Digital transformation opens door to more cyber risk

Cyber threats and attacks have only increased since the start of the pandemic, particularly ransomware and COVID-themed phishing attacks

John Heaton, Partner, Cybersecurity Advisory Services, KPMG in Canada

As organizations move toward remote work, digital processes and cloud-based technology, the levels of risk they are exposed to naturally increase. Add a global pandemic into the mix and those risks have been even further exacerbated.

The audit committee plays a crucial role in overseeing risk management activities and monitoring management's preparations to respond to cyber threats. These responsibilities include assessing cyber-risk mitigation investments and how the organization will respond in the event of a breach.

Three cybersecurity challenges in the COVID-19 era

Audit committees should be aware of three major challenges facing organizations in the realm of cyber risk: the move to digital processes; the move to cloud; and an increasing number of cyber threats and attacks. These challenges existed before the COVID-19 pandemic, but the abrupt, unplanned migration to remote work arrangements — including digital processes and cloud-based technology — at the start of the pandemic has opened the door to additional risk.

Almost overnight, organizations moved their digital transformation into overdrive. Everyone — whether adequately prepared, willing or not — started using video conferencing platforms, enterprise collaboration solutions and consumer social media applications, often from home-based Wi-Fi that employees might be sharing with the rest of their family. In many cases, core business operations now happen on home-based IT, where there are weaker security controls in place. And, an organization's security team (if one exists) is now tasked with managing security outside of the office and in employees' homes.

Cyber threats and attacks have only increased since the start of the pandemic, particularly ransomware and COVID-themed phishing attacks. These prey on people's anxieties and insecurities, enticing them to click on links related to vaccines or financial support, for example. There are costs associated with these attacks, both from downtime and potentially from the loss of data, but there are also soft costs, such as reputational damage. Some organizations might not even be aware they've been attacked and their data is up for sale on the dark web. In many organizations, it's therefore up to the audit committee to ask whether the right controls are in place to detect and thwart such attacks and challenge management into taking the necessary steps to ensure their organization's digital assets are safeguarded.

With the move toward remote digital processes and cloud-based technology, audit committees need to consider how the organization's risk tolerance may have changed (and how that's being monitored). A year ago, they may not have considered running enterprise applications in the cloud. Today, faced with fewer alternatives given the pandemic, they might be willing to accept more risk.

> "People may be the weakest link in your organization's cybersecurity efforts but they can also be your best line of defence. Organizations need to ensure their employees are educated on cyber risks and what to do if they're the victim of an attack."

John Heaton
Partner, Cybersecurity Advisory Services
KPMG in Canada

Taking control over existing and emerging risks

Audit committees should make sure management has considered what's being done, or could be done, to monitor existing and emerging risks and put additional controls in place where necessary. This includes controls to authenticate and validate anyone who accesses the network, whether they are employees, suppliers or customers, as well as assurance from cloud service providers that proper security controls are in place.

People may be the weakest link in an organization's cybersecurity efforts but they can also be the best line of defence. Organizations need to ensure their employees are educated on cyber risks and what to do if they're the victim of an attack. For example, if they're the victim of a ransomware attack while working remotely, do they know who to call and what to do? The IT team can put the best tools and technologies in place to secure the organization's data, but if an employee clicks on a malicious link, none of it matters.

Ultimately, cyber risk is a business problem, not an IT problem, and should be ranking high on the audit committee agenda to monitor and challenge management on how they are managing risk. Security used to involve building a virtual fortress around a physical building to protect the IT infrastructure within it. But with workers at home and data in the cloud, there is no fortress anymore. This may be our 'new' reality, but organizations aren't likely to go back to the fortress once employees get used to the convenience of on-demand cloud applications they can access anytime, anywhere.

Dealing with cyber risk, during COVID-19 and into the future, means audit committees will need to ensure the organization's processes are robust as they move further into this digital, cloud-based world. But there's value in doing this. There's opportunity in cloud and digitization to transform the business and be better prepared for whatever is to come.

What should audit committees be asking?

- How have we changed our cyber risk tolerances, monitoring tools and processes with the move to a digital world?
- How are we ensuring that we have appropriately authenticated and validated users, customers and partners who use our digital tools?
- How have we evaluated the risks of cloud solutions when moving from an on-premise solution?
- How do we obtain assurance that the cyber controls are in place and performed at the cloud provider?
- How have we educated our people and enhanced our processes to take account of the new reality of working to identify and respond to these new threats?

Contact

John Heaton
Partner, Cybersecurity Advisory Services
KPMG in Canada
416-476-2758
johnheaton@kpmg.ca

Let's do this. home.kpmg/ca/audit