EQUANTIIS

Cybersecurity: How Much Does the Board Know About it, and is it Enough?

Cybersecurity

Cybersecurity is paramount for any business enterprise or organisation in today's rapidly changing and digitally exposed world. Beyond this, the Board is responsible and accountable to ensure that the valuable and sensitive information assets of an organisation are protected at all times. Given other business priorities and challenges, the question remains whether the Board of Directors knows enough about the organisation's cybersecurity posture. If not, how do they ensure that they do know enough?

The tone at the top goes a long way in building a risk-aware culture in an organisation where individuals remain committed to protecting the confidentiality, integrity and availability of its information assets. The ideal leader leads by example. To do so, the leader has to be aware of the situation and know how to deal with it accordingly. Developing such a tone at the top can result in the percolation of the right message down the line. Today, one of the most significant risks to any organisation concerns the cybersecurity of its critical information assets.

The employees at the lower ends of the hierarchy look up to the top management for inspiration and encouragement. While the IT security or SOC (Security Operations Centre) teams might be capable of handling critical situations, they require unstinted support from the top as managing cyber incidents requires one to take prompt decisions. A cyber security-aware Board can prove to be an asset to the organisation and provide much-needed guidance to the lower rungs. Gartner predicts the increased role of boards of directors in ensuring enterprise cybersecurity and forecasts that approximately 40% of them will have a dedicated cybersecurity committee by 2025.

How the world is changing in a post-covid era!

Key drivers such as what is now known as the 'new norm' and the move to asynchronous working has introduced many technology challenges. Aside from the rush to equip the workforce with robust IT equipment and the need to develop new cultural responses to engaging the workforce remotely, the security risks are perhaps the most significant further issue.

Add into this, the notion that these 'almost urgent' changes to the corporate IT strategy were themselves, foundational catalysts for change and you can see why many organisations considered the pandemic as an accelerant to other transformational activities.

According to the recently published 'Gartner 2020 Board of Directors Survey', 69% of the Board of directors have accelerated their digital transformation journey and increased the IT/Technology budget significantly post COVID-19. The board members rate cybersecurity-related risks as the second-highest source of trouble, followed by regulatory and compliance risks for the enterprise.

Increased cloud adoption at a rapid pace is another challenge facing senior management. According to a McKinsey & Company report, approximately 80% of organisations would migrate 10 per cent or more of their workload to the public cloud or double the usage of cloud by the end of 2021. Increased cloud adoption will bring in new cybersecurity and data privacy challenges.

People, Process and Technology

What does the board need to know about its organisational cybersecurity posture?

Amongst the different types of risks that the Board has to deal with, cybersecurity risk has assumed enormous proportions today. It is admirable that technology is improving by leaps and bounds. Still, the flip side is that the number and intensity of cyber threats are also increasing at an astonishing rate. Therefore, it becomes imperative for organisations to develop a robust cybersecurity posture. No discussion on cybersecurity is complete without examining the role of people, processes, and technology.

1. People

When it comes to people, processes, and technology, the Board of Directors can be as vulnerable as the lowest level employee in the organisation. Threat actors are always on the lookout for loopholes to exploit. While it is essential to ensure that each employee in the organisation can handle cyber threats, the Board members themselves need to display a specific level of cyber awareness.

Malicious actors are sophisticated today and increasingly use advanced modalities of infiltration. They deploy spear phishing, BEC (Business Email Compromise), and social engineering instead of regular phishing, as they have realised that employees have attained a basic level of cybersecurity awareness.

While phishing remains the most commonly used modus-operandi by malicious actors, the instances of spear phishing and Business Email Compromise (both involving top management level employees) are on the rise.

Hence, ensuring that the top management is cyber vigilant has become a crucial ingredient of the overall cybersecurity posture.

People, Process and Technology

2. Process

The process is a critical aspect of cybersecurity posture that focuses on risk management, compliance, incident reporting, and audits. Proper risk management is possible only after identifying, assessing, and analysing the risk.

Risk assessment is critical to managing the process because it includes various types of risks that could arise; identifying these risks paves the way for essential control systems required to mitigate or avoid them. The Board members need to be aware of the cyber threats that could emerge in the future to provide the right kind of guidance down the line.

