BARNES & THORNBURG LLP

A Ransomware Attack Could Devastate Your Company. Will Your Insurance Cover It?

November 4, 2019 | Policyholder Protection,Cyber Insurance,Data Security

Carrie Marie Raver
Partner
Insurance Recovery and Counseling Group Co-Chair

What Is Ransomware?

Ransomware is a form of electronic kidnapping. Typically, cybercriminals use malicious software to gain access to your company's computer systems or files and block user access. Hackers hold the systems or files hostage using encryption until the victim organization pays a ransom in exchange for the encryption key. The hackers then – if they are "reputable" criminals – supply the organization with a key that permits the organization to access the systems or files encrypted by the software.

How does this happen? Hackers perpetrate ransomware attacks by sending phishing emails that appear legitimate to unsuspecting employees, who then click on the emails and introduce the malware onto the organization's systems. Ransomware may also be triggered by an employee's visit to an infected website or to an advertisement containing malware injected into a legitimate website.

Ransomware Trends

RELATED PRACTICE AREAS

Commercial General Liability
Copyright, Trademark, and Media Liability
Credit and Mortgage Insurance
Data Security and Privacy
Directors and Officers Liability
Employment Practices Liability
Fidelity Bonds and Commercial Crime Policies
First-Party Property
Insurance Recovery and Counseling
Internet and Technology
Ocean Marine and Cargo Coverage
Professional Liability
Representations and Warranties
Workers' Compensation and Employers' Liability

RELATED TOPICS

Cybersecurity
Cyber Insurance

Why should companies be concerned about this risk? Because the frequency and severity of these attacks are on the rise. Hiscox, a liability insurer, recently reported in its Cyber Readiness Report 2019 that "[b]oth the costs and frequency of attacks have increased markedly compared with a year ago." Another insurer, Beazley Group, reported a "105% increase in the number of ransomware attack notifications against clients compared to Q1 2018." In the same report, Beazley stated that "in the first quarter of 2019, the average ransomware demand reported to the [Beazley Breach Response] BBR Services team was 93% higher than the 2018 average."

Also in the spotlight are reports of crippling ransomware attacks perpetrated against local governments. The computer networks for the cities of Atlanta, Newark and San Diego (as well as major health care providers, the University of Calgary and others) were infected with SamSam ransomware. The FBI reports that the "toll of these cyberattacks was staggering: more than 230 entities infected, $6 million in ransom payments extorted, and an estimated $30 billion in damages to the affected public and private institutions."

Baltimore also suffered a ransomware attack on May 7, 2019, that led to the email accounts of city employees being shut down for nearly three weeks. The Baltimore Sun reported that "Baltimore's budget office estimates a ransomware attack on city computers will cost at least $18.2 million – a combination of lost or delayed revenue and direct costs to restore systems."

Cyber Extortion Coverage

After all of this bad news, consider some good news: There is insurance for these risks. A best practice for companies and governments is to consider procuring a first-party cyber insurance policy that provides coverage for cyber extortion and ransomware events, as well as third-party coverage for liability to others arising from cyber events (such as liability to a customer the policyholder cannot serve because of a ransomware attack).

Insureds must do their homework when purchasing a first-party cyber policy covering their out-of-pocket losses resulting from ransomware and other cyber intrusions, working alongside experienced brokers and cyber coverage counsel to carefully study the following extortion-related definitions, terms and conditions:

High-Level Considerations

A best practice for insureds is to purchase coverage for extortion demands and ransom payments, lost income resulting from the ransomware attack, extra expenses incurred to keep the business running, defense and indemnity for customer claims and other losses that could result from these events.

Definition of Extortion Should Be Broad

The definition of extortion defines the trigger for coverage of ransomware attacks. Insureds should understand the policy's extortion definition and determine if they agree with the insurance company drafter's characterization of the hazard. For example, an insurer may define extortion as involving an explicit threat to misuse or sell information. The insurer may deny coverage if the ransomware attack on your organization involves only a demand for

money.

Secure Consent by the Insurer to Pay Ransom

Extortion coverage very often requires insureds to seek and obtain written consent from the insurer before agreeing to pay the ransom. A slow insurer response may lead to delayed payments and increased monetary demands by the cyber thieves. Insureds put their extortion coverage at significant risk if they do not obtain their insurers' prior written consent before paying a ransom.

Notice to the Insurer

Insureds should avoid making the assumption that a low ransom demand negates the need to provide notice of the attack to their insurers, or that strategic withholding of notice will ultimately cost them less by controlling premiums. When an organization gets hit with a ransomware attack, it should notify all of its liability and first-party insurers of the attack. The small demand could turn into a much larger demand at some point, which the insurer may refuse to pay based on late notice. If this happens, any premium savings that might have been achieved by withholding notice could be dwarfed by the non-covered loss. Notice to all relevant insurers is also important because coverage may also be provided under non-cyber liability policies such as liability, crime and property policies.

Avoid Sublimits If Possible

Certain insurance policies set a lower limit of coverage for cyber extortion and ransomware attacks. For example, a $10 million limit cyber policy may provide only $500,000 for cyber extortion. Insureds should consider whether a proposed sublimit amount is sufficient to cover a possible ransomware attack. Many insurers provide a full limit of liability for cyber extortion events, and the full policy limit might be offered without an additional premium.

Deductibles Must Be Considered

A deductible for a ransomware event may be so high that your organization will be forced to pay a ransom demand from its own pocket. Insureds should consider how much financial responsibility is cost-effective to retain, and adjust the deductible to reflect this.

Cooperation Is Key

Cyber policies require insureds to cooperate with the insurer regarding coordination with relevant law enforcement and regulatory authorities. Often, policies state that the insured may not disclose the existence of cyber coverage to the cybercriminals (or risk rescission of the policy), and that insureds must use expert incident response service providers and legal counsel selected and appointed by the insurer.

Consider Insurer Reputation

Insureds should consult with their cyber coverage counsel and cyber broker

regarding the reputation of the insurers before buying cyber extortion coverage. Insurers' track records for paying ransomware attack claims and other cyber breaches should be considered.

Getting the right cyber extortion policy is all about sweating the details. If the insured makes the correct buying decision, the pain and business disruption of a ransomware attack can be minimized. If it buys the wrong coverage, or has no coverage at all, they can be a costly distraction at best, and catastrophic at worst.

This article was originally published in the Fall 2019 edition of Corporate Policyholder Magazine.