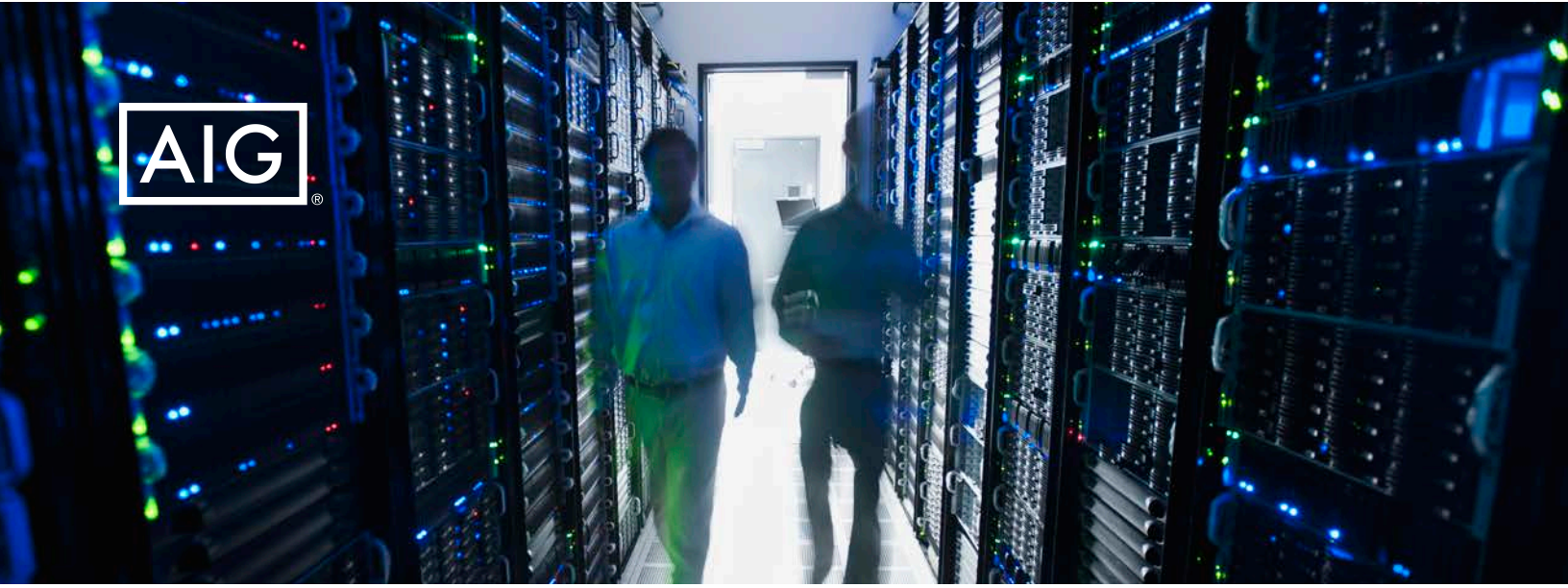

Rethinking the Role of Boards in the Cyber Age

In a world where everything is trackable, quantifiable, will directors & officers find themselves navigating new liabilities sooner than expected?

Company directors could be easily forgiven for feeling lost when it comes to managing cybersecurity risks. With seemingly daily headlines on cyber breaches at some of the world's largest companies, the threat of cybercrime or a breach is real, but navigating the market for solutions often feels like a meandering path without a destination.

Unfortunately for those same directors, their fiduciary duty to shareholders and the personal liability they face as board members requires them to take informed steps to protect the company against cyber risks and cybercrime. Indeed, AIG sees cybercrime as one of the most pressing threats facing boards today.

Nowhere does cybercrime represent more of a risk than in Asia, particularly in China. A November 2016 survey by Pricewaterhouse Coopers revealed that Chinese companies had seen cybersecurity incidents increase by over 900 per cent since 2014. But in spite of this, cybersecurity budgets for Chinese companies actually dropped in 2016 by 7.6 per cent from the prior year. This troubling underinvestment in cybersecurity capabilities is unlikely to end well for Chinese corporations.

The liabilities for companies and their directors that are arising from cyber risks are nearly unlimited. A cyber breach can destroy a company's reputation overnight, taking its stock price down with it. Incredible sums of money are at stake, and while today's attacks are sophisticated, easy to execute, and oftentimes anonymous, cybercrime is only in its infancy and set to rapidly evolve.

