Cyberattacks prompt higher insurance premiums, lower coverage limits

September 24, 2021 | Susan Orr

KEYWORDS CYBERSECURITY / INSURANCE

(Photo illustration/Adobe Stock)

If your business's cyber insurance policy is up for renewal soon, be prepared: You might be facing higher premiums, lower coverage limits and more scrutiny of your company's cybersecurity protections.

In large part because of the recent increase in the number and severity of ransomware attacks and other cybercrimes, insurers are tightening up their cyber insurance underwriting standards.

"The application process for renewal is becoming much more stringent, more onerous," said Reid Putnam, vice president of property and casualty at Indianapolis-based broker Gregory and Appel Insurance. "This has been a real shift from where we were a year ago."

Putnam serves as chairman of the Indiana Security and Privacy Network, a volunteer-led not-for-profit that focuses on the health care industry. He also serves as an adviser to the Indiana Executive Council on Cybersecurity, created by Gov. Eric Holcomb in 2017.

Reid Putnam

Putnam said much of the shift is being driven by the pandemic and the work-from-home boom that resulted. When people started connecting to their employers' networks remotely, criminals saw security vulnerabilities they could exploit, and cybercrimes—especially ransomware attacks—exploded.

The FBI's Internet Crime Complaint Center received 2,474 reports of ransomware incidents last year, up from 2,047 in 2019 and 1,493 in 2018. The cumulative losses associated with those ransomware attacks totaled $29.2 million last year, up dramatically from $9 million in 2019 and $3.6 million in 2018.

And those ransomware incidents represent a small fraction of the 791,790 cybercrime reports made to the FBI last year, up from 467,361 in 2019.

The proliferation in cybercrimes means insurers are facing more cyber insurance claims.


Mark Swearingen

Indianapolis attorney Mark Swearingen, who specializes in health care law and health information privacy at Hall Render Killian Heath and Lyman PC, said his law firm used to see one or two cyber incidents each month among its clients. Since the pandemic began, he said, the volume of incidents has doubled or tripled.

In response, Swearingen said, his clients whose cyber insurance policies are up for annual renewal are seeing everything from increased premiums to reductions in coverage limits and increases in deductibles. The insurers are also requiring clients to adopt certain policies and procedures.

All of this started over the past three to six months, Swearingen said. “It’s a dramatic change.”

Higher cost, less coverage

Cyber insurance can include a variety of coverages. A policy might cover the business costs associated with a data breach or cyberattack such as data recovery, forensic investigations, communications with customers and lost business. It might also cover the cost of a ransomware payment, or the legal costs if a company is sued over a data breach or other incident.

According to The Council of Insurance Agents and Brokers’ second-quarter commercial property and casualty market index, released last month, premiums for cyber insurance rose an

average of 25.5% last quarter, following an average increase of 18% in the first quarter and 11.1% in the fourth quarter of last year. In comparison, the average premium increase for all types of property and casualty insurance combined was 8.3% during the second quarter.

Some individual carriers increased their premiums even more. American International Group Inc., commonly known as AIG, said its cyber insurance rates were up nearly 40% in the second quarter over the same period a year earlier.

Putnam said some of his customers have seen premiums increase as much as 100%.

In addition to raising its premiums, AIG is also taking other measures.

“We continue to carefully reduce cyber limits and are obtaining tighter terms and conditions to address increasing cyber loss trends, the rising threat associated with ransomware and the systemic nature of the cyber risk,” AIG President and CEO Peter Zaffino said during an earnings call last month.

In many cases, insurers are imposing new requirements about what customers must do to even be eligible for cyber insurance.

Ron Pelletier

“Are you insurable? That’s the big question now,” said Ron Pelletier, founder and chief customer officer at Indianapolis-based cybersecurity firm Pondurance LLC. Insurers “are being much more discerning about who they underwrite.”

Pondurance works with companies to both reduce their online risk and to respond to incidents once they happen. Pondurance

also works with insurers to help them understand security risks their customers may face.

Better security standards

Before they write or renew a cyber insurance policy, insurers are putting more scrutiny on their clients' internet security practices and protections.

Some insurers are requiring that clients strengthen their employee training and testing programs. This might include not only training employees about best security practices but actually putting employees to the test by sending out fake emails and seeing how many people click on suspicious attachments or links.

"People continue to be our weakest link in all of this," Putnam said.

