Deloitte.

The changing role of the board on cybersecurity

Robust oversight ‘Now’ for a secure ‘Next’
2021

The Now: Cyber concerns for the Board in the 'New Normal'

The phrase 'cyber everywhere' has never been more powerful than it is in today's world of digitisation. Cyber is rapidly moving beyond the four walls of an organisation and is focusing on the IT environment, the products that they build, and the plants from where they operate. Every product an organisation creates, right from a wearable fitness device to a smart TV, has some element of cyber involved in the process. COVID-19 has compounded the omnipresence of cyber, as organisations move from data centre security to cloud security and expand their digital footprint through their digital transformation journeys.

In the current era, there is a greater demand for omni-channel platforms creating an optimal customer experience. The convergence of the physical and digital is crucial to build trust that enables meaningful human experiences. The Board should be aware that to create such human experiences, personal data is critical. They should ensure that the management has considered all local, regional, and international data usage regulations for this.

The pandemic led to vast amounts of sensitive data being exchanged digitally, along with a heightened use of personal devices and home networks. With the workforce being distributed and distracted, cyberattacks across platforms are increasing. Prominent examples include an American multinational consumer credit reporting agency's data breach that cost the CEO, CIO, and CISO their jobs.

A WannaCry attack caused worldwide damage estimated between **US$1.5-US$4.0 billion**, and an American multinational telecommunications conglomerate purchased a web services provider at a discount of **US$350 million** owing to the latter's data breach

As per the Sophos global cybersecurity report[1], ransomware attacks have targeted more than **80%** of Indian organisations and only **8%** of targeted organisations in India were able to prevent encryption of their data. Also, about **66%** of organisations whose data was encrypted had to pay the ransom amount demanded

[1] https://secure2.sophos.com/en-us/content/global-cybersecurity-results.aspx

These cyber breaches have prompted the Board and senior leadership to lay more emphasis on cyber risk. Boards have now started looking at cyber risk as an enterprise-wide risk management issue, rather than a pure IT security issue, owing to its firm-wide implications. With the ever-expanding boundaries of an enterprise with connected ecosystem of partners, suppliers, customers, and other third parties, organisations have also started looking at an extended enterprise risk management in the area of cybersecurity and data management.

In addition to the cost of a cyber breach, which itself can be staggering, there is also the added burden of various reputation and litigation losses that it can bring, along with the effect it can have on the overall functioning of an organisation. Take the recent example of the breach of the US government's treasury and commerce departments; while the extent of the impact is as yet unknown, cybersecurity experts are of the opinion that because the affected software touches several parts of a business, this breach is potentially devastating for organisations not just in the US, but across the globe.

Simply 'Being Aware' of cyber risks is not enough for the Board in this 'New Normal', which is why they need to understand the criticality of each breach and the steps being taken to mitigate it.

Cybersecurity oversight has now become the most important topic for the Board after strategic planning. However, one of the challenges that the Board faces includes the lack of a logical channel through which it can look at cybersecurity and compliance issues. This may lead them to under or overreact to certain cybersecurity breaches. However, there is scope to create awareness for the Board on the emerging cyber threats.

Key regulatory requirements

So far, the Board has been largely independent in its workings, but it is now time to oversee the internal audit and risk management teams, as well as other compliance teams, to cater to the all-pervasive and changing cyber risk landscape.

The role of the risk management committee has been brought forward by the Securities and Exchange Board of India's (SEBI) Listing Obligations and Disclosure Requirements 2015 regulation, and the Board must check if the committee meets frequently enough to discuss cyber risks, presents them to the risk office or information security office on a periodic basis, and addresses comments or asks from them adequately.

The Kotak Committee Report of 2017 on corporate governance, which was implemented by SEBI, has enhanced the role of the risk management committee to include cybersecurity. Additionally, it now requires the top 500 companies to look into this as a mandate and calls for an emphasis on cybersecurity concerns as part of the risk management committee review.

The Reserve Bank of India (RBI), in its recent circular, has mandated awareness training programmes for the senior leadership team and board of directors to familiarise them with the relevant cybersecurity concepts. It also mentions creation of an IT strategy committee to evaluate cyber and information security; though this has not been mandated under the Company's Act 2013 or SEBI. The RBI also issued a notification to all commercial banks informing them about an immediate requirement for a Board-approved cybersecurity policy that needs to be distinct from an IT or information security policy.

