beazley

Article

Protecting your business from Day 1 to Day 600+ of a cyber attack

Wayne Imrie

The recent wave of cyber attacks targeting UK retailers[1] highlights the growing reality of cyber risk in today's hyper-connected world. Every business, regardless of size, sector or location, is now on the front line, facing increasingly sophisticated and persistent threats from hackers.

Despite this our recent Risk & Resilience report showed that 83% of global leaders feel prepared to deal with the evolving cyber threat, up from 75% in 2024[2]. It is this potential misjudgement in the level of preparedness that is driving insufficient investment into cyber security and leading to underinsurance and gaps in cover. While large organisations may have the financial resilience to absorb losses relating to an incident, underinsurance can be catastrophic for small and medium-sized businesses.
As retailers across the world are learning the potential cost, perhaps the real challenge comes not in the immediate aftermath of a cyber attack but when shareholders demand answers to:

- How did the threat actors get in?
- What due diligence was in place and how quickly was the breach identified?
- How was the breach handled and how was it remediated?
- What contingency plans did you have in place?
- Why has the share price been so negatively impacted?

In this environment, executives need to be proactive in ensuring that they have the capabilities, insurance and resilience to manage throughout the potentially long lifecycle of a cyber attack. Which could move from mobilising an effective disaster response on Day 1 to working through the legal minefield of shareholder and regulatory

scrutiny that could see them in court on Day 600+.

End to end solution

To protect themselves, businesses of all sizes need end to end risk management support and insurance coverage. This encompasses, pre-emptive, ‘always on’ cyber security services that consistently scan and protect them from new and emerging threats, reactive incident response expertise that ensures they can get back up and running quickly and adaptive post attack support to ensure the business makes the right recovery and learns the lessons. All of this needs to be backed up by meaningful insurance cover so that a business is fully protected for the worst impacts of a cyber attack.

Crucially company boards must be able to demonstrate not only that they handled the impact of the attack well, but that they had invested time, money and process in preparing their firm ahead of any attack. This will stand them in good stead if they become subject to a long drawn out legal or regulatory process that puts their decision making in the spotlight.

Company boards need to increasingly treat cybersecurity as a core governance issue, not just an IT concern. That means not just investing in cybersecurity defence, but ensuring cyber security is high up the boardroom agenda and that they have purchased insurance cover that meets the needs of an ever expanding era of cyber threats.

Wayne Imrie

Head of London Market Wholesale Executive Risks | Specialty Risks

[1] UK Cyberattacks: Restoring Retail Resilience | Supply Chain Magazine

[2] R&R Methodology

beazley