber security roadmap	
Source: Business Standard	**Date:** 11 Ocotber 2018

A cyber security roadmap

Many of our banks and capital market participants have cyber risk management plans at an institutional level. What is needed is an industry standard

VIKRAM LIMAYE

Emerging technologies and waves of digitisation have brought in their wake new challenges and exposed organisations to new risks. It is estimated that cyber attacks cost companies an estimated $500 billion in damages every year. Today, cyber risk is a top agenda item at the board level. With the cyber risk landscape changing fast and attacks becoming more frequent, severe and systemic, the primary concern facing organisations is that security breaches to technology and physical infrastructure could lead to data loss, financial losses, regulatory sanctions, reputational damage, operational disturbances, among other things. Increasing global interconnectedness and the complexity of systems make large-scale cyber attacks on financial market infrastructure even more pertinent and threaten the stability of financial markets.

The strategies adopted for cyber risk management currently focus on two objectives — one, reducing the risk of a cyber attack and minimising the impact of a breach, and two, building resilience, that is, detecting and recovering quickly from the impact of a breach. Globally, organisations are investing in developing a comprehensive set of cyber risk management capabilities that cover the entire value chain and ensure the risk is efficiently managed across the ecosystem. Some parameters of this risk management framework include:

- Cyber risk appetite: This refers to clearly articulated top-of-the-house qualitative statements and quantitative metrics to define the acceptance level of cyber risk.
- Risk quantification: This is about determining the severity and likelihood of cyber risk in monetary terms. Cyber risk quantification measures the value-at-risk (VaR) and helps in the assessment of the impact in financial terms. Cyber stress testing framework helps in identification and quantification of VaR under various scenarios.
- Dashboard: A digital cyber risk dashboard facilitates monitoring of metrics, escalation of risk alerts and supports management decision making. The dashboard's control effectiveness scorecards show the performance of control measures, the impact of control failures and ongoing investments in mitigating risks.
- Operating model: This refers to clearly articulated roles and responsibilities for cyber risk management across the three lines of defence in the organisation.
- Cyber risk playbooks: This includes a comprehensive set of response mechanisms and governance for cyber incidents linked to risk identification and remediation.

Traditional approaches to cyber risk mitigation have failed thus far and organisations are investing in identifying new approaches that include the use of advanced cloud-based SaaS services and platform-based approaches to security risks. Government institutions, such as NCSC in the UK and NIST in the US, have established cyber security centres and developed frameworks. Capital markets players are recognising that it is sub-optimal when institutions deal with cyber attacks in silos and many countries have put in place central agencies focused on cyber risk management.

Many of India's leading banks and capital market participants have a well-defined plan for cyber risk management at the institutional level. However, as an industry, we can all take a few steps to ensure greater effectiveness of our plans. We should consider adoption of a common set of standards by capital market participants. They should continuously strengthen IT governance, review policies, processes and systems to keep pace with changing risks and attack vectors.

Increasing collaboration among financial institutions is important. Traditionally, financial institutions have operated risk functions in silos. However, the nature of unknown threats today requires industry participants to work together. Industry — wide investment into a collaborative initiative would be the first step. A recent report by The Depository Trust & Clearing Corporation and Oliver Wyman, which includes discussions with 50-plus domain experts, concluded that effective response and recovery requires continued industry collaboration and, in some cases, common industry utilities and approaches.

On their part, Indian regulators have focused on cyber security as a core concern for several years now. Securities market regulator, the Securities and Exchange Board of India, issued guidelines on cyber security and cyber resilience to market infrastructure providers in 2015 and developed guidelines for registrars in 2017. In 2011, the Reserve Bank of India (RBI) issued comprehensive guidelines on information security, electronic banking, technology risk management, and frauds for risks emerging from digital adoption. In 2016, the RBI released a comprehensive set of requirements for internal cyber security frameworks.

The government has also undertaken initiatives including the Information Technology Act, 2000. It has set up the nodal cyber security agency, CERT-In, to respond to computer security incidents. The National Critical Information Infrastructure Protection Centre, is the central agency to facilitate safe, secure and resilient information infrastructure for critical sectors of the economy.

The author is MD & CEO, NSE