In US, the **Securities and Exchange Commission (SEC)** issued a guidance in 2018 on cybersecurity-related disclosures in an organisation's periodic SEC filers. In this guidance, the expectation of the Board is to better understand the cyber risk associated with that company and look at cybersecurity with the same urgency as other business and economic risks.

The SEC has also understood the importance of the 'tone at the top', as demonstrated by an important directive, that requires executive certifications regarding the design and effectiveness of disclosure controls encompassing cybersecurity matters. The percentage of public companies that have **appointed technology-focused Board members** has grown over the past six years **from 10% to 17%**; and while this is not mandatory, the legislation requires organisations to explain in their SEC filing whether such expertise exists on the Board.

Increased levels of cyber warfare, cyber political interference, and government demands for backdoor access to software and services have resulted in new geopolitical risks in software and infrastructure buying decisions. The Board, in consultation with senior leadership, may want to consider certain geo-political factors that impact partners, suppliers, and jurisdictions important to that specific company.

Keeping in mind all the factors above, it is clear that cybersecurity conversations need to be at the 'top of the mind' amongst the Board and have the primary role in all their discussions.

The next: Role of the board in cybersecurity conversations

Now that the importance of cybersecurity in the Boardroom has been established, the next step is to understand the exact nature of the role that the Board needs to play. In its role of oversight, the Board not only looks at the company's financial systems and controls but is also duty-bound to oversee its overall cybersecurity management, including appropriate risk mitigation strategies, systems, processes, and controls. From a governance perspective, one of the most important priorities for the Board is to verify that management has a clear perspective when it comes to how business will be affected and also has the appropriate skills, resources, and approaches in place to minimise the likelihood of a cyberattack and mitigate any damages that may occur. In some organisations, monitoring cyber risk is a Board responsibility, while in others, the oversight is under an audit or risk committee. The following are a few ways to create a strong ecosystem to enable cybersecurity decisions at the Board level:

Adoption of a cybersecurity framework

To assess a company's possible cybersecurity measures, one conceptual roadmap that Boards should consider is the Framework for Improving Critical Infrastructure Cybersecurity, released by the National Institute of Standards and Technology (NIST). In today's technology-driven world, all stakeholders of an organisation, including regulators, expect the Board to be aware of key cyber risks affecting the company. The evolution of these risks calls for a joint attention from the Board, senior leadership, internal audit, risk management, and cyber teams to address this enterprise-wide risk. The need of the hour is to hold the management accountable for not only creation of a cyber strategy, but also its implementation and monitoring. This feedback, which must be channeled back to the Board, should forgo jargon and be put across in a way that is easily intelligible by the Board.

Most cybersecurity strategies have moved from the flawed Castle-and-Moat security model to a **Zero-trust model**, as the world perimeter becomes non-existent in this cloud dominated, mobile-driven, and work from anywhere world. The Board should be up to date on these changing cybersecurity models and strategies, so that they can make more informed decisions when a cyberattack takes place.

Holistic enterprise level security

With more advanced dynamic and pervasive cyber threats faced by organisations today, the need of the hour is to have proactive enterprise-wide security solutions which comprise tools, policies and monitoring mechanisms to increase the overall cyber resiliency of the organisation. Organisations need to ensure that third parties such as business partners, contractors and other vendors who interact with them also maintain an acceptable level of cybersecurity. Finally, as industrial systems become more digital as part of Industry 4.0, such enterprise-level security programs should focus on the **IT/OT integration.**

Protection of crown jewels

With the advent of advanced adversaries, there will always be gaps in cybersecurity controls, which makes it impossible to protect everything. The best practice is to look at key assets or crown jewels (which may differ from one organisation to another according to industry-based regulations) and have risk or value-based governance mechanisms around it. These risk categorisations will be an important input to the cyber strategy and help the Board evaluate the risks to be accepted, mitigated, transferred, etc. It is important for the Board to have a mutual and trustworthy relationship with the management, which can be enabled by keeping an open and robust channel of communication.