He advises clients to conduct tabletop exercises in which the company goes through a simulated cyberattack and practices how it would respond.

A cybersecurity practice known as multifactor authentication is also becoming a common requirement, Pelletier said. A company might, for instance, have an employee log on to the computer system by entering his or her username and password, then receiving a unique code via smartphone that also must be entered.

Insurers also want their cyber insurance clients to have strong security processes, Pelletier said. This can include policies about which employees have access to certain company information, and processes for verifying the legitimacy of a password-change request or a funds transfer.

Policyholders might also be required to employ technology like antivirus software and end-point detection and response systems, which can monitor and respond to unusual or unauthorized network activity.

Insurers are also starting to require that their cyber insurance clients include cyber incidents in their business continuity plans, just as they might for floods, fires or other disasters.

“Insurers are looking at these things very closely, so they know who they’re insuring and what they’re insuring,” said Janet Ruiz, director of strategic communications at the New York City-based Insurance Information Institute Inc.

Certain types of clients might be more at risk of cyberattacks, Ruiz said. If criminals are looking for personal information they can steal, health care providers, financial firms and colleges are common targets.

If the criminals have a ransomware attack in mind, “They’re really going after whoever they think they can get to,” Ruiz said. “That’s really kind of a wide range.”

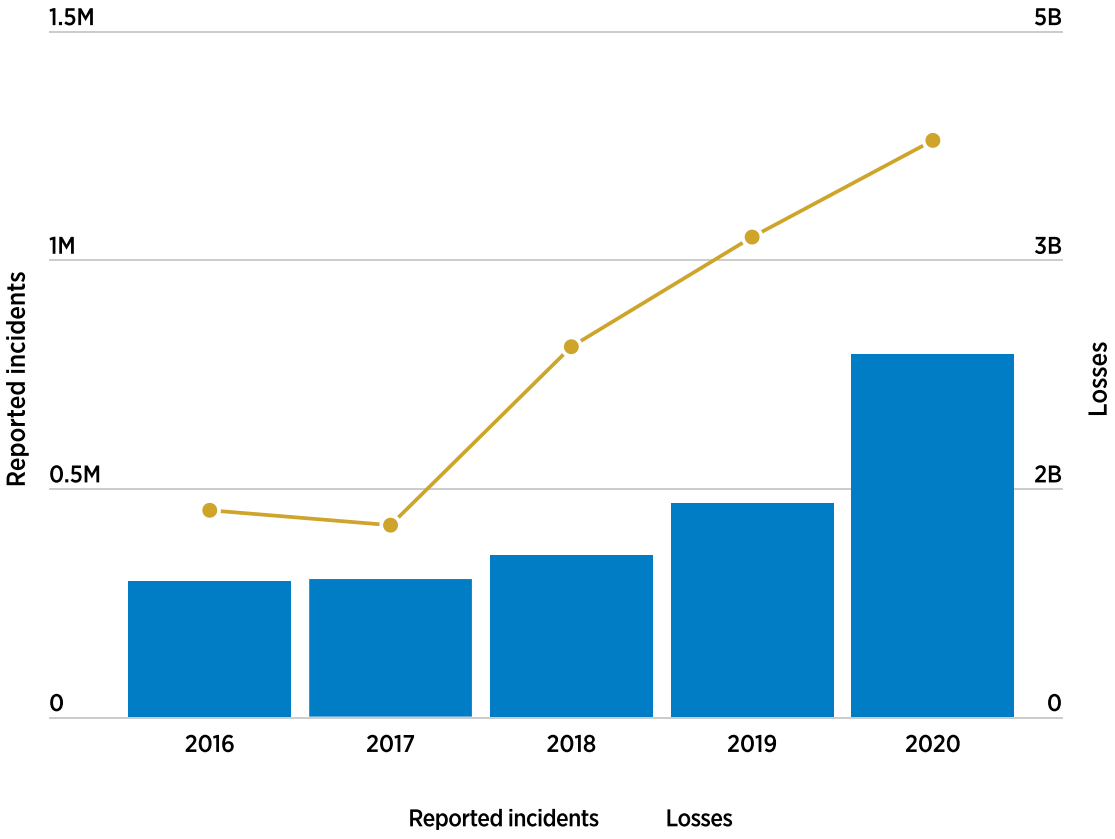
Just last month, Eskenazi Health shut down its data network and diverted ambulances in response to what the hospital system called an “attempted ransomware attack.” Eskenazi later said some of its data was obtained and released online, and that employees, patients, providers and vendors should watch their bank and credit-card statements for signs of suspicious activity.