One of the most crucial aspects of risk assessment is incident reporting. The Board has to know the nature of attacks that have taken place, the methods employed by the IT security team in addressing them and the mode of resolution. Having this information on the table enables the top management to formulate a proper strategy to identify the risk before it fructifies into a cyberattack. Therefore, the onus is more on developing a proactive approach towards handling risk rather than being responsive.

While incident reporting is critical, compliance with statutory regulations is another significant issue. Regulatory laws and acts like GDPR, HIPAA, and others require the respective organisations in their sectors to comply with various mandatory requirements and disclosures concerning trust, privacy, security, and data protection. The Board should be aware of these compliances and the liabilities that could arise because of non-compliance. The penalties can be massive and could end up eroding the entire net worth of the organisation.

Next, Cybersecurity Audits are critical to maintaining any cybersecurity posture. Besides the regular operational audits, audits of infrastructure form a significant area of discussion. Cybersecurity infrastructure involves firewalls, mobile/web applications, wearable and user devices, switches, routers, servers, and even access provided to third-party supply chain vendors.

The gaps identified during such audits need immediate mitigation, with the Board having updated knowledge about their status. The Board should offer its assistance in the form of stipulating and adhering to a specific time frame for the closure of these audit reports. The discussions could also involve the purchase of new solutions to handle these gaps. Having adequate knowledge of these aspects is essential for the Board members.

People, Process and Technology

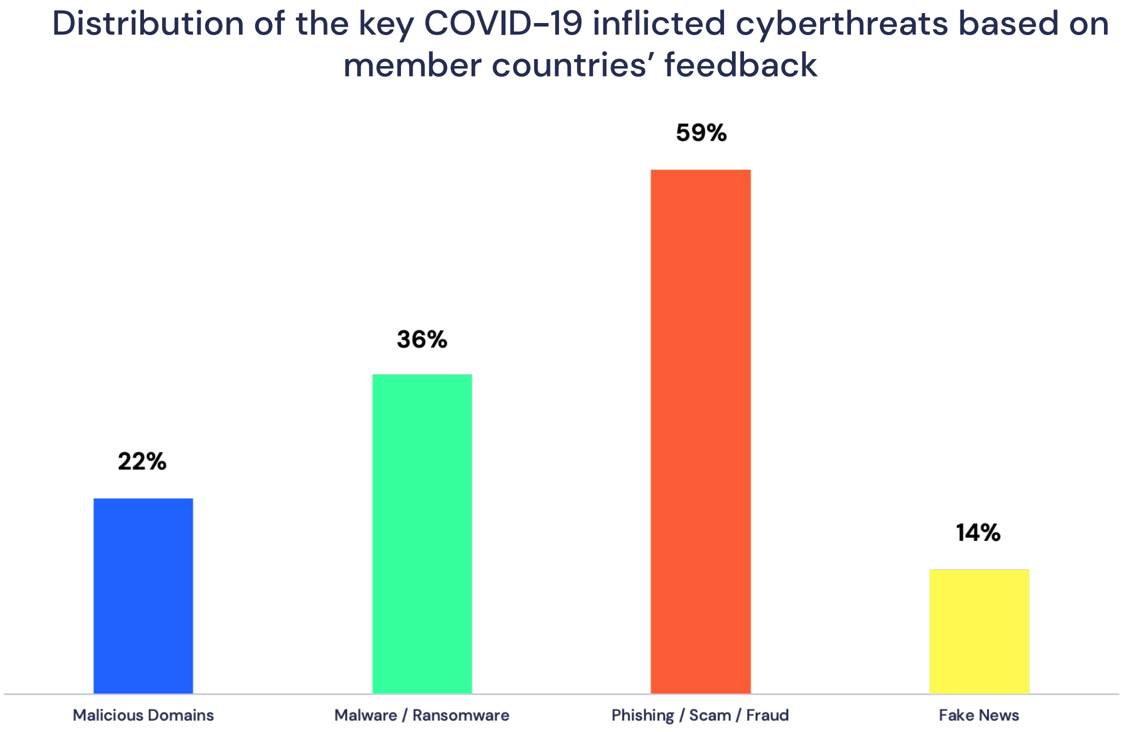
3. Technology

While people and processes play a critical role in maintaining a robust cybersecurity posture, technology is the third leg of this tripod. An organisation should have updated technology in all its systems, including the wearable devices that people use today in the aftermath of the pandemic as they work from remote locations.

