ROCHESTER BUSINESS JOURNAL

Part of the BRIDGETOWER MEDIA network ■ OCTOBER 9, 2024

Insurers tackle new issues in cyber risks while improving current practices

■ CAURIE PUTNAM

Over the past year, 62% of U.S. companies have filed a cyber insurance claim and over 27% of those businesses have filed multiple claims, according to Delinea's 2024 Cyber Insurance Research Report released last month, underscoring the ever-increasing importance of cyber insurance for businesses.

“Even among the people who've had insurance policies, there's been an increased activity in making those claims, which I think is reflective of the increased risks and attacks, but also reflective of the sophistication of companies and the realization that that's what insurance is there for,” said Anna Mercado Clark, an attorney who is a partner at Phillips Lytle LLP.

Anna Mercado Clark

Clark, who is also the Chief Information Security Officer (CISO) at Phillips Lytle, says a trend in cyber insurance is a shift in pricing in some cases.

“We're seeing a little bit of a dip in some situations and some circumstances — not all — of lowered premiums in the market, which is good news for the insured,” said Clark who attributes this to insurance companies being better able to anticipate to some degree the risks depending on the type of organization.

Generative artificial intelligence (AI) also plays a role in helping companies mitigate insurance costs due to the advanced cybersecurity technologies it allows.

“In some circumstances, the use of AI in the security of an organization can be very helpful in reducing the risk and therefore can be helpful when an insurance company is determining whether they should be covered or whether they should underwrite the policy for a particular entity, as well as determining what the appropriate premium is for a particular entity,” Clark said.

She notes that the flip side of generative AI is that it can be exploited by bad actors and potentially lead to data privacy and security breaches.

“Also, there are AI risks with respect to a company using a third party's data or third-party software,” Clark said. “So that's something that I think insurance companies are examining in terms of coverage, the scope of that coverage and the amount of that coverage.”

Kevin Merriman

Kevin T. Merriman, an attorney who is a partner and team leader in the Insurance Recovery, Counseling & Litigation group at Lippes Mathias LLP says the leading causes of cyber loss continue to be ransomware, phishing scams, and other data breaches. However, the quantity and the quality of the attacks are increasing.

“Ransomware attacks are developing to extract as well as encrypt data,” said Merriman, noting that historically, ransomware attacks involved compromising a system and encrypting data so that an organization could not access that data until a ransom was paid. "There is a growing trend to extract and threaten to sell data in addition to locking organizations out of their data, adding a new layer of costs if ransom is not paid."

The industry is also seeing a rise in hacking as a service, Merriman said, where attackers are setting zero-day attacks, which exploit a vulnerability unknown to software developers, until the opportune time, sometimes selling the code for others to use.

"Dark web large language models can be used by non-tech savvy individuals to produce malicious code that can be copied and pasted to carry out an attack," Merriman said. "There is also an increase in hacking organizations selling their services."

Additionally, phishing scams that appear legitimate and convincing have been bolstered by deepfake phone calls or videos generated by AI. In Q3 2024, there was a 25% increase in the use of AI to launch more sophisticated and targeted cyber-attacks according to British IT company Haptic.

With AI being used to improve the scale and quality of cyber-attacks, Merriman says its impact on cyber insurance will take two forms – new issues in data protection and improvements to existing attacks.

"AI presents new risks in data management because it is difficult to identify precisely how AI programs use input data," Merriman said. "The emergence of AI has the potential to give rise to claims under professional liability, employment practices, general liability, and E&O policies in addition to cyber policies."

He notes that AI can be used by businesses to enhance their cybersecurity by preventing zero-day attacks by identifying system vulnerabilities, identifying and responding to attacks faster, and developing patches more quickly.

John D. Bouchard

John D. Bouchard is an attorney and vice president of Brown & Brown Insurance Services, Inc. the sixth-largest insurance broker in the world. He works from the company's Rochester office where he has a strong relationship with many of the major carriers that write cyber insurance.

"They're all struggling, frankly, with how to deal with AI," said Bouchard, who explains carriers (of which there are only about 25-30 nationwide who offer cyber insurance) are in the initial stages of understanding and defining AI in the context of coverage.

What he has seen from carriers thus far is that irrespective of whether there's a compromise of some kind, if whatever occurs (ex. a phishing attack or ransomware attack) triggers the policy, there's going to be coverage regardless of whether AI was involved or not.

"The carriers are not putting an AI exclusion on the policies, not yet," Bouchard said. "With that said, a couple of the leading carriers – to avoid any ambiguity in terms of coverage – are starting to come out with what is basically an AI endorsement that's added to the policy that specifically states that if the breach is caused by an AI actor of some kind, it's covered."

From non-profit library boards to large publicly held banks, Bouchard encourages every organization to have cyber insurance. Most will never need it for a liability claim, he says but can use it for first-party costs such as computer forensics, notifications to potential victims, business income loss and data restoration should a cyber security incident occur.

"Irrespective of the size of your organization, every entity, whether not for profit or for profit, should at least have some cyber policy in place for the real costs that are going to be incurred so that they can transfer the bulk of the cost to an insurance policy," he said.