# Ransom Remedies

*Hackers are attacking companies in more sophisticated ways. Liability expert* ***PATRICIA KOCSONDY*** *explains how to fight back.*

**Dear Expert,**
**I've been reading about the Ryuk ransomware attack that affected Tribune Publishing. How can my company reduce fallout from an attack?**
**– *Fretful in Fresno***

**Dear Fresno,**
Since I wrote about ransomware in *TFM*'s September/October 2017 issue, attacks have become more targeted and sophisticated.

"Bad actors" are becoming better at discovering media companies' most valued data; oftentimes they encrypt not only the victim's front-end systems, but also the back-ups. Moreover, the amount of the ransom demand has increased into the seven figures in some cases.

Ransomware – a malicious form of malware preventing people from accessing systems and data until a ransom is paid – is the most prevalent type of cyber incident, according to Chubb's real-time claims data. (Find out more at chubbcyberindex.com.)

Unlike WannaCry and NotPetya, newer malware strains like Ryuk are not buckshot ransomware attacks. The bad actors have upped the ante by deploying insidious banking trojans like TrickBots and Emotet. Often used in combination, they penetrate technology systems and networks, typically via an email phishing scam containing a malicious link. Once inside the network, they devote considerable energy to conducting deep reconnaissance of the targeted entity.

Their activities include harvesting user credentials; navigating the network to determine which data is crucial to ongoing operations and business value; searching data centers for file backups; and scouring financial statements to discern the company's wherewithal to pay a certain size ransom.

The result is that the bad actors have become increasingly successful in launching effective attacks for greater reward.

## PAY THE RANSOM?

The Federal Bureau of Investigation has advised against paying extortionists. But to pay or not to pay is a decision for the victim organization to make.

If the company declines to pay up, it may risk significant disruptions in ongoing business. Many companies are tempted to simply pay and move on, eager to resume operations with minimal disruption, financial cost and reputational damage. There is no easy answer. On its website, the FBI states that the decision requires "the evaluation of all options to protect shareholders, employees and customers."

> ***The FBI has advised against paying extortionists. But to pay or not to pay is a decision for the victim organization to make.***

Given that this is a business determination, cyber insurers generally leave the decision to the policyholder. Depending on coverage terms and conditions, policyholders may obtain reimbursement for the cost of the ransom and business interruption losses.

## ADVANCE PREPARATION

The best solution is for companies to prepare themselves in advance of an attack, so they can respond quickly and decisively if bad actors strike. Otherwise, that most precious commodity, time, is squandered, increasing the length and related cost of the business disruption. This positioning should include proactive plans with internal stakeholders, so each understands their role and contribution. It's also wise to line up external assistance from specialist law firms, forensic investigators, crisis management experts and firms with bitcoin wallets to pay the ransom in cryptocurrency, should the company decide to pay the demand.

Do this before a crisis occurs. Retaining these firms after an attack – an effort that includes recruitment, due diligence and contractual negotiations – can take days or even weeks, inevitably delaying the deployment of an effective incident response.

The external services' level of expertise is also important. Law firms that specialize in cyber-incident response understand the different types of ransomware events and can help select an optimal forensics investigator.

Attorneys also can help media companies navigate niche issues such as the legalities of payment and the need to conduct a so-called OFAC check to ensure the bad actor is not listed by the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) in its record of "specially designated nationals and blocked persons."

Forensics firms that specialize in responding to ransomware incidents have expertise negotiating with bad actors. They can also test parts of the decryption code in advance of a ransom payment to help ensure the decryption key will work. In most cases, they can further facilitate the payment in bitcoin.

In addition, cyber insurance can help, since some insurers can provide access to a panel of specialists to assist companies with both incident preparedness and response.

*Patricia Kocsondy is senior vice president and the media professional liability product manager for Chubb. She can be reached at Patricia.Kocsondy@Chubb.com.*

***Do you have a professional puzzle that MFM and BCCA experts might be able to answer? We'll mine the contact base and find the right person to answer your question. Just contact TFM editor Janet Stilson at TFMeditor@mediafinance.org.***