beazley

Industry Insights

Navigating the shifting business risk landscape

April 25, 2022

The last 5-10 years has seen major shift in the application of D&O cover and there are now many more event-driven D&O claims. This trend will continue with evolving threats such as increased ESG requirements and employer risks. A mismanaged cyber incident could well turn into a D&O claim against the executives of a firm.

Raf Sanchez, our Head of Cyber Services and Catherina MacCabe, our Focus Group Leader International Management Liability, discuss the complex business risk landscape and how business leaders should look to their insurers for insight and risk management advice on how to better protect their operations in a featured article in Raconteur's 'Business Risk' edition.

To read the full report click here.

As the business risk landscape continues to shift, now, more than ever, businesses should consider their insurer less as a last resort and more as a trusted adviser. Developing a long-term relationship can provide the added value, insight and risk management that is invaluable at to help protect their operations.

Risks are all around. The principal risk is, of course, the risk to the executives of an organisation. The directors and officers of a business shoulder the greatest responsibilities and face personal and corporate liabilities if they make the wrong decisions.

"In the last five to 10 years, there has been a major shift in the application of director and officer liability (D&O) insurance cover," says Catherina MacCabe, focus group leader international management liability at Beazley. "Once reserved for financial problems arising from the need to restate earnings or profits, there are many more event driven D&O claims made today."

ESG and reputational risks go far beyond concerns about climate change. Today the diversity of board members, claims about

greenwashing a firm's green credentials, mismanaging the firm's adherence to ever changing regulations and governance requirements and the personal and financial conduct of senior executives all fall under D&O risk, and can result in costly disputes and litigation. Employer risks, covering everything from how you recruit, reward and retain staff are also under close scrutiny – not only from business analysts, but shareholders, regulators, lobbyists and employees.

EVERY RISK IS ALSO A REPUTATIONAL RISK WITH THE POTENTIAL TO NOT ONLY DISRUPT THE BUSINESS IN THE SHORT TERM, BUT TO CAUSE PERMANENT DAMAGE.

"This is where insurers with a depth of experience and claims data insight can help. By sharing their vast experience of risk to identify not only where businesses experience losses, but also to help identify the specific risks within a client's organisation, and tailor D&O cover to suit their needs" says MacCabe.

UNDERSTANDING THE BUSINESS MINDSET

Specialist insurer Beazley's annual risk & resilience report asks C-suite directors to identify the key risks they believe threaten their business. The list includes supply chain instability, business interruption, boardroom risk, crime and both reputational and employer risks.

Employer risk was considered to be a key concern in 2021 by 11% of respondents. They also predicted it would remain the same for 2022, but it has actually increased dramatically in the last 12 months, with almost a fifth (19%) now considering it a major concern.

Some of this may be associated with reputational risks from ESG concerns. ESG was a new entry into Beazley's questionnaire for 2022, it jumped up the agenda for 18% of those surveyed. According to Beazley's research, boardroom risks have remained a high priority for many business leaders.

Cyber risk has, rightly, become a primary concern for business leaders, and the impact of a cyber breach is not only increasing each year, but becoming more expensive to resolve. This is because cyber threat actors are becoming more aggressive in their exfiltration of target's data and are looking at more inventive and aggressive ways to extort money from their targets.

The Covid-19 pandemic forced organisations to open up their systems in ways that they had never envisaged in order to permit employees to work remotely, says Raf Sanchez, head of cyber services at Beazley. "This sudden shift to homeworking meant organisations had to implement remote access to business systems often before they had the time to understand and mitigate the risks this entailed" he says. "Some businesses rolled out training and adopted additional security measures such as multi-factor authentication (MFA) but many had neither the resources nor the budget to ensure these measures were implemented in time. Optimism about business risk does not equate to mitigation."

Ultimately, adopting new technology practice is only part of the process of building business resilience and reducing the threat of cyber risks.

CYBER RISK CANNOT BE IGNORED

One of the greatest misconceptions about cyber risk is a belief that attackers only want access to high-profile, blue-chip companies, Sanchez says. “The reality is that just like in any marketplace, we see attackers that specialise the mass-market and who can deploy automated attacks with almost zero cost (or risk of being caught) against any business or organisation regardless of size or sophistication,” he adds. “Businesses that find their operations disrupted are as likely to be small enterprises or even sole traders as a multinational bank or entertainment company.”

The risks, and therefore the impacts, are not contained to just financial considerations. They are operational, financial, legal and reputational. Data exfiltration raises trust issues with clients and employees, data unavailability results in immediate operational impact and organisations may be under contractual duties to notify their clients of cybersecurity incidents that can result in automatic termination of customer contracts.

Since many attackers use extortion, specifically the threat of publicising the cyber attack, as a lever to encourage payment, it can be tempting for organisations to consider paying off the criminals, but this comes with its own risks, Beazley argues. Sanchez asks: “How can you ensure that the criminals will honour their commitment to delete the exfiltrated data? Is your organisation contravening legal or regulatory prohibitions against interacting with them?”

He adds: “The data you have paid to be destroyed is just as likely to turn up on the dark web, be shared among threat groups or even be accidentally released. The only sensible way to deal with these risks is to implement mitigations for them and try to prevent them from happening in the first place.”

Mitigating these risks is not as difficult as it may appear at first sight. Businesses can materially decrease their exposure to cyber risk by taking a small number of key actions. For instance, implementing multi-factor authentication for all remote access to their systems is a simple and effective step that will greatly reduce the risk of having an incident. It is also important for organisations to understand that implementing these actions in a consistent and comprehensive manner are essential to their success.

The team at Beazley has seen examples in which MFA has been implemented, but those at the greatest risk of targeted phishing attacks – such as senior executives – have been excused from complying with that control. It is also not just a question of expediency or consistency; senior management and executives should also be leading by example to ensure that a culture of security is cultivated within the business. Also, a mismanaged cyber incident could turn into a D&O claim against the executives of a firm.

A STITCH IN TIME SAVES MORE THAN NINE

Some of these risk management measures will cost money and many will take time to implement. However, the fast-paced nature of technology innovation is also helping businesses. Where once a business would need to invest in new hardware and software – and the IT staff to manage it – new cloud services and solutions allow

companies to implement and scale sophisticated risk management solutions that were previously only available to a large enterprise.

Executives must be seen to be monitoring cyber risk to strengthen business resilience. “We understand there’s no silver bullet,” says Sanchez. “Nor is there a magic money tree to cover every conceivable risk. But we can help clients identify which controls will have best effect and give them insight into cyber risk trends.”

MacCabe adds: “We don’t get paid for telling clients how to reduce their risks and improve their operational resilience. Our reward comes from clients with good risk management that protects their business and reduces both the corporate and personal risk so they don’t become subject of a claim.”

However, if the worst happens and a business does have to make a claim, then business leaders need to be sure that they have the right insurance partner who will help to successfully manage the claim on their behalf.

The more inclusive the discussion is between insurers, those responsible for risk management, the CFO, compliance, the responsible business team, human resources and beyond, the more comprehensive, coordinated and effective the risk planning, and therefore more valuable, it will be.

Read our Risk & Resilience Deep Dive Report into Business Risk
https://reports.beazley.com/2021

More on Beazley’s executive risk safety net
CryptoGuard | beazley

This article was first published here: Navigating the shifting business risk landscape - Raconteur

beazley