Lowenstein Sandler

Information Age

September 29, 2017

Ransomware, Cyber Insurance and Cryptocurrency: Are You Covered?

By Rob Reznick, Flashpoint, Matthew Savare, Lowenstein Sandler LLP, and Eric Jesse, Lowenstein Sandler LLP

The Problem

Rampant, worldwide cyber security incidents such as data breaches, phishing attacks, and malware across various industries have caused tremendous damage (physical, monetary, and reputational) to companies and consumers. One only has to open a newspaper (likely a digital one) to witness a new attack. Just in recent years, billions of records have been compromised in massive, high-profile breaches.

Although not a new phenomenon, ransomware has emerged as another nefarious cyber threat. Insurance company Beazley reports that the number of ransomware attacks reported by its insureds quadrupled from 2015 to 2016. In 2016 and 2017, various strains of ransomware such as WannaCry and Petya have entered the global lexicon and wreaked havoc on hundreds of thousands of computers.

Even though each ransomware attack is different, a consistent pattern has emerged. The perpetrator releases some type of malware that encrypts the files on a system's hard drive. The victim is then sent a ransom demand in exchange for the key to decrypt the data. Recently, the ransom demand is almost invariably in some form of anonymous, difficult-to-track cryptocurrency, such as Bitcoin.

Such ransomware attacks have affected numerous industries, most notably the healthcare and financial industries, which rely so heavily on data. For instance, in February 2016, Hollywood Presbyterian Hospital in Los Angeles reported that it paid the Bitcoin equivalent of $17,000 after cyber criminals locked its patient and doctor records for almost two weeks. More recently, in June 2017, South Korean web provider, Nayana, paid the Bitcoin equivalent of $1 million after a ransomware attack had locked up more than 3,400 websites.

Cyber experts and government officials almost universally recommend not paying any such ransoms, because there is no guarantee that the cyber criminals will honour the bargain, and the common fear that any payments will embolden the rogues leading to more and greater demands.

What is a company to do, however, if the loss of its data paralyses its operations and risks immediate, significant, and irreparable harm? For Nayana and numerous other victims, paying the ransom has been the answer.

In such cases, damages arising from business interruption and the costs of remediating the incident (e.g., notifying affected individuals, conducting a root cause analysis and addressing any security vulnerabilities, and reputational harm) frequently far outweigh the ransom payment. When aggregated, these damages and costs often run into the millions.

Insurance, part of the solution

With the meteoric rise in cyber incidents, many companies have purchased cyber insurance policies. Could a cyber policy cover ransomware attacks? Does it matter if the victim pays the ransom in Bitcoin or some other cryptocurrency? What steps need to be taken to secure coverage if there is an attack? As cyber policy forms continue to evolve, the devil is in the details. Therefore, companies, with the aid of their insurance broker or coverage counsel, must delve into those details to fully understand the scope of coverage.

In addition to insuring the remediation costs for a data breach, business interruption, or lawsuits by those affected, many cyber insurance policies on the market today include "cyber extortion" or "ransomware" coverage. Even so, that coverage may not be adapted to current risks. For instance, many standard cyber policies that insure cyber extortion do not expressly contemplate covering a ransom demanded in Bitcoin or other cryptocurrencies.

In those cases, insurers may deny coverage, using the policy's silence to their advantage, thus setting the stage for a coverage battle. But a proactive policyholder can avoid that. Many insurers will amend their standard policy forms to explicitly cover ransom demanded and paid in a digital currency. But companies need to ask for it.

Maximising cyber extortion coverage also requires companies to understand other policy components.

Cyber policies provide a limit of liability, but certain types of coverage, like cyber extortion, are often subject to much lower sub-limits.

A sub-limit of $50,000 for cyber extortion may suffice for some companies, but be wholly inadequate for others. Rather than being surprised by the amount of any sub-limit after the ransom demand is made, companies should purchase insurance eyes wide open and confirm that any sub-limits are consistent with their risk tolerance.

In the same vein, cyber extortion coverage often extends to credible threats by a hacker to enter a company's network, shut down its website, or infect its computer systems unless a ransom payment is made. But who decides whether the threat is credible?

Companies cannot afford to debate the credibility of a threat with insurers while the hacker's countdown clock ticks and the company is in imminent risk of reputational and/or financial harm. This pitfall, like others, can be avoided by understanding the policy's terms at the outset and insisting that insurers amend any deficient policy to give company executives the sole discretion to determine the credibility of a threat.

If and when a cyber extortion threat is made, companies will need to respond immediately. But in the (hopefully controlled) chaos of the moment, insurance cannot be forgotten.

Many insurance policies require immediate notice of cyber extortion threats or ransom demands. And many policies will require the insurer's consent to any ransom payment – whether in Bitcoin or otherwise – for it to be covered. Therefore, companies' response plans must incorporate cyber insurance, starting with an understanding of the policy's notice requirements.

Article Link:
http://www.information-age.com/artificial-intelligence-right-123468747/

Contacts

Please contact the listed attorneys for further information on the matters discussed herein.

Matthew Savare, Esq.
Partner
T 646.414.6911 | msavare@lowenstein.com

Eric Jesse, Esq.
Counsel
T 973.597.2576 | ejesse@lowenstein.com