The upgrading of hardware and software is of critical significance. The Board should know whether the organisation's network systems have the necessary OS patches, antivirus solutions, router firmware and switches, and updated software. The management should seek information from the CISO in the form of metrics on dealing with non-updated systems. The CISO should have the solutions and recommendations ready for deploying the relevant software for such updates.

The new cybersecurity challenges facing organisations in a post-pandemic world

The world will not forget the year 2020 anytime soon, thanks to the pandemic that is not showing any signs of abating. The pandemic has brought with it health risks. Besides, not many people anticipated that there would be a deluge of cyberattacks. Statistics show that the number of cyberattacks increased manifold during the pandemic.to develop new cultural responses to engaging the workforce remotely, the security risks are perhaps the most significant further issue.



Interpol report shows an alarming rate of cyberattacks during COVID-19
(Image Source: *Interpol*)

The new cybersecurity challenges facing organisations in a post-pandemic world

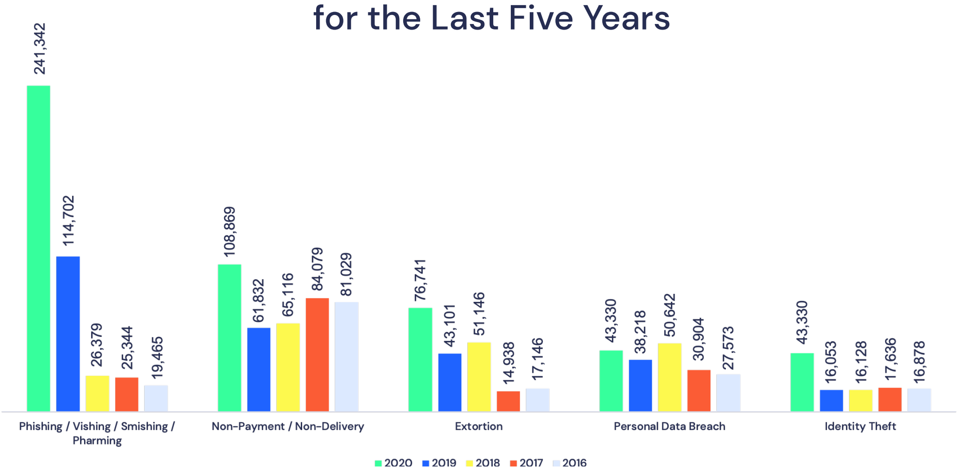
The pandemic introduced a new work culture, that of working from home or remote locations to the delight of the workers. However, the CISOs had their hands full because of the shifting of the goalpost. Instead of handling their routine tasks and working towards achieving long-term goals, their priorities changed to secure connections for these new distributed workstations. As a result, the cybercrime graph witnessed a massive upswing. Here are some significant cybersecurity challenges faced by a post-pandemic world that the Board should know.

Increased Phishing Attacks:

According to FBI-released data, phishing incidents nearly doubled as the number of incidents increased from 114,702 in 2019 to 241,324 in 2020. Along with phishing, its variants like spear-phishing and BEC attacks also started witnessing a growing trend. As discussed earlier, the BEC attacks and spear-phishing involve targeting the top officials of the organisations that handle finance and other business improvement departments. Hence the Board and the top management should treat this issue with utter seriousness because:

- 68% of business leaders feel that phishing is a significant threat to the industry.
- Google has detected more than 2.1 million sites as phishing websites.

Top Five Crime Type Comparison
for the Last Five Years



(Graph Source: *ic3*)

