Cyber security considerations

Board Leadership Center (India)

Technology has revolutionised the way organisations operate and has paved the way for new opportunities. However, the extensive use of technology brings different set of risks and vulnerabilities which can lead to cyber threats. Cyber-attacks/threats can damage, disrupt, or steal information technology assets, computer network, intellectual property, or any other form of sensitive data. Cyber threats include computer viruses, data breaches, Denial of Service (DoS) attacks, unauthorised access and other such attacks. Cybers threats are complex and are an evolving issue with serious implications for companies, board of directors, investors and other stakeholders.

Cyber threats can arise from within an organisation by trusted users or from remote locations by unknown parties. Malicious employees can also collect large amounts of sensitive company information and remove it from company premises. They can also introduce malicious software which can corrupt company databases or sabotage network operations.

Therefore, organisations should develop effective and efficient cyber security polices and controls to address these kinds of risks. Cyber security deals with the safeguarding of systems, devices, programmes, and networks from cyber-attacks. Cyber security is not just a technical issue, it is an integrated approach to preparing, protecting, detecting and responding to cyber incidents.

In order to strengthen the cyber security landscape, there are regulatory requirements under the Companies Act, 2013 and Information Technology Act, 2000 (IT Act) requiring organisations to comply with cyber security norms. Additionally, the Government of India issued the 'Draft Digital Data Protection Bill, 2022' on 18 November 2022 to introduce IT rules, National Data Governance Framework Policy and a new Digital India Act. The bill provides greater emphasis and encourages organisations to digitise personal data. Further, in November 2022, SEBI has issued consultation paper on review of disclosure requirements for material events or information under SEBI Listing Regulations. The consultation paper proposes additional disclosures in relation to 'cyber security incident' or 'cyber security breaches' or loss of data/documents of a listed entity in the quarterly corporate governance report.

Security architecture and building trust

A cyber security architecture is the starting point for establishing a defence mechanism against cyber threats. It also ensures that all components of the IT infrastructure are protected. A cyber security architecture would help organisations to plan, implement and monitor their network security systems.

Environments that are secured by a cyber security architecture include cloud, networks, Internet of Things (IoT), endpoints and mobile. A well-developed cyber security architecture ensures that the main network architecture of the organisation, including its most sensitive data and critical applications, are fully protected against any existing or future threats or security breaches.

If cyber security architecture complies with the principles of the Zero Trust security model, an organisation would be able to secure data and IT resources. A zero trust approach puts user identity, access management and data at the heart of cyber security. It is an evolutionary cyber security approach and model that has been developing in response to the ever-expanding threat landscape. Zero trust is not a technology solution but a model and approach that requires a mindset shift based on three key principles: Assume nothing, check everything and limit access. More and more businesses are wisely turning to a zero trust mindset to restructure their cyber defences. The zero trust model consists of five main pillars being identity, device, network, application workload, and data. Each pillar also includes general details regarding visibility and analytics, automation and orchestration, and governance.

In today's business, trust is paramount. Business depends on fairness, integrity and transparency in the way information is collected and processed. Therefore, corporate leaders should also focus on digital trust. Digital trust refers to the confidence stakeholders have in the ability of an organisation to harness digital technology to protect their interests and uphold societal expectations and values. Cyber security and privacy play a key role in building and maintaining trust of stakeholders. Therefore, companies are working towards strengthening such areas.

Organisations are becoming data driven and risk resilient. Use of new-age technology brings new risks to the brand and profitability e.g. they could violate privacy policies as well as limit the capacity for autonomous and individual decision-making. Therefore, there must be a robust risk management policy in place, oragnisations must comply with the laws and regulations and consider privacy and security regulatory trends.

It is imperative to instill trust across multiple dimensions in order to implement emerging technologies such as Distributed Ledger Technology (DLT), quantum computing, 5G networks, Artificial Intelligence (AI) and Machine Learning (ML) technologies. Therefore, entities must embed security and privacy controls with transparency, reliability and integrity.

[1] The Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015
[2] As defined in Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Function and Duties) Rules, 2013.

Key considerations for the Audit Committees

Cyber security is among the most complex and rapidly evolving issue companies are facing these days. The Audit Committee's accountability for monitoring cyber security risk also increases as cyber threats are becoming more complex. Most corporate governance codes around the world provide that the internal control and risk management systems reviews are the responsibility of Audit Committees unless specifically handled by a separate board risk committee or by the board itself.

