KPMG

Top cyber security considerations in 2019

KPMG Board Leadership Centre

Several factors have increased the focus on cyber security and information protection in recent years: from rapid shifts in technology, the explosion in in the volume of data and the ongoing migration to automated and cloud-based services; to the growing number and sophistication of threats and ever more rigorous regulatory requirements. Cyber security is high on everyone's agenda. In this paper we explore the critical issues for the board to consider.

Skills shortage

A shortage of talent in the cyberspace is one of today's biggest issues. In a poll of over 600 directors and executives, only 16% said they are confident that their company has the talent required to keep pace with cyber security risks.

The role of the chief information security officer (CISO) has also changed dramatically in the last two to three years. The best CISOs are razor focussed on the strategy of the organisation they are in. They understand how to translate cyber security into business enablement, and they are helping to show how a good cyber programme can improve a company's business results.

Coming from the other side, many internal audit departments are working to ramp up their skill sets to perform robust and independent assessments of the cyber security programmes which exist.

However, the dearth of adequately trained, appropriately skilled personnel to protect vital processes, intellectual property, and sensitive data is an issue across virtually every industry. Boards should ask to see and understand the organisation's cyber talent plan and ask management about efforts to automate manual tasks, freeing up people to focus more time on strategic activities.

Data privacy compliance

The board's view of data privacy sets the tone for the way it is addressed throughout the organisation. Engagement across every part of the organisation is required as security professionals look to embed privacy into the DNA of operations and people engagement.

A strategic approach to privacy and information governance can reduce the overall cost of compliance and enhance customer trust.

In light of data privacy regulations, such as GDPR, consumers are rightfully demanding more visibility over how a given organisation is protecting their information and how they are using it. Organisations must therefore know where all of their data is and understand what processes are using it so they can react to data privacy regulations by giving people the right to opt in or out. That exercise can be a significant challenge.

Fraud risk and cyber risk

Fraud and cyber should garner equal attention from a security perspective. New and improved strategies for collecting and leveraging personal data, particularly authentication data, should be on the business agenda. Is the organisation doing enough to understand typical customer behaviour, recognising anomalies, and, in turn, educating customers about the value of using personally identifiable information conscientiously to prevent fraudulent activity?

Artificial intelligence (AI)

AI has the ability to correlate numerous data sources to identify patterns or anomalies that might point to malicious activities. How are an organisation's leadership and cyber professionals thinking about AI and security in general in the context of the organisation's longer-term platform strategy?

Just like AI being used to attack the perimeter of a business – or, once they're in, learn the patterns of where to inject malware – defence is working the same way. Imagine a security system able to adapt how it defends itself based on the patterns it sees.

However, it's important to remember that technology alone has never solved the cyber security problem. A philosophical shift in defence that we've seen over the past few years is that forward-thinking organisations are focusing on protecting their most important assets. They are applying specific controls to make sure the most important data is the most protected.

Authentication

Identity and access management is evolving from a security-driven initiative to a driver of business enablement. Directors should probe management about what the company is doing in the areas of advanced authentication, identity proofing, fraud, and analytics, including a move away from passwords to biometric-enabled apps.

From a security perspective, the notion of opting in and opting out is going to become very important. For example, organisations that deploy 5G technology will need to help their customers make informed decisions about giving up their data – helping them understand for example, what they're giving it up in exchange for; whether it's convenience, flexibility, or ease of use.

Phishing

Despite the growing sophistication of today's attack methods, phishing remains one of the toughest threats to defend. A key differentiator will be internal analysts who are constantly engaged, updating the internal messaging throughout the organisation as the operations and the threats evolve. The cyber team must be out in front.

What we see is that people are the best defence here – while technologies designed to stop phishing will continually evolve as the threats change, the best thing businesses can do to protect themselves from attack is training and awareness programmes so staff know what to look out for.

Key questions to drive robust boardroom discussions about cyber security

- Is our cyber security risk management framework evaluated frequently enough?
- How do we keep up with regulatory changes and new legal requirements?
- Are we staying abreast of industry practices and connecting with law enforcement?
- Is our incident response plan tested and up to date?
- Are we getting the information we need to assess the cyber effort status?
- Do we have the talent we need to keep pace in cyber?

The KPMG Board Leadership Centre

The KPMG Board Leadership Centre offers support and guidance to non-executive directors, whether managing a portfolio non-executive career or embarking on a first appointment. Membership offers you a place within a community of board-level peers with access to topical and relevant seminars, invaluable resources and thought leadership, as well as lively and engaging networking opportunities. We equip you with the tools you need to be highly effective in your role, enabling you to focus on the issues that really matter to you and your business.

Learn more at www.kpmg.com/uk/blc.

Contact us

Timothy Copnell
Board Leadership Centre
T: +44 (0)20 7694 8082
E: tim.copnell@kpmg.co.uk