Cybersecurity and the Board bringing Cyber threats and Cybersecurity onto the Board Agenda

* Chaitanya Kunthe & Gautam Sashittal

Cyber-attacks and data fraud have consistently been in the top 5 risks as per the global risk report by the World Economic Forum (WEF). Cybersecurity is however not well understood by boards and appears infrequently on board agendas. Boards instinctively know that cyber risks are going to be key risks to address, especially with the acceleration of digitization and automation during COVID-19. Boards understand that there is this sceptre of cyber risks that needs management, but may not have the technical expertise to understand and manage these risks. Cyber security is therefore left largely to the technical experts, who in turn may not be able to influence board agendas in terms of cyber risks, the investment that needs to be made to protect the organization from these risks, and the state of cyber security preparedness. Boards increasingly want cyber risks to be a part of board agendas, but don't know how. It is not a skill or knowledge gap that makes it difficult, but the lack of clarity in knowing what cyber risks mean to the organization.

Cyber risk is the elephant in the room that needs understanding and management by board. It needs to come out of the realm of technical experts and appear regularly on board agendas.

Is your risk my risk?

This is no philosophical question. The WEF global risk report mentions 'cyber attacks' and 'Data Fraud or Theft' as the risks. If the board were to ask if they were vulnerable to cyber-attacks, the expected response from the CISO (Chief Information Security Officer) would be "depends, but yes."

Data fraud and data theft mean different things but often get clubbed together as a global top five risk. No wonder then, that boards find it hard to ask the right questions. Boards should correct this 'gap' before their organizations suffer a breach. And time is of essence.

Clear and Present Danger

The pandemic has exponentially increased cyber risks. National cyber security agencies recognize it and have had to come up with plans to tackle them.

Boards need to recognize that cyber threats change by the day, by the minute and need ongoing 24x7 monitoring and reporting. What worked yesterday will not work today. Are boards prepared for these ever changing scenarios? How can boards be assured on an ongoing basis that sensitive data is not compromised, that the company is not vulnerable to denial of access attacks that some external actor is not masquerading as us.

As cyber warfare tactics intensify, organizations that are classified as 'critical infrastructure' by nations have seen cyber-attacks grow. The size and complexity of attacks is increasing. They are more targeted. They increasingly pose Advanced Persistent Threats (APTs).

APTs refers to highly skilled cyber attackers, typically state sponsored, who have the time and resources to attack and stay in the compromised network for a long period of time. The recent use of network management SolarWinds is an example of a large scale APT attacks.

According to the New York Times, the SolarWinds hack which targeted US government agencies and private corporations may be even worse than officials first realized, with some 250 federal agencies and business now

believed affected.

Supply Chains and Attack Vectors

'Sunburst' is the name given to the massive attack on US government agencies and Fortune 500 companies in December 2020. The sheer resources and skills required for the advanced attack on some of the most secure companies in the world point to the direction of the source being a nation state. The attackers made use of a path that is difficult to exploit – the software supply chain.

What is software supply chain? It takes the work of many companies for us to get usable software on our computers. All these companies form a part of the 'supply chain'. These software companies regularly release updates to their software that either fix bugs or provide new features. If attackers can breach these companies, they can send malicious software as a part of a trusted update. This is what happened with Sunburst. It compromised the SolarWinds network management software used by the victim companies and got malicious files onto the victim networks.

Supply chain attacks are difficult. Once successful, attacks can go undetected for long periods of time. Hence the name - advanced, persistent threats. These attacks are designed and executed to work against the most protected of systems. They were successful against the air-gapped computer systems of Iran's nuclear project.

Board FUD, Risks and Budgets

Not every organization is a top-secret nuclear project or the keeper of government secrets. Most just need to get the basics right.

When boards start adding cybersecurity to their agendas, they are immediately beseeched with the biggest selling points of cybersecurity – Fear, Uncertainty and Doubt (FUD). First, boards should understand their cybersecurity risks, quantify the losses should these risks occur and then allocate resources for the same. This is easier said than done.

Boards have to understand cybersecurity as a business issue. What is the risk if the corporate email server gets affected by a virus and sends out spam to millions of people? It could lead to the email domain being blocked by antivirus and none of the corporate emails being delivered. It could lead to a trust loss when users receive spam from a corporate email they were slowly starting to trust. This translation is what the board should expect from a competent CISO.

What questions must the board ask?

There is no cheat sheet available. The board must ask the right questions. Here are some questions that can help any board make an initial assessment of their cybersecurity risks.

- What is our cybersecurity governance organization? What skills do we need? What do we have in house? What are our training requirements? What are our outsourcing requirements?
- What are our top 5 cybersecurity risks? What are our losses if they materialize? What are the chances of the risks materializing? How do we know if these are the top 5?
- Have we implemented a well-known cybersecurity framework? What is an ideal security framework for our industry? What are our peers implementing?
- How do we ensure employee awareness and involvement in cybersecurity? How do we measure it?
- What is our incident and breach response program? Do we have a cyber-crisis management plan? Have we tested it? How frequently do we test it? What is the role of the board and the senior management in these plans?
- How well are we monitoring cyber threats to our environment? How do we know we are doing a good job? How many threats have we protected against? How many got through?

On the agenda – Every time

Cybersecurity should be on the board agenda at every relevant meeting. Creating a sub-committee to manage cybersecurity may perhaps be warranted as well. The board should ask for plain speak from the management and have a clear risk map of cybersecurity to be able to make better decisions. ■

Mr. Chaitanya Kunthe is the COO of Risk Quotient, responsible for building and growing their cybersecurity consulting practice. He is also a consulting CISO to various organizations. He is a certified CISSP, CISA, ISO 27001 and ISO 22301 LA.

Mr. Gautam Sashittal is a Director at Risk Quotient. He has worked across diverse sectors and prior to to this was the CEO of the DMCC. A large part of his career prior to that was with the Royal Dutch Shell Group. He also serves as non-executive director on boards with focus on oil trading, hedge funds and trade finance.