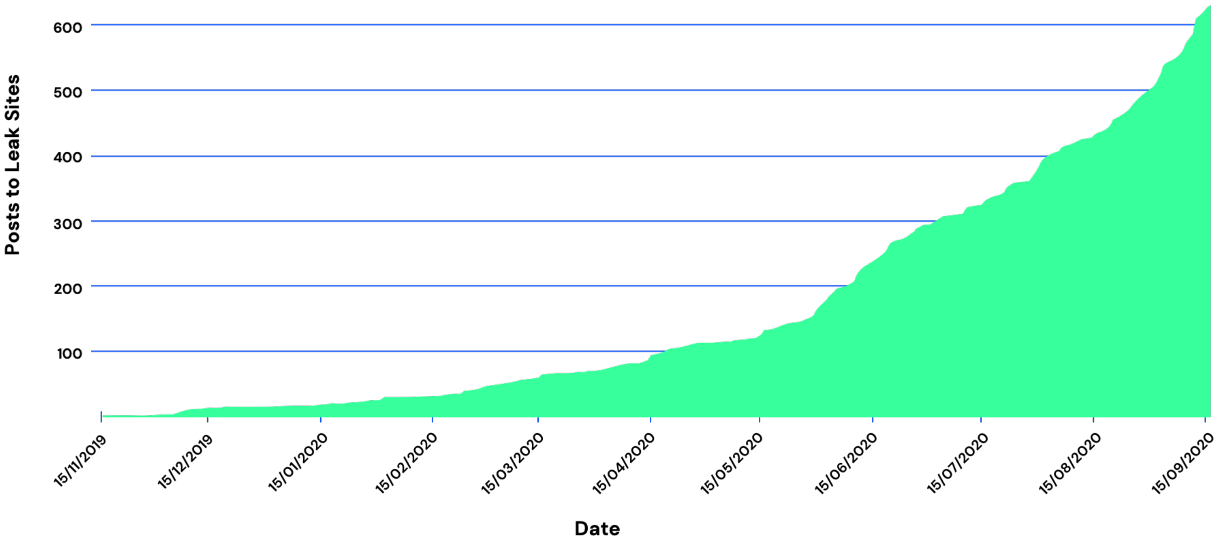
The new cybersecurity challenges facing organisations in a post-pandemic world

New attack vectors and increased risk of data breaches:

With improving technology, malicious actors have also evolved. Though phishing and other cyber risks continue to exist, the growing awareness in the workforce has forced these malicious actors to switch over to new attack vectors like ransomware attacks. Attacks like the Oxford University Lab ransomware attack, Cambridge Meridian Academies Trust ransomware attack, and the NHS vaccination leak are examples of some of the recent ransomware attacks that disrupted business operations on a massive scale. Besides, the following statistics drive home the point:

- The first half of 2020 witnessed data breaches exposing more than 36 billion records.
- As the pandemic started grappling the world ransomware attacks increased exponentially within a span of a few months.
- There is one ransomware victim somewhere in the world every ten seconds.

Running total of data leaks sine November 2019



(Graph Source: *www.pwc.co.uk*)

The new cybersecurity challenges facing organisations in a post-pandemic world

Emerging Technologies And Proliferating Attack Surfaces:

functioning online and organisations shifting towards the latest technologies, on-premise methods and methodologies are gradually going obsolete. Technologies such as cloud computing, AI and ML are disrupting how businesses operate and have been a boon for organisations, for the major part. On the other hand, these emerging technologies have given rise to new cyber-threat vectors; for instance, intruders can deceive cloud systems into redirecting the cloud user's request to an adversary's module and enable the threat actors to manipulate and steal data.

- By 2023, the number of DDoS attacks is expected to reach 15.4 million globally
- Malware increased by nearly 358% in 2020

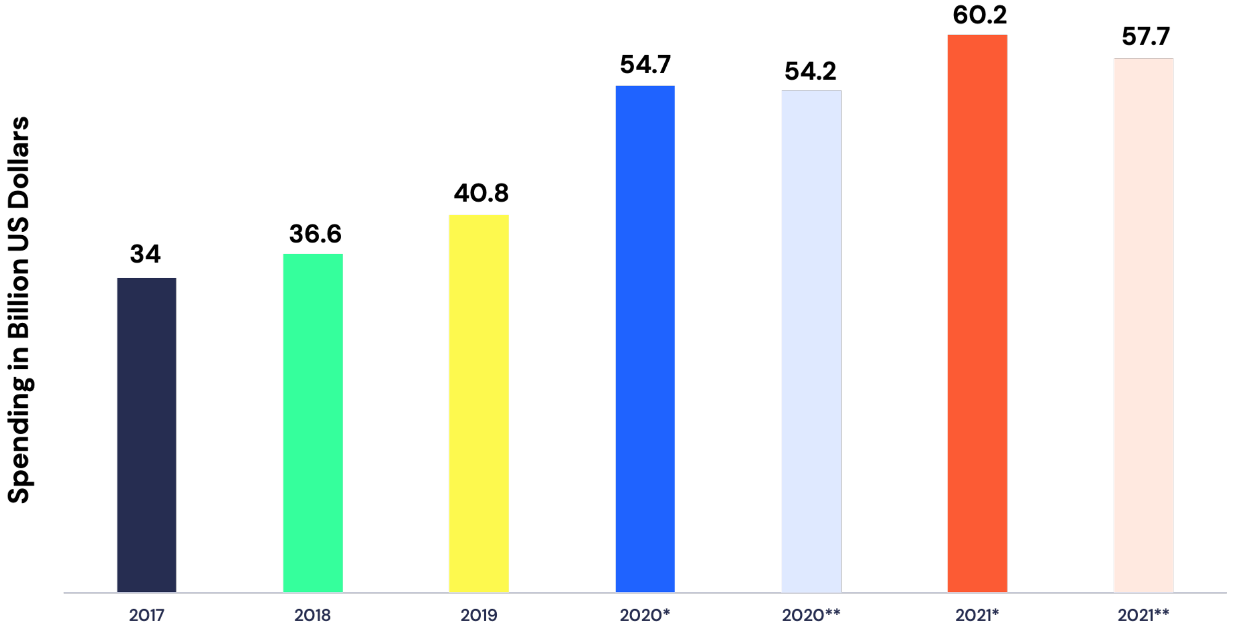
The new cybersecurity challenges facing organisations in a post-pandemic world