Audit Committees are expected to play a crucial role in providing guidance and ensuing there is sufficient governance and policy in place so that the organisations have strong cyber security defences. It's vital that Audit Committees comprehend the organisational risks and vulnerabilities connected to a distributed workforce, cloud usage, and accelerated digital transformation. Following are some of the key cyber security considerations:

Cyber security strategy and compliance management

Audit Committees and the board members should be aware of the cyber security trends. As cyber strategy is essential to building trust with key stakeholders, building a strong cyber strategy is challenging as the threat landscape is continuously evolving. Therefore, Audit Committees should ensure that the organisation is keeping up with the evolving threat landscape and has strategies in place to identify and mitigate risk. They should also ensure that the cyber security policies of the organisation are in compliance with all the applicable regulatory laws and regulations.

Regular trainings

Audit Committees should also ensure that the organisation imparts regular cyber security training to the employees to prevent cyber security leakages and to make them aware of the main forms of cyber security attacks and the ways to prevent them. This is because every personnel of the organisation is accountable with respect to their security responsibilities.

Risk assessment

Cyber threats should be considered as part of the organisation's risk management process, and the Audit Committee should test whether the organisation has adequate, effective and efficient controls and prevention measures against such threats and vulnerabilities.

Co-relation with Environmental, Social and Governance (ESG) factors

Considering the increase in the regulatory world to report on ESG parameters across all industries, there has also been a corresponding increase in reporting security breaches in the cyber environment since there is a demand for transparency as to how organisations use and protect the confidentiality and integrity of data. Therefore, the board should consider including cyber security parameters while reporting on ESG as this would promote the digital trust.

Penetration testing

Penetration testing refers to a testing method wherein testers target an application to determine whether vulnerabilities can be exploited to compromise the application, its data, or its resources. Audit Committees should inquire whether the organisation conducts penetration testing from an independent entity and actions taken against any vulnerabilities identified. The Audit Committee should also consider reviewing the findings and results of the penetration testing on a regular basis.

Assessment score card

The Audit Committee should undertake periodic reviews of the cyber security protocols established by the organisation by developing a cyber security score card to assess the volume of identified cyber incidents, the materiality and nature of cyber incidents and how they are being managed, key trends and to understand the happenings in the external environment.

Interaction with other committees

There must be frequent interaction between the risk management committee, internal auditors and audit committee in order to develop and monitor an effective cyber security programme. The Audit Committee plays a strategic oversight role of risk management activities and monitoring procedures related to cyber security.

Needless to say, organisations must develop a risk-based approach for cyber security as they can't protect everything and prevent all breaches. They must understand which data is of utmost importance to the organisation, where does sensitive data reside and who all have access to the same. Further, effective and efficient processes and controls should be established and implemented for developing a strong cyber strategy.

Questions for the Audit Committees

1. What aspects of the company's business and operations give rise to cyber security risk?
2. Does the company have a framework/programme documented for managing its cyber security related process, controls and actions against breaches? If yes, how often is the cyber security framework/plan reviewed?
3. Whether the cyber security breach has resulted from a material weakness or significant deficiency in internal financial controls?
4. Has the company performed a simulation to practice and evaluate cyber security breach protocols? How frequently are such simulation exercises performed?
5. Has the management identified the critical information assets which it wishes to protect against cyber-attack?
6. Whether a mechanism has been established for monitoring the effectiveness of the cyber security controls, including where appropriate, independently testing, reviewing and assuring such controls?
7. What are the results of the independent testing conducted and reviews performed? How was the deficiency dealt with?
8. Whether the data protection strategy of the organisation is in accordance with regulatory requirements?
9. Whether the budgets and funds earmarked for digital transformation and cyber security are sufficient considering the technological needs of the organisation?
10. In case of use of third-party or outsourced technology softwares, whether a third-party vendor assessment is being undertaken?

We would like to thank our Audit Committee council members for their time in providing us with their valuable insights and perspectives that have contributed to preparing this point-of-view document.

Audit Committee Council Members: Mr. Milind Sarwate, Mr. M.D. Ranganath, Mr. Narayanan Kumar, Ms. Revathy Ashok, Mr. S Madhavan, Ms. Sudha Pillai.

KPMG in India contacts:

Ritesh Tiwari
Partner
Board Leadership Center
E: riteshtiwari@kpmg.com

kpmg.com/in/en/home/social

30 years and beyond