Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Global Ransomware Attack Shows Cyber Coverage Is Critical

By **Jeff Sistrunk**

Law360, Los Angeles (May 15, 2017, 10:55 PM EDT) -- A massive global cyberattack that began Friday illustrates the need for businesses to obtain robust insurance policies to cover everything from hackers' ransom demands to restore system access to business interruption losses, experts say.

The wide-ranging attack, carried out by hackers wielding ransomware dubbed "WannaCry," has hit public institutions and private business alike in 150 countries. Britain's national health system, FedEx and the Russian Interior Ministry are among the most high-profile of the tens of thousands of victims. The malicious program locks users out of their computer systems and blocks access to data until a ransom is paid.

While maintaining comprehensive cybersecurity measures is critical, broad insurance coverage is equally important for companies and institutions to protect themselves against risks such as the WannaCry attack, according to experts.

"Clearly, companies should be engaging in sound cybersecurity practices and employing security patches in a timely fashion," said Roberta Anderson, a partner in Cohen & Grigsby PC's data security and insurance recovery practice groups. "However, there is no such thing as perfect cybersecurity. The very reason companies purchase insurance is because things go wrong."

Here, experts discuss how companies can best shield themselves from the ever-evolving ransomware threat.

Include Cyberinsurance in a Response Plan

As the WannaCry attack demonstrated, new cyber risks can emerge out of the blue and strike suddenly and mercilessly. For that reason, experts say, it is essential for a company to have a well-defined incident response plan mapped out in advance — and that plan should include a cyberinsurance policy with expansive coverage for digital extortion.

According to experts, companies can negotiate with cyberinsurance carriers to obtain extortion coverage that will encompass payments made in either cash or bitcoin, as well as any other forms of nonmonetary consideration demanded by hackers.

For example, one common form of ransomware coverage on the market defines "cyber-extortion

expenses" as "reasonable and necessary money, property or other consideration surrendered as payment" by the policyholder with the insurer's consent in order to prevent or limit a cyber-extortion threat, which, in turn, is defined as a threat to the insured's business operations or to alter, damage or destroy data on the network, among other things.

On top of helping to cover an insured company's payment of a cyber-extortion demand, a cyberinsurance carrier can also aid the company at the outset of a hacking incident by leveraging the expertise of outside data security specialists. Many cyberinsurance policies provide that the insurer will pay for forensic analysts to investigate the cyber incident and for data breach liability "coaches" to counsel the policyholder through potential risks tied to the hack.

"Insurers can be very helpful for companies, particularly companies that are not large and sophisticated and need help in dealing with these crises," Anderson said.

Avoid Exclusions for Inadequate Security

In order to obtain cyber coverage, companies typically have to attest to maintaining certain "reasonable" data security standards, and some cyber policies contain exclusionary language allowing insurers to deny coverage if the policyholder fails to uphold those standards.

Those types of policy requirements could potentially pose problems for insureds affected by the WannaCry attack and similar incidents. Security researchers have said many of the computers targeted by WannaCry were running Windows XP, a legacy system that Microsoft no longer supports, meaning that security patches are no longer issued.

Microsoft issued a new patch on Saturday for the vulnerability in unsupported Windows XP systems, but if a company failed to install the patch and its computer system was later infected with the ransomware, a cyberinsurance carrier could deny coverage on the basis that the insured didn't take reasonable steps to prevent the infection, according to experts.

"These cyber policies typically have requirements that system administrators or chief IT officers take reasonable steps to make sure their systems are reasonably hack-proof," said Jenner & Block LLP partner Matthew L. Jacobs. "If Microsoft sent around a patch that allegedly could have prevented these malware attacks in a timely manner, and insureds didn't take advantage of it, insurers could use that fact to argue against coverage."

When shopping for cyberinsurance, therefore, companies should avoid buying policies permitting insurers to deny a claim if the policyholder fails to employ certain security measures, attorneys say.

"Aggressive positions taken by insurers are troubling for the cyberinsurance marketplace, because so many cyberinsurance claims start with some kind of failure or problem," said Barnes & Thornburg LLP partner Scott Godes. "If there were no failures or problems, there would be no need for cyberinsurance to cover these types of risks. Even if a company takes the most steps possible to prevent an incident, there is always the chance that something could go wrong."

Identify All Potentially Implicated Policies

The actual ransom payment demanded by cyber-extortionists is rarely the greatest financial risk posed by a ransomware attack, experts say. The hackers behind WannaCry, for instance, are demanding just

$300 in bitcoin from targeted users, and as of Monday afternoon, they had pulled in less than $60,000 in ransom payments, according to data from Elliptic, which tracks "illicit" bitcoin transactions.

However, an interruption in computer access — even if it only lasts for a few hours while a company is going through the process of making a ransom payment — can have potentially devastating consequences, particularly for small businesses and for health care providers and other institutions that treat injured patients. Britain's National Health Service, for instance, said Friday that 16 of its hospitals had been hit by WannaCry, leading to delays and cancellations.

While no injuries have been reported in connection with the hospitals' troubles from the ransomware attack, such risks remain within the realm of possibility and could carry another layer of exposure, according to experts.

"We could certainly see some type of bodily injury or malpractice insurance claims arise where an allegation is made that the facility is responsible not only for the patient's health but securing data so they can treat patients on an emergency basis," said Anderson Kill PC shareholder Joshua Gold.

Cyber policies usually exclude coverage for any claims stemming from bodily injury, so a company facing injury claims following a ransomware attack would have to look to a general liability or other policy for coverage. And policies in a company's arsenal may provide coverage for property damage and other losses resulting from hacking incidents, according to experts.

"When an event like this hits, policyholders should inventory of all of their insurance policies to see which ones get noticed," Gold said. "Even if one doesn't have a cyber policy, there may be other policies that respond to this type of loss. Property insurance policies often provide some measure of cyber protection. Following certain hacking events, the majority of policyholders have won the battle over whether there was 'physical' damage. Critically, property policies may also cover business interruption."

When in Doubt, Always Give Notice

A company eager to regain access to its computer systems after a cyber-extortion attack may make the ransom payment without informing its insurers, especially if the demand is below the applicable deductible.

However, experts say such a move can prove to be a mistake if the company is later hit with another cyberattack carried out by the same hackers or involving similar circumstances. If that happens, an insurer may argue that the policyholder's failure to give notice of the earlier attack is fatal to coverage.

"Sometimes, even after a target buys the decryption key and unlocks its system, the malware stays on the system and may trigger another attack in, say, six months, if it is not removed following a forensics analysis," said Jacobs. "That could cause problems for coverage purposes if the second attack is traced back to the first. The insurer on the risk during the second attack may argue that the insured didn't disclose the first attack adequately when it applied for the new policy. It would become a question of whether that constitutes material nondisclosure."

Indeed, even demands for a small ransom shouldn't be viewed as a "nonreportable event," according to Anderson. Instead, experts say, companies should always err on the side of caution and notify all insurers whose policies could potentially be implicated by a cyber incident.

"Notification is a low-hanging fruit, and it easy for an insurance carrier to argue that you didn't provide notice fast enough, so providing timely notice to all insurers whose coverages are potentially implicated is key," Anderson said.

--Additional reporting by Allison Grande. Editing by Mark Lebetkin and Aaron Pelc.
