Cybersecurity: What is the role of the Board?

Numerous industries have implemented a long-term remote working model that is still being followed in the aftermath of the epidemic. These new working models have made it possible to build a more globally connected infrastructure, which has increased the amount of data generated across borders, industries, and organizations.

Unfortunately, this has heightened cyber risk as thieves take advantage of every opportunity to commit cybercrime against individuals and enterprises. Cyber risk management, which spans people, processes, and technology, is now a must-have for any company hoping to thrive in a connected, digital world. No company, regardless of size or industry, is immune. Business leaders have become more aware of potential factors that could pose a risk to operations, reputation, or generate additional costs for the company. Boards of Directors play a critical role in ensuring that an effective plan is in place.

Including cyber risk on the Board agenda is one of the most effective strategies to lower the likelihood of a successful attack and the financial consequences of a breach. Here is what the Board can do:

Stop neglecting business risk: Many times, management ignores the business risk that cybercrime poses. In certain cases, this is because of the Board members' lack of understanding of the gravity of the threat posed by the current wave of industrial-scale cybercrime. Sophisticated criminals are continuously looking for new ways to steal or distort private data, and it is the Board's obligation to ensure that their business, customers, and employees are protected.

Devise ways to reduce the impact: Boards can have a significant impact on lowering the likelihood of a successful cyber-attack and lessening the reputational and financial consequences if one does occur. The Board's action can improve the outcome by reviewing cyber security risks and management at the Board level, preparing an incident response plan, and making cyber security a specific Board member's responsibility.

In the words of Anant Agrawal, Managing Director, Skillmine Technology Consulting, **"Cybersecurity threats are real and more pertinent these days. Organizations need to adopt countermeasures to prevent financial, reputational, and regulatory damages. Prevention and management are successful when a top-down approach from the Board members is applied – this enables the right defence mechanisms to be created to manage the menace of cybersecurity threats."**

Board governance to mitigate the risk: Board governance is necessary to reduce the danger of cyber-crime. A cyber attack's effect on a company is a strategic challenge that requires crucial Board leadership. Leaders have a role to play in the following:

Awareness: Board members must be aware of the threat that cyber-risks represent to them as top executives, including their personal information and the company's data. This necessitates a review of the value of data and cyber assets that are both vulnerable and attack targets.

Responsibility: While most businesses believe cyber-protection is the responsibility of the technology function or the CIO/CTO, the Board must take broader responsibility for ensuring the business is protected, so it is critical to either assign cyber-protection to a specific person or assign it to a committee.

Strategy: A focused strategy is needed that both replicate a potential attack and allows for a quick response plan that minimizes the impact on the business and its stakeholders.

Thus, it’s time for Boards to determine the steps that each member must take to control and minimize risk and losses and also identify which board member is best suited to overseeing cyber-security.