Creation of cyber talent

Another area of Board oversight is to ensure that the management has the requisite skills and individuals for the appropriate job, which includes executive positions at the top. This is quite critical to implement the strategy put in place by the management. While initially the IT support function was entrusted with the duty of protecting the organisation from cyberattacks, several companies have now separated the IT and information security teams, as part of their governance strategy.

Finally, it is imperative to have a cyber expert on the Board to bring in some much-needed technical expertise, set the right 'tone at the top', and bring down the **Cyber Exposure by Design**. A cyber expert will also be able to understand the overall cyber landscape and probe the organisation's cyber compliance posture. While talking to the management about talent, it is also imperative for the Board to ask about **Human Layer Security (HLS)**, which is often overlooked in the clutter of the organisation's machine layer.

Inclusion of robust reporting mechanisms

If cybersecurity is to truly occupy an important place in the Board, there needs to be a quarterly or bi-annual reporting requirement on the effectiveness of the cybersecurity compliance programme in the organisation. Cyberattack simulations and other cyber gaming exercises are useful for the Board to identify possible vulnerabilities and measure the overall resilience of the system.

Cloud delivered security services

According to Gartner, the demand for cloud delivered security services is set to beat the total security market demand by a considerable margin[2]. The most common incarnations of cloud delivered cybersecurity are access management and managed security services. This new shift towards cloud delivered services is essential, as the latest threat detection technologies, activities, and authentication work with a lot of data and can be taxing for an on-premise set up.

Definitions

Zero-trust model
A security concept with a motive of 'Never Trust, Always Verify'. This concept says that instead of assuming everything behind the corporate firewall to be safe, we must assume a breach and verify each request, whether internal or external, as if it originated from outside the network.

Cyber exposure by design
Cyber exposure by design is a proactive approach, which includes incorporating cybersecurity from the outset into each aspect of your organisation to help avert cyber risks.

Human Layer Security (HLS)
Human Layer Security means having security controls with all humans, including employees and other stakeholders, by educating them of various security attacks, their affects and the ways to resolve them.

IT/OT integration
IT/OT integration is the end state sought by organisations (most commonly, asset-intensive organisations) where instead of a separation of IT and OT as technology areas with different areas of authority and responsibility, there is integrated process and information flow.

These essential transformations will ensure that the Board is kept updated on the key happenings in the cybersecurity realm and will enable them to make informed decisions for the organisation.

"While Boards do have a significant focus on cybersecurity, both from a compliance as well as an operational standpoint, they need to ensure that security and privacy is embedded and implemented by design at the start of any operational/digital transformation initiatives. One of the other important aspects is to ensure that the ecosystem that supports an organisation has efficient cyber strategies, governance, controls and mechanisms (such as adequate code reviews, RED Teams) in place. While the Board does have knowledge on cybersecurity, its members should be open to having an annual refresher training on the subject to stay up to date with new threats and strategies in the cyber space. Cybersecurity cannot be taken for granted, and the management should set aside an adequate amount for it from their annual overall organisational budget."

- Professor N L Sarda, Independent Director

[2] https://cio.economictimes.indiatimes.com/news/cloud-computing/global-cloud-based-security-services-to-grow-21-pc-in-2017-gartner/59159570

A ready reckoner for the Board's cybersecurity journey from 'now' to 'next'

To truly build cybersecurity into the Board's agenda, it is crucial that they have visibility and oversight of cybersecurity instances in the organisation. The following questions can be a good starting point for the Board to introspect on whether cybersecurity is getting the importance it deserves at the Board level:

