beazley

Article

A Big Problem for Smaller Businesses: ever-evolving cyber risk

Patricia Kocsondy

Cyber threats are no longer just a big business problem. Small and medium-sized enterprises (SMEs) are increasingly in the crosshairs of cyber criminals and the risks are growing more complex by the day.

Vulnerable connections

One major shift is the rise of third-party risk. Many SMEs rely on external IT and software vendors and service providers, to help them to run their operations. But if one of those providers is attacked, your business could be caught up in the incident as the impact of the attack can ripple across interconnected supply chains. Recent cyber incidents involving school software1 and auto dealership platforms2, and others, show how a single breach can impact hundreds of businesses at once.

Random ransomware

When it comes to ransomware, there's no clear pattern or method of approach, with attacks becoming more unpredictable, and AI helping to make cyber criminals' attacks more effective and efficient.

Despite this, many companies still believe they're ready. Our research3 shows **81%** of global executives of SMEs feel confident in their cyber preparedness, but our claims data tells a different story. The most common cause of claims? Phishing attacks, where an employee inadvertently clicks on a malicious link. It's a simple mistake, but one that can have serious consequences.

Vital support

SMEs often lack the internal resources to manage cyber incidents, making comprehensive risk management support essential. Without expert support, a cyber incident can be devastating, potentially leading

to bankruptcy for cash strapped businesses and overwhelmed management teams.

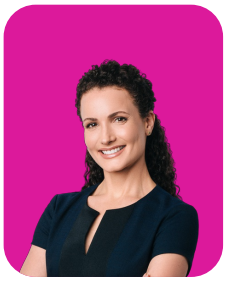
Specialist insurance, like Beazley's Full Spectrum cyber policy, offers more than just financial protection against first and third party losses. It also provides access to expert incident response services and cyber security specialists, helping SMEs to stay ahead of evolving cyber threats, prepare effectively, and if an incident does occur, minimise the disruption and recover quickly.

Complex regulatory web

Another challenge SMEs face is navigating regulatory differences across regions. Even SMEs with a relatively local footprint may handle data that is subject to differing international regulatory requirements – as companies serving customers in the US, UK, the EU and Asia will face a patchwork of rules from each jurisdiction. And keeping abreast of the latest regulations can be hard. Making managing international, cross-border cyber security difficult without expert help, and risky, as costly fines are likely for firms not compliant with local regulations.

Preparation is paramount

Being prepared for an attack is paramount. While strong cyber security and risk management can help to deter threats, as most cyber criminals are looking for the path of least resistance, no firm is immune. Making having a well-rehearsed business continuity plan, and cyber insurance that provides access to incident response and cyber security experts essential in today's digital and interconnected world.



Patricia Kocsondy

Global Head of Cyber Digital Risks

[1] PowerSchool says hackers stole students' sensitive data, including Social Security numbers, in data breach | TechCrunch

[2] Over 50% of US Car Dealers Are Shut Down Following CDK H

[3] R&R methodology

beazley