Limited Or Further Shrunken Cybersecurity Budget:

The COVID pandemic has hit the industry where it hurts the most – the finances. Many countries had to shut their borders and ordered lockdowns, thereby impacting the supply chain severely. As a result, the bottom line for most organisations has shrunken. Under such circumstances, one cannot expect organisations to allot more funds towards their cybersecurity budgets. Board members should be aware of these aspects, so adequate strategies can be devised to tackle such situations.

- Data breaches cost business enterprises an average loss of nearly £2.83 million.

Spending on cybersecurity worldwide from 2017 to 2021 (COVID-19 adjusted)



(Graph Source: *Statista*)

The new cybersecurity challenges facing organisations in a post-pandemic world

Tightening Regulatory Landscape:

With the introduction of regulations like GDPR (General Data Protection Regulation) back in May 2018, organisations are under increasing pressure to ensure data privacy. The slightest of lapses can end up with companies paying massive penalties running into millions. Though the tightening regulatory landscape is good for data subjects themselves, the industry, their organisations, their employees, and their Boards must understand the severe implications of non-compliance with regulatory conditions.

- GDPR led to regulatory fines that added up to £45 million in its first year.
- Organisations spent around £6.5 billion on preparing for GDPR.

How can the board know enough to address the growing cybersecurity challenges?

A balanced cybersecurity budget, employee training and education on basic cyber hygiene, a thorough vetting process before hiring third-party vendors and contractors, a robust cybersecurity framework and processes around it, etc., are some of the key areas the Board must focus on. It will strengthen and help them know more about their organisational cybersecurity posture. Here are some fundamental questions board members must ask themselves that can help the Board know enough to address the growing cybersecurity challenges:

1. Do you understand your enterprise information security needs adequately?
2. Do you understand your information security risk appetite and risk tolerance?
3. Is your enterprise information security risk aligned with the enterprise risk? And, are you balancing your business objectives with cybersecurity requirements?
4. Do your leaders practise due care and due diligence before making any decision related to cybersecurity risk management?
5. What did you find out from your recent penetration testing exercise? And, are there any lessons learnt? Are the open issues being tracked and closed effectively?
6. Is your internal audit team effective? Or, is there any plan to hire a third-party audit/advisory firm? What are your evaluation criteria going to be?
7. How do you evaluate the effectiveness of your cybersecurity risk management framework? When was the last time you met the CISO?
8. Are you balancing information security vs data privacy well?

Asking the right questions to define a board's role in cybersecurity also provides a framework on how the board members can help integrate cybersecurity into the organisational culture.

What good governance looks like to deal with the threats

Not very long ago, the consensus in the industry was that financial organisations like banks and insurance services alone were prone to cyberattacks. However, attacks such as the WannaCry Ransomware attack continually open executives' eyes and make the industry realise that cyberattacks can affect almost anyone, regardless of being on any cyber adversary group's hit list.

Malicious actors today do not work in isolation as they have industrialised their operations. A particular group identifies vulnerabilities and then shares them with criminal groups. Ransomware developers today share them with malicious groups in return for a share in the profit. The above-discussed 'Colonial Pipeline Attack' is a perfect example. Therefore, organisations need to be prepared to handle such advanced threats. The proper direction to mitigate these risks should undoubtedly flow from the top.

