PROFESSIONAL LIABILITY

LEADERSHIP & ANALYSIS

Time for Asian company boards to wake up to cyber

By Denise Choy of Allied World

As it increasingly becomes a question of "when" not "if" companies will fall victim to a cyber attack, the associated risks to directors and officers are also on the rise. In the aftermath of a breach, if shareholders believe that the board was asleep at the wheel and the business was inadequately protected, they may choose to pursue claims against individuals that would see them being held personally accountable and left liable.

Cyber plays by different rules

Cyber attacks are evolving rapidly to include different types of threats such as data breaches, cyber extortion and ransomware, to name just a few. Recent events such as WannaCry and Petya have proved that hackers don't operate inside traditional geographic boundaries. But with the severity of the cyber threat remaining high and the spread of attacks becoming global, the response by multinational companies is at best inconsistent across different regions. This is despite the fact that companies are under more scrutiny today than ever before as cyber breaches inevitably attract the attention of regulators who are poised to launch an investigation.

Most countries in Asia currently do not require mandatory breach reporting but, if you have operations in the US this is certainly the case, as it soon will be in Europe following the introduction of the new General Data Protection Regulations in 2018. This means that many businesses in Asia are simply not focusing closely enough on these issues and still do not have the necessary cyber infrastructure in place.

The buck stops with the board

Too often directors and officers in Asia assume that cyber security is something to be dealt with by the audit committee or the IT team.

But this is a real and pressing issue that cannot be delegated or outsourced to a third party. The buck stops with the board of directors and senior management. It needs to take responsibility for understanding the myriad nuances of the cyber threat and ensuring that their business is protected. Essentially a shift in mindset is required: This is not an IT problem, it's a business problem.

Failure to grasp the severity of this issue can have significant repercussions for directors and officers. At the end of the day, the issue isn't just about the loss of data; it could be material that leads to disclosure of misleading corporate statements containing sensitive financial information about the growth prospects of the company; which is a much bigger issue for the company and all its stakeholders.

Cyber attacks can also have a devastating effect on a company's cash flow and balance sheet. The impact of business interruption, and the subsequent costs of complying with regulatory fines and notifications can quickly become alarmingly high. The company would need to hire a PR firm to mitigate the damage to its reputation and brand, a law firm to ensure compliance with regulatory requirements and an IT forensic firm to investigate the cause and avoid any future breaches. Meanwhile, the impact of the loss of valuable assets like trade secrets or other corporation information can be difficult to quantify.

CONTINUED >

No time to lose

Directors and officers have to start taking this seriously. They need to be proactive in making sure that data security is a high priority for the company. This means raising awareness of the issue at all levels of the organisation, and beyond. Education across the market is needed to adequately understand the full nature of the cyber threat and the insurance solutions that exist to protect against it. Beyond this, companies have to find people with the right skills to stay in front of what is rapidly changing threat landscape; this will often mean hiring someone with the requisite knowledge and experience. And, of course, having the right insurance solution in place provides directors and officers with peace of mind that they have adequate protection should the worst happen.

It's time for directors and officers in Asia to wake up to the exposures they are facing with today's cyber threat or risk facing the considerable financial consequences.

ABOUT THE AUTHOR

Denise Choy
Vice President
Professional Liability Division,
North Asia

Denise is currently the Vice President for Professional Liability Division responsible for North Asia. She is responsible for the supervision, underwriting and management of the professional lines book and has 15 years of experience in the insurance industry underwriting all product lines within Professional Liability across the Asia Pacific region.

Prior to her current appointment, Denise was the Commercial Professional Indemnity Regional VP responsible for the Southeast Asia and China Region at AIG. Denise joined Allied World in July 2011 and has an undergraduate degree from New York University majoring in Finance and Economics.

For more information about Allied World's insurance and reinsurance solutions, please visit www.alliedworldinsurance.com

alliedworldinsurance.com