Securing the new business reality through pragmatic cybersecurity

KPMG Singapore Board & Governance Institute

To both sophisticated organised crime outfits and lone hackers, the rapid shifts that companies have made to keep their businesses up and running during the COVID-19 pandemic — such as remote working arrangements, supply-chain adjustments, and increased reliance on online platforms — spell opportunity.

With scams ranging from phishing emails to sales of sham coronavirus testing kits and fabricated government claim portals, to ransomware attacks on hospitals to extort money, cyberattacks have surged during the pandemic. Temporary operating models and longer-term implications of a "distance everything" business environment—largely driven by information technology (IT)—will require particularly a vigilant focus on cybersecurity going forward.

Companies that provided digital flexibility, granted security waivers, and boosted their online presence as a part of their immediate response to COVID-19 should now be adapting their security and fraud controls to secure and retain the longer-term benefits of those digital shifts.

For example, where the company previously relied on securing physical facilities, online management oversight of employees, or use of controlled corporate IT, the company may need to rethink its cybersecurity approach using a different blend of protective and detective security controls to allow for use of personal devices and untrusted networks, including remote meeting platforms. Another consideration is that the security controls on employees' home IT networks are often weaker than those in a corporate environment, and while allowing employees to use their own devices can be convenient and efficient, there are downside risks that need to be actively managed and mitigated.

Also, the shift to digital channels — with more money now in the digital economy — is attracting the focus of cybercriminals who will always follow the money. Security around digital payment platforms, as well as customer data and intellectual property, should be paramount.

As companies move from response and resilience to thinking about what recovery and the new reality will look like for the business and its operating model, robust boardroom conversations will need to focus on the following key actions:

— **Providing employees with tools, technologies, and training to operate in an increasingly distance-business environment.** Here, directors should ask: What will the future of work look like? Is there a strategy in place to identify the remote working model(s) and technologies the company will rely on going forward, including cybersecurity training and awareness for employees?

— **Embedding cybersecurity and data governance into digital transformation efforts.** For example, a move to cloud services provides an opportunity to embed security controls with a degree of consistency that is challenging to achieve across older legacy systems. Security should be an integral part of the development of new applications and systems, rather than an afterthought and potential roadblock to the aggressive transformation that many firms will have to drive to remain viable in a post-COVID-19 world.

- **Maintaining the IT skills, resources, and investments required to keep pace with cybersecurity challenges.** In many sectors, the security function will remain under cost-reduction pressures along with the rest of the business. Has the company considered opportunities to automate its security processes? And what is the right budget model for security going forward?
- **Reinforcing the board's cybersecurity protocols.** In addition to greater vigilance regarding the security of board meetings and communications, directors' use of personal email, personal devices, or unauthorised software to conduct board business can present serious cyber risks. Has the general counsel or chief information security officer briefed the board on company cybersecurity protocols that apply to directors as well as to employees in the context of the new operating environment?

In the emerging environment, companies with robust digital models that drive customer and supply chain channels, employee connectivity, and data-driven operations and insights are likely to fare best. That advantage going forward, however, will hinge on the underlying security and the company's overarching digital mind-set.

This article originally appeared in the July/August 2020 issue of NACD Directorship magazine. Contributed by Tony Buffomante, global coleader and US leader for Cyber Security Services at KPMG, and John Rodi, leader of the KPMG Audit Committee Institute.

Contact us

Irving Low
Head of Board & Governance Institute
T: +65 6213 2071
E: irvinglow@kpmg.com.sg

Emilie Williams
Director,
KPMG Asia Pacific
T: +65 6411 8007
E: emiliewilliams@kpmg.com.sg

KPMG Services Pte Ltd
16 Raffles Quay
#22-00 Hong Leong Building
Singapore 048581
T:+65 6213 3388
F: +65 6225 0940

kpmg.com.sg

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.