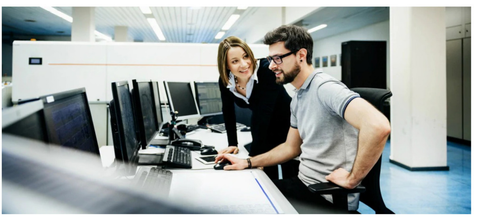
February 07, 2019

Risk Management: Do You Need Cybersecurity Insurance?

As the number of data breaches continues to grow, cybersecurity insurance may be a good idea for your business. But what if you don't have sensitive information—does it still make sense?

Rodika Tollefson
Freelance writer and journalist



In a data-driven, digital economy that relies on interconnected systems—both internally and across the vendor and partner networks—cybersecurity insurance is a smart component of risk management. For smaller organizations, however, the question of whether cybersecurity insurance makes sense is a complicated one.

To be insurable or keep premiums low, you first need to adopt cybersecurity best practices. But while many small and mid-market businesses are concerned about a cybersecurity incident or data breach, their risk management often lacks a strong cybersecurity component.

In a 2018 survey by the Insurance Information Institute and J.D. Power, nearly 60 percent of respondents said their company was very concerned about cyber incidents.

Yet only 31 percent of those companies had cybersecurity insurance, and 70 percent said they didn't plan to purchase it in the next 12 months. (Of the 536 respondents, 85 percent represented small businesses, largely with 50 or fewer employees; the rest were insurance brokers, agencies, carriers and suppliers.)

The top reason for not having coverage—cited by 42 percent of the respondents—was the notion that their business profile didn't warrant coverage.

Small breaches hardly ever make the mainstream news. This leads to denial among smaller organizations, according to leading consultant on professional liability Rick Betterley.

"Most of the data breaches they hear about are from very big companies and organizations. It's easy to read that and say, 'It's not going to happen to us'," says Betterley, who is president of independent risk-management consulting and research firm Betterley Risk Consultants and produces The Betterley Report, a cyber and privacy market survey for insurance and risk professionals published by the International Risk Management Institute.

Smaller Company Size Equals Greater Risks

The 2018 State of Cybersecurity in Small & Medium Size Businesses report sponsored by Keeper Security and conducted by Ponemon Institute debunks that "won't happen" mentality. It found that the number of small and medium-size businesses that experienced a cyberattack grew from 61 percent in fiscal year 2017 to 67 percent in FY 2018. The number of those that had a data breach grew from 54 percent to 58 percent. (Approximately 1,045 U.K. and U.S. IT and security practitioners participated in the survey, with businesses ranging from fewer than 100 employees to 1,000).

Former National Security Agency global network vulnerability analyst Terry Dunlap says businesses need to take the perspective of an attacker. Cybercriminals know it's much more difficult to "go after the guys who spend millions of dollars on their security systems."

"The attacker's going to go after the low-hanging fruit, and unfortunately that's small and medium-size businesses," says Dunlap, who co-founded ReFirm Labs, a company whose platform monitors firmware of embedded devices, and is also the founder of Tactical Network Solutions, which does tactical work for clients like the U.S. military.

ReFirm Labs has been working with insurance companies to help them better understand risks related to connected devices. The Internet of Things, Dunlap says, compounds the risks for smaller businesses because many of these devices don't have strong security features.

A 2018 survey of 605 risk-management professionals conducted by Ponemon Institute for Shared Assessments found that the number of organizations that had a data breach due to unsecured IoT devices or applications grew from 15 percent in FY 2017 to 21 percent in FY 2018. At the same time, the number experiencing IoT-related cyber attacks grew from 16 percent to 21 percent.

For smaller businesses, IoT is especially risky because they often use consumer-class devices and applications. Dunlap uses security cameras as an example. A small business is likely to buy a consumer system at an electronics store or online.

"What we have discovered, on a very routine basis, is that these consumer-grade devices are hackable, and it doesn't take a lot of skill from an attacker to penetrate these things and get into your network or steal the video feed," he says.

> "Most of the data breaches they hear about are from very big companies and organizations. It's easy to read that and say, 'It's not going to happen to us.'
>
> *—Rick Betterley, president, Betterley Risk Consultants*

He points out that many businesses have the false sense of security that their general liability policy covers cybersecurity incidents.

"Check your general liability coverage because there's a near certain chance you're not covered," he says.

Determining the Right Coverage

Risk posture and risk exposure are more important than company size or geographic reach, says cybersecurity executive leader Rocco Grillo. Think about the potential implications—from legal or regulatory issues to business interruption and customer impact.

"It really comes back to risk management from an enterprise standpoint," says Grillo, who has extensive experience with several leading security companies and has been a board adviser to industry organizations and a member of the steering committee board for Shared Assessments, a membership organization focused on third-party-risk best practices.

When the evolving technology, regulatory landscape and sophistication of attacks converge, cybersecurity insurance is one of the ways to mitigate risks. Start by identifying your most critical assets, or crown jewels, Grillo advises, and then understanding your known exposures or risks and even unknown exposures for those critical assets.

"When we're able to achieve that, we want to mitigate those risks with a comprehensive risk assessment, enterprisewide," he says.

Without going through those three steps, you don't know what cybersecurity insurance coverage you need and may allocate your policy to the wrong area, Grillo says.

Businesses that don't have sensitive or regulated information like customers' financial data or intellectual property may think they don't need cyber insurance because they're not a high risk for a data breach. Grillo recommends thinking about two other aspects of cybersecurity besides confidentiality: data integrity and availability.

"Everyone regardless of size has a critical asset and it's not necessarily regulated data," he says.

Business interruption, in fact, ranked as the top risk in 2018 among 340 businesses surveyed by global insurance company Allianz. Business interruption due to a cyberattack could mean huge financial losses for businesses from any sector.

"They may be in breach of contract, or they may lose contracts and customers, and face litigation for breach of contract," Grillo says.

Cybersecurity insurance varies widely from one carrier to the next (and often from industry to industry), and navigating policies is an undertaking in itself. Betterley says one area of differentiation is coverage for third-party exposure.

"You'd want to know that breach of your data includes data that's outside of your immediate control," he says.

He also recommends paying attention to the policy's value-added services, which sometimes are free.

Dunlap says startups likely don't have enough customers or intellectual property to warrant cybersecurity insurance, but as they mature, their assets will hold more value.

"Then you need to start considering how to protect yourself against failure in a particular area," he says. "You may need to consider it in stages, based on where you are."

Ultimately, cautions Grillo, it's important to view cyberinsurance as one component of your overall risk-mitigation strategy and not as a standalone catch-all.

"It's a misconception that if you buy cyber insurance, you're all set and don't have to worry about everything else," he says. "Cyber insurance is an excellent solution, but it's not a standalone."

Photo: Getty Images

MORE IN GETTING CUSTOMERS

How 3 Businesses Successfully Adapted to Social Distancing

What Kind of Business Should I Start? How to Decide

How to Grab the Attention of Working Mothers

How Businesses Can Use Data and Customer Service to Adapt to Social...

Want to Dig Deeper?

Rodika Tollefson | Getting Customers | Digital Tools

About the Author

Rodika Tollefson
Freelance writer and journalist