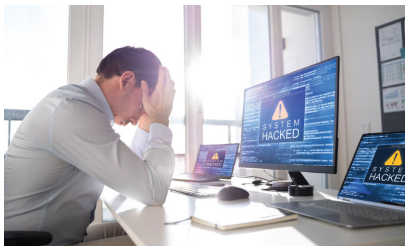
BUSINESS INSURANCE.

Prompt notification of cyber insurers can mitigate effects of hacker attacks

Posted On: May. 3, 2023 12:00 AM CST

Judy Greenwald



One of the first things an organization should do if it suspects it is the subject of a cyberattack is contact its cyber insurer.

In addition to putting the insurer on notice of a potential claim, the policyholder may be able to access a range of incident response experts through the insurer. Also, the coverage often requires that a policyholder only use pre-approved vendors, experts say.

The policyholder should then, under the guidance of legal advisers, promptly notify regulators, customers and investors of an incident.

Before an incident occurs, carefully and correctly filling out cyber insurance applications can help smooth the claims handling process and avoid friction with insurers (see related story).

Policyholders should contact their insurers at the first suspicion of a cyberattack, said Theresa Le, Cupertino, California-based chief claims officer for Cowbell Cyber Inc. They should do this even if "it's not altogether clear" there has been an attack, she said.

And policyholders shouldn't attempt to investigate the incident alone, according to experts.

By acting alone, policyholders without cybersecurity expertise may corrupt evidence and worsen the situation, said Matthew Cullina, Providence, Rhode Island-based head of global cyber insurance business for CyberScout LLC, a data breach services company.

When an incident occurs, policyholders should have information including the name of the policyholder, the insured entity's name and address, a description of the loss, and, if relevant, a screenshot of the ransomware demand, said Joni Mason, New York-based senior vice president, national executive and professional risk solutions claims practice leader, of USI Insurance Services Inc.

"It is more important to make the call promptly than it is to have everything on hand to answer every question the insurance company might have for you," said Tim Zeilman, Simsbury, Connecticut-based global cyber product owner at Hartford Steam Boiler Inspection and Insurance Co., a Munich Reinsurance Co. unit.

"You don't have to spend the next 10 hours figuring out what happened," said Tara Bodden, general counsel, head of claims, at insurtech managing general agency At-Bay Inc. in San Francisco. "That's our job, to help through all the investigations."

Observers give insurers high marks for their cyber claims handling.

CLICK IMAGE TO ENLARGE

PREPARING FOR CYBER CLAIMS

To limit disputes over cyber liability insurance claims, policyholders should:

- ✔ Fill out insurance submissions with care and accuracy.
- ✔ Be sure privacy policies line up with security practices.
- ✔ Closely examine the coverage and ask questions if unclear.
- ✔ Call the insurer promptly as soon as an incident is suspected.
- ✔ Contact a data breach attorney immediately after calling the insurer.
- ✔ Notify regulators, customers and investors of any incident.
- ✔ Avoid independently hiring vendors or launching an investigation.
- ✔ Use only insurer-approved vendors.
- ✔ Check whether ransomware hackers are on the U.S. Department of Treasury's Office of Foreign Asset Controls' sanctions list.

Source: *Business Insurance* interviews

"They're doing an excellent job," said John Farley, New York-based managing director of Arthur J. Gallagher & Co.'s cyber liability practice. Claims disputes occur in all lines of coverage, but, overall, insurers are responding to cyber claims, he said.

Axa XL, a unit of Axa SA, has a 24/7 hotline for cyber incident reporting, said Danielle Roth, New York-based head of cyber and tech E&O claims for the insurer. After the call is made, a handler will soon respond and make the initial intake call to get more information, with the understanding that at that point there are a lot of unknowns.

The panels of experts that insurers have available include lawyers, allowing policyholders to quickly contact a breach attorney.

An attorney will "provide a cloak" of attorney-client privilege around the subsequent process, said Karrieann Couture, Chicago-based assistant vice president and cyber E&O claims leader at Aon PLC.

Attorneys will also "help guide (policyholders) through the legal minefields they'll have to negotiate," Mr. Farley said. With insurers' 24/7 hotlines, "you'll get an attorney any time you need one," he said.

Using pre-approved vendors reduces the potential for claims disputes. Evan Bundschuh, commercial lines manager for brokerage Gabriel Bundschuh & Associates Inc. in Scarsdale, New York, said he has seen instances where policyholders who hired a forensic investigator without first getting their insurer's approval were later told the costs would not be covered.

Insurers are "just not making room for exceptions on this," said Ms. Mason of USI.

In addition, policyholders should be aware of cyber disclosure regulations and adhere to any pertinent notification laws in a timely manner, whether applicable to regulators, customers, investors or other affected parties, Mr. Bundschuh said.

If policyholders are subject to a ransomware attack, cybersecurity companies will arrange for ransom payments on the policyholders' behalf. When situations develop, "our firm gets pulled in to negotiate with the bad guys and manage transactions," including obtaining bitcoins, said Darin Bielby, Philadelphia-based managing director of Cypfer Corp., a cybersecurity company.

Paying ransomware demands, though, is not necessarily recommended.

"The decision to pay or not pay is not black and white," said Lindsey Nelson, London-based cyber development leader for CFC Underwriting Ltd.

There are "lots of considerations needed to be made" and making an informed decision "is incredibly important when it comes to claims litigation," she said.

Among other considerations, policyholders should be aware that they and their insurers face penalties if they facilitate ransomware payments to entities sanctioned by the U.S. Department of Treasury's Office of Foreign Asset Controls. Such entities might include organizations affiliated with or controlled by governments hostile to the United States, terrorist groups or drug traffickers.

However, companies that are attacked by state actors will still be covered for restoring their operations, said Deborah D'Angelo Hirschorn, New York-based managing director, U.S. cyber and technology claims leader, for Lockton Cos. LLC.

While "it's more common to get the full coverage," for ransomware attacks, some insurers have sublimits or co-insurance provisions for ransomware-related events, said Ms. Couture of Aon.

Meanwhile, the impact on the claims process of the Lloyd's Market Association's introduction in March of four new war, cyber war and limited cyber operations exclusions for standalone cyber insurance policies is undetermined.

"You wonder how long the claim will take to be adjusted" as insurers determine to which entity a cyberattack should be attributed, Ms. Hirschorn said.

If policyholders do not get the coverage they thought they were entitled to, they should assemble the facts of what was needed for "a complete fix" to obtain coverage, said Daniel J. Healy, a partner with Brown Rudnick LLP in Washington.

When claims are covered, insurers are reluctant to pay for system upgrades intended to prevent a future attack, said John Scordo, New York-based cyber claims advocacy leader for Marsh LLC. It is not considered "relevant to the incident," he said.

And "silent cyber," or cyber-related coverage contained within other property/casualty policies, remains a concern for insurers that have sought to eliminate coverage for cyber risks from nonspecialist policies, experts say.

While cyber policies have been available for more than 20 years, observers say there has been relatively little litigation over the coverage, so there are few guiding precedents.

"Cyber coverage is a new animal in the scale of things, and we don't have a really developed body of case law on cyber and insurance issues," said Robert L. Wallan, a partner with Pillsbury Winthrop Shaw Pittman LLP in Los Angeles.

Furthermore, because of confidentiality provisions, it is unknown how many cases are settled, he said.

"I haven't seen a ton of disputes over the coverage from the cyber forms," said Thomas H. Bentz Jr., a partner with Holland & Knight LLC in Washington.
