CRC Group
Wholesale & Specialty

State of the Market

Ransomware Attacks Show Benefits of Cyber Insurance

Ransomware Attacks Show Benefits of Cyber Insurance

If 2016 was a year of increased ransomware attacks, just wait. Ransomware risks are becoming frighteningly pervasive.

The Los Angeles Times, in an article published March 8, presciently stated that "2016 is shaping up as the year of ransomware." According to a report by Internet security firm McAfee, more than 100,000 new ransomware variants are released daily by hackers targeting unsuspecting e-mail users. Even more disturbing, McAfee has observed ransomware-as-a-service -- malware available for sale -- on the anonymous Tor network.

Online Anonymity

- Tor is a network of servers that support anonymous Internet browsing and communication. The goal of the volunteer organization that maintains Tor is to protect users' privacy and freedom from surveillance. Tor users are diverse, ranging from the armed forces to political dissidents to human rights activists to hackers. Using the Tor browser, it is possible to search hidden sites that are beyond the reach of standard web browsers. This small subset of sites is known as the Dark Web, which facilitates illicit activities and is where ransomware-as-a-service resides.

At its core, ransomware is simple extortion. Hackers gain access to computer systems by hiding their malware in security patch updates or inducing e-mail users to click on an attachment or phishing link. These actions activate the ransomware, locking down the computer or encrypting files. Computer users are greeted with an onscreen demand for payment in exchange for decryption keys. These demands are often nominal, most under $1,000, and payable in cryptocurrency such as bitcoin. In February 2016, Hollywood Presbyterian Medical Center was hit by a ransomware attack and paid the attackers' demand for $17,000. Organizations that fail to pay such ransoms risk the permanent loss of their files, unless they have separate backups in place to restore them.

There is no guarantee that paying a ransom in exchange for decryption keys will work, but hackers realize that victims will ultimately stop paying if the keys fail. In a report by TechNewsWorld, 72 percent of companies infected could not access data for at least two days and 32 percent could not for five or more days. Denial of access to any files can halt a business in its tracks, resulting in an immediate loss of productivity. For some organizations, particularly healthcare and e-commerce companies, denial of access to patient records or customer transactions for any period of time is likely to also create a significant financial loss.

For an organization without backup files or that cannot tolerate any delay in access to files, there is no option but to pay the extortion demand and hope the decryption keys work. For those unable to restore their files, the financial impact may be nearly incalculable. Years' worth of valuable proprietary information such as research documents, patents, designs, formulas, customer files, accounting records and other information could be lost.

For criminals, ransomware attacks are low risk and high reward. With payment in anonymous cryptocurrency and no way to trace the attackers as the encrypted data remains on the victim's network, the risk of arrest is low. It is turning into a high-profit, volume-driven enterprise, with ease of entry. With no easy form of defense, a critical action to mitigate the risk of ransomware is to educate individuals to scrutinize suspicious emails, which may look surprisingly authentic.

Cybersecurity experts say it is possible to mitigate most forms of ransomware through an application whitelist, which allows only approved files to execute. The downside to a whitelist is it creates a much more restrictive environment for users, who may be accustomed to using their Internet connections for both personal and professional purposes. Many organizations are simply reluctant to impose that kind of restriction.

Experts have offered conflicting advice on responding to ransom demands. The FBI, for example, in 2015 advised victims to pay ransom demands. In 2016, however, the bureau changed course, suggesting that paying ransoms was no guarantee of gaining back access to encrypted files. Other computer security experts also warn companies not to pay, as word may get out in the hacker community of payment, inducing new hacker groups to target the organization, creating a cycle of attacks. Even the act of obtaining bitcoin can put organizations at risk. While there are a few bitcoin ATMs, most victims buy bitcoin on unregulated exchanges that have been hacked, leaving buyers' bank account information stored on these exchanges vulnerable.

In general, it's better to avoid paying if you have backups. Sometimes attackers provide a partial encryption key and seek additional payments. In other cases, the ransom demand may be a diversion, to distract victims from the attackers' true purpose, such as stealing records.