Around the country, the Georgia-based energy company Colonial Pipeline, Colorado-based meat producer JBS USA Holdings Inc., and the Washington, D.C., police department have also been ransomware victims so far this year.

Cybercrime on the rise

The number of internet crimes reported to the FBI, and the financial losses suffered in those crimes, has been rising in recent years.

All types of cybercrime



Some subcategories

Business or individual email account compromise

	Reported incidents	Change	Losses	Change
2018	20,373		$1.3B	
2019	23,775	▲ 16.7%	$1.8B	▲ 38.5%
2020	19,369	▼ 18.5%	$1.9B	▲ 5.6%

Corporate data breach

	Reported incidents	Change	Losses	Change
2018	2,480		$117.7M	
2019	1,795	▼ 27.6%	$53.4M	▼ 54.6%
2020	2,794	▲ 55.7%	$128.9M	▲ 141.4%

Health-care related

	Reported incidents	Change	Losses	Change
2018	337		$4.5M	
2019	657	▲ 27.6%	$1.1M	▼ 75.6%
2020	1,383	▲ 110.5%	$29.0M	▲ 2,536.4%

Intellectual property theft/counterfeiting/ copyright infringement

	Reported incidents	Change	Losses	Change
2018	2,249		$15.8M	
2019	3,892	▲ 73.1%	$10.3M	▼ 34.8%
2020	4,213	▲ 8.2%	$5.9M	▼ 42.7%

Malware/scareware/virus

	Reported incidents	Change	Losses	Change
2018	2,811		$7.4M	
2019	2,373	▼ 15.6%	$2.0M	▼ 73.0%
2020	1,423	▼ 40.0%	$6.9M	▲ 245.0%

Phishing/vishing/smishing/pharming

	Reported incidents	Change	Losses	Change
2018	26,379		$48.2M	
2019	114,702	▲ 334.8%	$57.8M	▲ 19.9%
2020	241,342	▲ 110.4%	$54.2M	▼ 6.2%

Ransomware

	Reported incidents	Change	Losses	Change
2018	1,493		$3.6M	
2019	2,047	▲ 37.1%	$9.0M	▲ 150.0%
2020	2,474	▲ 20.9%	$29.2M	▲ 224.4%

Spoofing

	Reported incidents	Change	Losses	Change
2018	15,569		$70.0M	

2018	15,569		$70.0M		
2019	25,789	▲	65.6%	$300.5M	▲ 19.9%
2020	28,218	▲	110.4%	$216.5M	▼ 6.2%

Source: FBI Internet Crime Complaint Center 2020 Internet Crime Report

Ransomware payments

To combat ransomware specifically, Ruiz said, some insurers are lowering their coverage limits for ransomware payments. Criminals who have breached a company's system sometimes look up a victim's insurance policy and tailor their ransomware demand to the amount of the victim's coverage, Ruiz said. Therefore, insurers are reducing their ransomware coverage with the theory that lower payouts will make ransomware less attractive to criminals.

Many criminals demand ransomware payments be made in cryptocurrency as a way to hide their identities. For this reason, Ruiz said, insurers are also lobbying for stricter regulations on cryptocurrency.

Jim Goldman

Since the components cyber insurance covers—the internet, online data stores and the like—are relatively recent developments, it has existed only since about the late 1990s, said Jim Goldman, CEO and co-founder of Indianapolis-based Trava Security Inc.

But it's becoming a topic of increasing importance for all businesses, Goldman said.

Trava, a High Alpha company, helps clients assess and mitigate their cybersecurity risks. The firm is also an insurance broker for cyber insurance carriers, and it's working toward developing its

own digital insurance policy platform so it can do its own underwriting.

Goldman said it's becoming more common for companies to require cyber insurance of their business partners. As of last year, he said, only 35% to 40% of small to medium-size businesses carried cyber insurance. But he expects that to grow.

"More and more, regardless of the size of the company, it's becoming a requirement to do business," Goldman said.

"All of a sudden, business has woken up to the fact. 'Wow, this is a real potential risk for us.'"•

Editor's note: Please note our updated comment policy that will govern how comments are moderated.