CYBER IN 2025

The future of cyber sales

Top 3 ways cyber insurance will come of age over the next six years

BY VISHAL KUNDI, *CEO and Co-Founder, Boxx Insurance*

We have all heard of the high-profile cybercrime cases involving stolen data, personal records, health information, and/or financial details. Technological advancements have increasingly connected businesses to sources of electronic data, further exposing them to cybercrime. Despite these major breaches and ongoing issues with privacy and consent, commercial cyber insurance in Canada remains a relatively hard sell.

Demand for cyber insurance has grown over the past few years. And yet, levels of uptake in Canada still lag behind those of the United States. Many Canadian businesses continue to believe they don't need cyber insurance. The reasons why typically fall in to one of three buckets:

1. Businesses that don't collect personal information as part of their operations believe they are not a target for cybercrime.
2. Bigger firms that have their own IT departments feel they can manage cyber risk exposure in-house.
3. A common belief held by small to mid-sized enterprises is that cyber criminals only target larger organizations, not businesses of smaller size.

The facts don't support these conclusions. For example, 75% of hacks target small businesses. In most cases, the attacks are fatal. What's worse is that 80% of the victims could have survived the attack financially had they been better prepared.

Future of cyber

As part of our development research for a new cyber insurance solution, we talked to insurance brokers and security industry specialists across Canada about where they see the cyber insurance market moving over the next five years. Overall, they felt cyber insurance would be a core pillar of every company's risk management strategy.

It is not always possible to predict the future (try predicting a cyberattack, for example). But based on our research, we have synthesized our Top 3 cyber predictions, presented in a list below:

Tougher cyber regulations

Tougher government regulation and oversight will continue, placing new requirements on businesses and insurers.

As long as cybercrime evolves and changes, so will the way in which regulators and governments respond to it. Year 2018 was a watershed for data protection and privacy regulation. With the introduction of the EU General Data Protection Regulation (GDPR), as well as amendments to the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada, we will undoubtedly see a rise in the demand for cyber insurance in 2019 and onwards as businesses fully come to grips with their requirements. The next few years will also be noteworthy for setting legal precedents for regulatory fines and class action law suits.

Countries around the world will adopt legislation that will increasingly require high-level assurance signatures on digital contracts and transactions in order to fight online fraud and criminality. These efforts to uphold the integrity of the process for ensuring identity will have an impact on the contractual relationships between businesses and individuals.

Insurers will be required to review their policy wordings and coverage regularly to keep up to speed with regulatory and compliance requirements.

New driver for cyber demand

Demand for cyber insurance will be led by the fear of losing business, not by the fear of losing stolen data.

Compromised data is valuable today, with plenty of opportunities to exploit it. Expect the value of breached data to decrease dramatically in the future, especially as organizations put in more controls to limit its use and collection.

As the value of stealing data for financial gain decreases, our bet is that we will see hackers increasingly shift their focus to other forms of crime that shut down and extort businesses. Examples of cybercrimes that may be on the rise include:

- using malware to take remote control of a computer network
- cryptojacking (the unauthorized use of someone else's computer to mine cryptocurrency)
- exploit kits (toolkits that cybercriminals use to attack vulnerabilities in systems to distribute malware)

Internet of Things (IoT) and smart devices will exacerbate the threat. IoT is inherently and chronically insecure; it is wide open to potentially devastating cyberattacks that may have far-reaching consequences for a company's vital networks and systems.

Canadian organizations will be required to think about how their business could be compromised by hackers who want to make money at their expense.

Better assessment of cyber risk

Insurers will have a better understanding of the risks and the methods to better assess and price these risks.

Data-driven underwriting in cyber insurance will no longer be elusive and cyber insurance will return to risk-based pricing fundamentals.

The 'market-based' underwriting of today will inevitably catch up with underwriters, and a hardening market will require them to take a closer look at their cyber risk assessment and pricing. Partnerships with security firms will help insurers better assess risk; also, they will help insurance professionals meet customers' needs, aiding the client's understanding of which cybersecurity safeguards should be leveraged. CU

Vishal Kundi is the co-founder of Boxx and Cyberboxx, its flagship cyber risk management product. He has created new operations in Asia and Latin America for insurance companies, and developed distribution partnerships in Europe and Canada.

CROWDSOURCED

MUST-HAVE SERVICES ON A CYBER POLICY

Al Recio

Assistant Vice President, AXIS Pro

A cyber policy requires pre-vetted vendors with specialized knowledge as expert resources. They must be available 24-7 to assist during a cyber incident. A breach coach can review and assess the cyber incident and provide expert resources to assist. Other must-haves include a notification service to alert those affected and report to the privacy commissioner; credit monitoring; a network forensic team to help determine the cause and resolve the situation; a public relations firm; and forensic accounting to determine if a business interruption income loss resulted from the cyber incident.

Sara Runnalls

Vice President and Associate - Public Sector Risk Advisor, BFL Canada

Three services are a good start to help reduce the risk of cyberattack. One is customizable, web-based training for employees on how to reduce cyber risk. Another, known as domain protection, identifies and blocks web domains used by cyber criminals. Finally, an infrastructure vulnerability scan examines an organization's internet-facing technology to identify vulnerabilities that are open to cyberattack.

Adil Palsetia

Partner, cybersecurity and privacy practice, KPMG Canada

A friend from a major commercial brokerage says, 'We almost force our policyholders to use a breach coach.' Typically a lawyer or a legal rep, a breach coach will help you with public relations and disclosure requirements and report to external stakeholders when required. Technical response teams will determine whether the attack is ongoing, sever ties with the affected systems and re-establish appropriate controls. They will help you with a post-event assessment, and set up a more resilient program going forward.