The pandemic has seen more organisations moving towards digitisation due to adapting to the cloud and having people work from home. Not many would have thought about the cybersecurity implications of such a move. However, those who have done so are reaping the benefits of foresight and preparedness.

The question on every Board's mind today should not be how to deal with a cyberattack if it happened. In contrast, they should think about when such a scenario would arise and whether the organisation is equipped enough to detect and manage the issue. The objective should be on having as little downtime as possible and bringing the organisation back on its rails quickly. Good governance is in anticipating a cyberattack and preparing to face the eventuality.

Another good quality that separates good governance from mediocre is effective and open communication. With every individual in the organisation speaking the same language of cybersecurity, it helps in promoting the cybersecurity culture within the organisation. A cyberattack can bring out the worst in the organisation and its personnel if they do not know how to deal with an attack or an intrusion attempt. Hence, adopting a concerted effort can help calm down the nerves and ensure that the attack is dealt with effectively.

Cybersecurity as a discipline all executives should have appropriate knowledge of

The Board of Directors has essential things to deal with, especially understanding the market demands, liaising with the government and regulatory authorities, and ensuring that the organisation is on the right growth track. However, in today's scenario, they cannot overlook cybersecurity risk and leave it all to the CISO to handle everything by themself. All executives should view cybersecurity as one of their critical responsibilities.

While the cybersecurity threat is dynamic and ongoing, the key to handling it is to be vigilant. However, the Board should understand that their role is not cybersecurity risk management but cybersecurity risk oversight. If it requires restructuring their committees to oversee cybersecurity risk management, they should not hesitate to do so.

It would be naive to expect a Board Director to immediately become an expert on cybersecurity and start giving directions to everyone. If they need more education about cybersecurity risk, they should, by all means, acquire it. The Boards have the power to engage third-party experts to oversee the organisation's cybersecurity posture. However, the Board should have the requisite knowledge to engage in meaningful dialogues with such third parties and understand the organisation's requirements. Here, the CISO can prove to be the most effective link between the Board and such third parties.

When appointing third parties to oversee cybersecurity risk management, the Board should follow the Zero Trust policy because intentionally or inadvertently, such third parties could end up opening the door to malicious actors.

Just as organisations set goals for their employees to achieve, the Board should set cybersecurity awareness goals amongst themselves. A healthy rapport among all the Board members to stay updated at the same level could well work in favour of the organisation. It enhances vigilance and thereby keeps bad actors, including rogue employees, in check.

The need to make cybersecurity a regular board item

The World Economic Forum has declared that cybersecurity is one of the top ten risks faced by organisations that require immediate attention. However, unfortunately, 40% of Board members admit that cybersecurity has never been a topic of regular board discussion.

The pandemic has changed the equation and shifted the goalposts for many organisations. Suddenly, they have to contend with cybersecurity risks because of people working remotely and on unrecognised devices. Hence, cybersecurity has become a priority and forced Board members to get themselves acquainted with cybersecurity risks.

The Board can argue that each organisation has a CISO to manage internal and external cyber threats. Legislation such as the GDPR will always be available to create a reason to instil cyber discipline in the organisation. Under such circumstances, the Board should concentrate on what they do the best, improve working conditions and ensure that the organisation keeps making profits. The above argument is flawed because the ultimate responsibility of any loss suffered by the establishment due to a cyberattack should rest with the Board of Directors. They have a job to oversee the entire risk management structure of the organisation, and cybersecurity risk is right there at the top of the pile.

With cybersecurity gaining significance, there is a need for it to be a regular Board item. Dedicated board sessions must be formulated for discussion, imparting knowledge, and brainstorming on cybersecurity matters on a periodical basis. It will help the Board be on a par with the required level of awareness to keep the organisation's overall governance on a healthy track. A change in the Board's attitude towards cybersecurity sends the right signals down the line that the top management can take tough decisions on matters concerning cybersecurity.

Cybersecurity as a crucial Board item provides proper assurance to investors and gives them the confidence that their wealth and data are safe with the organisation. Such a scenario requires the Board members to enhance their knowledge on cybersecurity and increase awareness and proficiency levels accordingly.

