Cyber risk threatens every part of a business, but whose responsibility is it to deal with it?

NWC ALLIANCE · WEDNESDAY, JUNE 19, 2019 · 5 MINUTES

The following is an opinion piece written by Andrew Beckett, managing director and EMEA Cyber Risk practice leader at global investigations firm Kroll. The views expressed within the article are not necessarily those of Corporate Risk and Insurance.

Cyber risk is one of the most serious challenges facing modern businesses, transcending different functions and departments, and presenting a threat to a whole company. Despite this, few organizations have adequate strategies to deal with cyber risk, caused in large part by confusion or lack of clarity over who is responsible for ensuring that cyber threats are mitigated.

Disconnect between risk managers and company boards plays a significant role in creating this situation, made worse by the unique and often complex nature of cyber risk. Kroll's findings in the 2018 Global Fraud & Risk Report indicate organizations are coming to this realization as well: 22% of respondents will be expanding their current use of board engagement to mitigate cyber risk, and nearly half (40%) are planning to launch new initiatives in the next 12 months to engage their boards.

Understanding the dangers

Cyber threats can take many forms, from distributed denial of service (DDoS) attacks, 'man in the middle' attacks, phishing, zero-day vulnerability exploitation, or malware in general, through to specific targeted attacks by state or non-state actors seeking very specific data or access. The unique quality of cyber threats is that they may not be confined to one area of a business, as specific financial or compliance risks may be. This is because an IT system doesn't exist in isolation – it underpins and enables business operations in every department, and therefore a breach or attack can potentially affect every employee and practice area.

This makes managing cyber risk and defending against cyber threats of vital importance, yet there is a significant gap between board members and other employees in terms of both understanding and trust. Many at board level are unsure how to tackle the issue, as they either don't know which questions they should be asking risk managers, or they don't know

how to interpret the answers they receive. Consequently, the location of responsibility for deciding cyber risk management strategies is often unclear, and risks can go unmitigated.

Dealing with the threat

The dislocation of board members from the coal-face of cyber risk mitigation is clearly an issue, but there are ways this can be effectively overcome.

The first and most cost-effective strategy is to improve internal communication between risk managers and decision-makers. Risk managers need to be conscious of the language they use, and define the problems posed by cyber threats in terms the board will understand. For example, given the many different sets of regulations with which companies must comply, explaining risks in terms of regulatory or legal obligations is often effective. Technical discussions about the exact way to mitigate risks can then be held with people situated lower in the company hierarchy, who have both the time and the knowledge to constructively engage in developing a technical response.

The second way to deal with cyber risk is to employ external consultants who can provide and develop the expertise and subject confidence which may be lacking at board level. These experts will often have dedicated cyber backgrounds and experience, know which questions to ask, and be able to interpret the answers they receive. To preserve the board's involvement and accountability when engaging consultants, it can be beneficial to appoint non-executive board members, who will have an obligation to act in the best interests of the company and bring additional experience to bare. However, suitably skilled and experienced individuals are still a comparative rarity although it is becoming the strategy of choice for those companies who can find a suitable individual.

Looking at the bigger picture

Cyberattacks can cause significant damage to businesses as companies rely on IT systems just to function day-to-day. Should an attack occur and prevent businesses from accessing information or, in the worst-case scenario, operating altogether, the impact can be unprecedented. Organizations can be left unable to fulfill contractual obligations, which ultimately results in brand and reputational damage not to mention exposure to legal claims. Robust cyber incident response plans reduce this risk, but they have to exist in the first place. To be most effective, they should be practiced as least annually so response team members know clearly their (and other people's) roles, the information they are expected to provide, and in what format. Effective presentation of data and rapid responses play a key part, but are only possible if those responsible for reacting are on the same page. Rehearsing response plans develops "muscle memory", meaning teams are better equipped to respond efficiently and minimize costly delays or mistakes.

Effective leadership and capacity to handle risks also has a significant impact on market valuation, so the incentive to ensure that cyber risk is effectively managed is not just operational, but potentially financial too.

Ultimately, responsibility for managing cyber risk doesn't rest in just one place, rather it should be dispersed among those with sufficient expertise and empowered by executive teams to meaningfully manage it. Whichever solution a company employs, they should be in no doubt about the operational, commercial, and financial importance of ensuring that they are effectively protected against cyber threats. They must have the capacity to act if the worst should happen and their defenses are penetrated because, ultimately, in the modern economy, it's not the breach that kills a business, but the nature of its response.

NWC Alliance

Nwcalliance.com

Wiseinsure.net/smart-cyber

https://www.insurancebusinessmag.com/us/risk-management/cyber/cyber-risk-threatens-every-part-of-a-business-but-whose-responsibility-is-it-to-deal-with-it-170159.aspx?utm_source=Pinpointe&utm_medium=20190619&utm_campaign=WIBA-Newsletter&utm_content=80243C9B-2D88-4675-964D-45293F6EE4B2&tu=80243C9B-2D88-4675-964D-45293F6EE4B2