This evolution is already apparent in the changing nature of cyber threats. While large-scale breaches of customer or company data capture global headlines, less high-profile cybercrimes are pervasive and can be immediately

damaging to the bottom line. Current cyber crimes on the rise include impersonation fraud, whereby a fraudster pretends to be a senior executive (or "fake president") and induces an employee to divert payments into the fraudster's account, as well as cyber extortion, which occurs when an employee inadvertently clicks a fraudulent link triggering a malware infection on the company's computer systems effectively holding the company's data for ransom.

As companies continue to seek efficiencies and optimise their business practices, we expect to see a greater use of technology aimed at streamlining expenses, boosting productivity, and gathering data. The use of cloud computing is expected to accelerate over the next several years as is the development and implementation of Internet of Things (IoT) devices. Cisco estimates that within the next 3 years, 83 per cent of all data center traffic will be based in the cloud. Rand Europe estimates that there will be 40 to 50 billion "connected things" worldwide by 2020.

A cyber breach can destroy a company's reputation overnight, taking its stock price down with it.

While IoT devices represent a vast expansion of data-gathering capability and are leading a revolution in industrial efficiency and operational insight, these devices offer multiple entry points for a potentially malicious hacker. In fact, the same PwC report attributed the rise in cyber incidents at Chinese companies to the "huge rate of adoption" of IoT devices in the region. These devices often lack basic cybersecurity measures and are easily hackable.

Examples of such hacks are easy to find. In 2014 a hacker broke into a baby monitor and was able to harass a toddler. In 2015, hackers were able to bypass an automobile's security system and disable the braking systems. Hackers were even able to hack into a pacemaker device and cause a fatal shock.

DIRECTORS AND OFFICERS IN THE SPOTLIGHT

Corporate officers and boards are thus faced with complex decisions around how to implement technology. If they choose not to modernise their operations, they run the risk of becoming an inefficient and outdated organisation that cannot keep up with technological benefits of the times. Conversely, by modernising their infrastructure, new risks are created, particularly in the form of cyber attacks and fraud; if not properly addressed, these cyber risks can destroy the value and reputation of a company just as fast as officers would have expected to see efficiency gains.

Directors and officers must perform this delicate balance while under the microscope from external stakeholders, most notably shareholders and regulators who will carefully scrutinise their decisions. Boards will face continual questioning of the logic behind cyber security investments, as well as their ongoing fiduciary duty to look out for the best interest of the company. Did management properly disclose the degree to which their systems could withstand a complex distributed denial of service (DDoS) attack? Does a past transgression regarding failure to update email security protocol threaten a potential M&A transaction? How is the board liable when a data breach occurs, revealing confidential data that sends the stock price plummeting?

These dilemmas remain difficult to resolve, and corporate boards and managers will find themselves the unknowing actors in this evolving drama.

UNPACKING SOLUTIONS

Company boards and management must commit time and resource to educate themselves on the ongoing and dynamic cyber threats posed in our digital and connected age. To fully capture the benefits of a technology-enhanced business, leaders must carefully assess and mitigate the risks that inherently arise.

A first step is to de-mystify the cyber security landscape. For their part, cyber professionals are still struggling to effectively communicate their value proposition. The jargon-heavy marketing of most cyber protection products does little to educate company managers and directors that lack a computer science degree.

IoT devices ... offer multiple entry points for a potentially malicious hacker.

Global insurance firms and consultants have a wide range of online resources available, including sophisticated yet practical advice for company directors. Staff trainings and robust internal confirmation processes are critical to identifying cybercrime and fraud. Yet even with the most modern available technology, the most prepared companies may easily find themselves falling victim to cybercrime.

Company directors and officers may have some provisions in their current D&O insurance policy providing a professional indemnity against claims arising from a security breach or cybercrime. Companies may further consider cyber insurance and crime policies that capture broader risks and liabilities related to cybercrime. Such commercial policies exist to help companies recover monies lost not only to issues like cyber extortion or "fake presidents" fraud, but also the cybercrimes and frauds of the future yet to emerge.

The good news is that boards are indeed starting to carefully consider such cyber insurance policies. AIG research on corporate governance attitudes at Asian corporations conducted in 2014 revealed that two thirds of respondents see cyber insurance increasing in importance in the future.

We expect cyber protection and insurance products to become increasingly relevant to Asian corporations over the coming years. With an unclear digital road ahead filled with potential cyber breaches and unresolved questions around liability, boards must urgently address their cybersecurity needs and prepare for future.