Final words

With more employees working and connecting from their home network, they may still have default manufacturer-provided passwords saved on their routers and modems. In this scenario, it is a challenge to ensure basic cyber hygiene as there are more endpoints for potential entry for cyber adversaries. "Cybersecurity is everyone's responsibility", and hence, the responsibility to protect the valuable information assets of an enterprise is extended beyond CISOs or SOC teams to each employee of the organisation and on 'the board.' The immediate call to action for the Board demands active participation in cybersecurity matters, continuous monitoring, and a proactive defence mindset. It calls for:

1. Staying a step ahead of cyber adversaries by building the next level of cybersecurity capabilities.
2. Fortifying the enterprise information infrastructure by employing dedicated SOC, threat intelligence, and a dedicated security advisor (e.g. a CISO, a third-party cybersecurity expert, etc.)
3. Assigning clearly stated Board-level oversight responsibilities for the protection of enterprise's information assets.

The Board should ensure they 'know enough' by keeping themselves updated on the emerging technologies and the consequently changing threat landscape. They must also keep themselves informed about the tightening global regulations around information security and data privacy. Having dedicated board sessions periodically concerning such matters from a governance angle will help maintain the organisation a robust cybersecurity posture.

References

1. Dobrygowski, D., Vadala, D. (2020, September 01). Does Your Board Really Understand Your Cyber Risks? Harward Business Review. https://hbr.org/2020/09/does-your-board-really-understand-your-cyber-risks

2. (Rosenthal, M. (2021, May 17). Must-Know Phishing Statistics: Updated 2021. Tessian. https://www.tessian.com/blog/phishing-statistics-2020/

3. Srivastav, V. (2019, August 15). What the Board needs to know about Cyber Security. LinkedIn. https://www.linkedin.com/pulse/what-board-needs-know-cyber-security-vivek-srivastav/

4. (Harisaiprasad, K. (2019, November 20). What the Board Needs to Know about the organisation's cybersecurity status. ISACA. https://www.isaca.org/resources/isaca-journal/issues/2019/volume-6/what-the-board-needs-to-know-about-the-organizations-cybersecurity-status

5. Neiswender, P. People, Process, Technology: A Three-Pronged Approach To Cyber Risk Governance. Corporate Board Member. https://boardmember.com/people-process-technology-a-three-pronged-approach-to-cyber-risk-governance/

6. Panettieri, J. (2021, June 7). Colonial Pipeline Cyberattack: Timeline and Ransomware Attack Recovery Details. MSSP Alert. https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/colonial-pipeline-investigation/

7. Khalili, J. (2021, May 07). NHS vaccination website leaks people's medical data. TechRadar. https://www.techradar.com/uk/news/nhs-vaccination-website-leaks-peoples-medical-data

8. Bryk, A. (2020, February 26). Cloud Computing Attacks: A New Vector for cyberattacks. Apriorit. https://www.apriorit.com/dev-blog/523-cloud-computing-cyber-attacks#:~:text=Cloud%20malware%20injection%20attacks&text=If%20the%20cloud%20system%20is,or%20stealing%20data%20or%20eavesdropping.

9. McKinsey & Company. (2019, March). Perspectives on transforming cybersecurity. https://www.mckinsey.com/~/media/McKinsey/McKinsey%20Solutions/Cyber%20Solutions/Perspectives%20on%20transforming%20cybersecurity/Transforming%20cybersecurity_March2019.ashx

10. Brooks, C. (2021, May 02). Alarming cybersecurity stats: What you need to know for 2021. Forbes. https://www.forbes.com/sites/chuckbrooks/2021/03/02/alarming-cybersecurity-stats-------what-you-need-to-know-for-2021/?sh=ea51d6b58d3d

11. Sobers, R. (2021, March 16). 134 cybersecurity statistics and trends for 2021. Varonis. https://www.varonis.com/blog/cybersecurity-statistics/

12. Lund, F., Richter, W. (2021, February 02). Boards and cybersecurity. McKinsey & Company. https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/boards-and-cybersecurity

13. Klemash, S. (2018, July 17). How boards can prepare for the next cybersecurity threat. EY. https://www.ey.com/en_in/board-matters/how-boards-can-prepare-for-the-next-cybersecurity-threat

14. Cracknell, P. (2020, September 28). Making Cybersecurity a Priority in the Boardroom. Infosecurity. https://www.infosecurity-magazine.com/opinions/cybersecurity-priority-boardroom/

Visit
equantiis.com

Call
0203 376 7447

EQUANTIIS