- Are cyber-related matters looked at the enterprise level individually?
- If a cyberattack or a breach is reported, what is the typical time frame by which it gets reported to you? Do you get a clear visibility of the business impact owing to the breach from the senior leadership?
- What is the most common type of cyberattack noted? Have you recently seen an increase in **Account Take Over (ATO) or Business Email Compromise (BEC) attacks**?
- Has an increased use of **ML techniques in the proactive threat detection area** been put in place by the management? If yes, in which specific area have you seen its influence the most?
- With Board meetings increasingly being held virtually, how do you ensure the privacy of the meetings? Do you feel the need for a more hybrid model?
- Do you see a change in the buying decisions of the management for cyber solutions based on the geo-political risk landscape? How prepared is the senior leadership on this aspect?
- Has there been a focus on improving security reflexes of the organisation through Human Layer Security (HLS), which allows automatic prevention and detection of threats based on the communication patterns and behaviours?
- Post COVID-19, have you witnessed increased discussions between the board of directors and the senior leadership, including the CIO and CEO?
- Is there a well-defined ownership of cyber risk at the Board or management level? Is it delegated to an audit committee or under your direct governance? Is there a resilient contingency plan in terms of dealing with a possible cyber breach or a changing risk landscape?
- Has management evaluated the legal and regulatory implications of cyber risks and the responsibilities that you have as members of the Board in case of any breaches? Has the management considered all applicable laws/regulations and standards, and have they aligned their practices including, but not limited to, International Organisation of Standards (ISO), Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), National Institute of Standards and Technology (NIST), Sarbanes Oxley Act (SOX), and General Data Protection Regulation (GDPR), etc.?

- Is there a periodic review by the management to update the crown jewels changed during a given period of time or due to disruption?
- Does your organisation have cyber insurance? If yes, is the coverage sufficient? Is this in-line with your decision of which risk to avoid, accept, mitigate, or transfer?
- Has the management factored in risk with third parties, including outsourced IT and other partners in cyber strategy (including cloud service providers)?
- Does the management's cyber plan anticipate and adapt to changes quickly? For example, how is the cyber risk in the 'new normal' of remote working being addressed?

Definitions

Account takeover

Account takeover is a form of identity theft and fraud, where a malicious third party successfully gains access to a user's account credential.

Business email compromise

Business email compromise attacks are a form of cybercrime that uses email fraud to attack commercial, government, and non-profit organisations to achieve a specific outcome, which negatively affects the target organisation.

ML techniques in the proactive threat detection area

A data-driven approach of learning patterns of threats from data and using it to protect the organisation's assets from future threats.

Looking towards the future

It is evident that COVID-19 is not a passing storm that organisations can wait out before they return to Business as Usual (BAU), but something that has transformed the way we conduct our business entirely. Organisations need to be more agile in managing business and technology strategies and align cybersecurity in a proactive and holistic manner, with adequate Board oversight.

Shareholders elect a board of directors to represent their interests, and, in turn, the Board, through effective corporate governance, ensures that the management effectively serves the corporation and its shareholders. Ensuring the adequacy of a company's cybersecurity measures needs to be a critical part of a Board's risk oversight responsibilities.

Boards must ensure that the 'tone at the top' is conducive for robust cyber management programmes protecting key assets, and that there is regular reporting to the Board on all matters related to cybersecurity breaches. Even though cyber incidents and breaches cannot be eliminated, the level that they impact the entire organisation and its surrounding ecosystem can be minimised through secure, vigilant, and resilient cyber programmes, which inculcate the security aspect into every decision that the management takes (secure by design).

The acceleration of digitisation in the 'new normal', the spike in cyber breaches, and the recent regulatory requirements have revealed that cybersecurity is all pervading and a business risk that can be best understood by the Board and senior leadership only, which is why it is imperative that cybersecurity conversations get prime place in all boardroom discussions.

The role of the Board continues to evolve day-by-day, considering the ever-changing business and risk scenarios, and as we have seen, their responsibilities include providing oversight, insight and foresight, which gets in built in the governance role that the Board plays for an enterprise. However, at the end of the day, it is the Board's responsibility to create a 'culture of cybersecurity' across the organisation 'now', to hinder the progress of its adversaries and ensure accelerated growth of the business in their 'next'.

Connect with us

Rohit Mahajan
President - Risk Advisory
Deloitte India
rmahajan@deloitte.com

Gaurav Shukla
Partner and Leader, Cyber, Risk Advisory
shuklagaurav@deloitte.com

Deepa Seshadri
Partner, Risk Advisory
deseshadri@deloitte.com

Vikas Garg
Partner, Risk Advisory
vikasgarg@deloitte.com

Key contributors

David George

Deloitte.