Value of Cyber Insurance

Because of the small dollar amount of most ransomware demands, many organizations do not see the need for cyber insurance protection from this threat. It is true that most ransomware demands historically have been below an insured's deductible. Many insureds pay these demands themselves without reporting them to their insurance carrier. That can be a mistake, however, in part because insurers often require policyholders to notify them of all ransom demands.

Cyber insurance can play an important role far beyond just reimbursement of an extortion payment. As a practical matter, because most demands seek payment in less than 72 hours and obtaining bitcoin under a deadline can be difficult, insurers can be a valuable resource to assist in this.

Another consideration is that many kinds of cyber insurance provide access to legal advice. Involving legal counsel from the outset can keep forensic investigations and findings privileged. That can be especially helpful if the cyber incident triggers third-party litigation.

Below are various components of Cyber insurance coverage and how they may be applicable when facing a ransomware incident:

- **Cyber Extortion Coverage.** This coverage is readily available and can pay ransomware demands and expenses in addition to other extortion schemes, such as threats to conduct a denial-of-service attack or unauthorized public disclosure of stolen personal or confidential corporate information.

- **Forensic Investigations Coverage.** Extortion demands may be smoke screens, diverting attention from the hacker's intent to place other malware on the computer system without discovery. Forensic investigations are needed to determine whether any other sort of attack has occurred -- and whether data has been stolen. Reporting an extortion event to the insurer can activate this important coverage.

- **Data Restoration Coverage.** This first-party coverage can be used to hire computer consultants to decrypt their data files using the decryption keys or, if data is not recoverable, reinstall data from backup sources. If the insured does not have backups this coverage will pay, where feasible, for the expense to re-create lost data files.

- **Cyber Business Interruption Coverage.** For many businesses, an extortion event will result in a loss of income while the insured is shut out of its computer system. This downtime may be extremely costly, especially for healthcare, retail and e-commerce organizations. Cyber Business Interruption coverage will pay for the loss of income and or extra expenses needed to help restore the system, after the application of an hourly waiting period ranging from 8 to 24 hours, a self-insured retention or both.

- **Breach Response Coverage.** Although nearly all U.S. states have breach notification laws, there has been a safe harbor for encrypted data. This may be changing, making breach response coverage even more valuable. Recently, the Health and Human Services Department's Office of Civil Rights announced that a ransomware attack may fall under the definition of a data breach under the Health Insurance Portability and Accountability Act. HIPAA prescribes breach incident risk assessments to determine whether notification is needed. Where notification is required by law or regulation, breach response coverage will pay for those costs. If a breach has occurred, organizations should retain counsel.

- **Regulatory Coverage.** Data breaches can trigger an avalanche of unwanted attention from the public and regulators. Notification, for example, can also attract the scrutiny of regulatory authorities that might want to conduct an investigation. Regulatory coverage in a cyber policy can provide defense coverage as well as pay for fines or penalties, if levied against the insured.

Conclusion

Retail insurance agents and brokers, and their clients, need to understand that ransomware and extortion demands are not as simple as they may appear. Ransomware attacks can trigger both first-party and third-party coverage in cyber insurance policies. Promptly reporting such incidents to cyber insurers is important not only to activate coverage but also to access specialized expertise and legal advice. For organizations concerned about ransomware attacks, cyber insurance is one of their most versatile weapons.

Cyber Safety Tips

- Besides cyber insurance, common-sense security measures can help mitigate the impact of ransomware attacks at many organizations. These measures include:
  - Daily file backup and offsite storage
  - Continual training of employees at all levels to recognize and prevent phishing
  - Continuous updating of spam filters and fire walls
  - Routine updating of security patches
  - Disabling macros, file sharing and auto play settings in e-mail

For more information on cyber insurance and risk management, please contact your CRC, CRC Swett or SCU representative.

To find a conveniently located broker visit us on the web at:
crcins.com, crcswett.com or scui.com.