CULHANE MEADOWS

InformationWeek

To Pay or Not to Pay?
The Ransomware Dilemma

By Carrie Pallardy
Featuring Heather Clauson Haughian, Partner
Culhane Meadows PLLC

> *"Your legal counsel and your cyber carrier will help you determine who else should be notified depending on whether the ransomware incident has comprised any systems that could have led to unauthorized access of data."*
>
> Heather Clauson Haughian, Partner
> Culhane Meadows PLLC

So, your company gets hit with a ransomware demand. What next? Law enforcement agencies, like the Federal Bureau of Investigation, typically caution against making ransom payments. But the ultimate decision isn't always easy to make, especially with costly downtime and sensitive data hanging in the balance.

Ideally, a company will have a well-rehearsed incident response plan in place, but the stakeholders involved will still have to make the tough call when incident response goes from a tabletop exercise to reality.

The Initial Response

As soon as a ransomware demand is made, a company's cybersecurity team needs to jump into action. The first step is to inform everyone who will be involved in responding to the incident, inside and outside of the company. "The IT/security team should never be operating in a vacuum when these events occur," warns **Heather Clauson Haughian, a co-founding partner of law firm Culhane Meadows.**

Continued on next page...

Each company's team, structure, and incident response plan will vary. Typically, internal stakeholders include the CISO, the rest of the leadership team, general counsel, impacted business group leads, and communications. Depending on the company and severity of the incident, a ransomware demand may also merit board-level involvement.

Outside of a company, external IT and cybersecurity vendors, external counsel, and the cybersecurity insurance carrier need a seat at the table. Leadership will also likely need to inform law enforcement.

"Your legal counsel and your cyber carrier will help you determine who else should be notified depending on whether the ransomware incident has comprised any systems that could have led to unauthorized access of data," **says Clauson Haughian.**

In addition to getting all the key players involved, cybersecurity teams need to determine the extent of the incident. "Confirm that the infected computers/devices have been isolated or completely severed from the company's network, because ransomware typically scans the affected network and attempts to propagate laterally to other systems," **says Clauson Haughian.**

Remember, do not panic. Prompt action is important, but some teams make the mistake of acting without considering the consequences.

"We have found some organizations will start wiping drives and reloading operating systems, and that can prevent them from learning what the hackers have done and whether they still have access to your systems, and it can hamper data restoration and recovery from the incident," shares Bala Larson, head of client experience at insurer Beazley.

To Pay

The question of whether to pay is not always easily answered. Both decisions come with consequences.

InformationWeek's Cyber Risk and Resiliency Report: How CIOs are Dueling Disaster in 2023 surveyed 180 IT and cybersecurity professionals. Of those respondents, 10% reported paying a ransom to recover files encrypted in a ransomware attack. The report found 33% of respondents believe that paying was the right decision, while 39% believe time will tell. Those who think it was the wrong decision to pay: 2%.

At a high level, the argument against paying begins with the message it sends. Ransomware is lucrative. Making the demanded payment incentivizes cybercriminals to continue pursuing extortion campaigns. On the individual company level, the decision to pay comes with the risk that the ransomware gang won't live up to their word. They may take the payment and never send a viable decryption key. And they may still go forward with publishing stolen data.

A 2023 report on ransomware trends from software company Veeam found that 19% of organizations that paid a ransom could not recover data.

"The potential for the total loss of the ransom payment coupled with the remaining cost of data and system restoration should also be included in the risk calculus of considering making any payments," says Lavonne Burke, vice president of security, resiliency, and IT legal at technology company Dell Technologies.

If paying would cause less damage than refusal, a company may conclude that payment is the best option. "If everything is locked and/or encrypted, especially for an organization that intimately depends on its data for operational success, like a hospital or educational institution, bouncing back from downtime could be near impossible," says Shelley Ma, incident response lead at cyber insurance company Coalition.

The Colonial Pipeline incident in 2021 is one of the most well-known examples of a ransomware victim opting to pay. The company paid a $4.4 million ransom to restore its fuel pipeline operations. (The Department of Justice did recover approximately $2.3 million paid to DarkSide, the group responsible for the ransomware attack.)

If a company's team determines paying is the right choice, it is important to understand the regulatory ramifications. Paying a ransom is not illegal unless an organization makes a payment to a threat actor on the Office of Foreign Assets Control (OFAC) sanctions list.

"Prior to making a payment, a company should consult with outside forensics, ransom negotiations and legal counsel, as well as with applicable law enforcement, to best ensure they are not making a payment to a known sanctioned entity," says Burke.

A company's cyber insurance carrier will be a critical player in the decision-making process. They could be the one paying the ransom demand, depending on a company's coverage. Ma explains that insurers can pay ransom on behalf of clients. "Some other insurance policies will reimburse clients after they've paid, causing a more immediate financial burden on the policyholder at the onset of the incident," she adds.

Burke points out that the ransom can also be accompanied by the cost of the negotiation process and increased cyber insurance premiums.

Working with a ransom negotiator may give leadership teams additional time to answer questions that will help them decide on the best course of action, according to Larson.

Not to Pay

What happens if a company opts not to pay? This decision may be made when a company has adequate offline backups to restore its systems. "Having robust backups that live in the cloud and are completely offline are critical to a successful recovery and reducing downtime as much as possible," says Ma.

Companies may also be able to unencrypt the ransomed data using free and publicly available tools.

"Victims are also increasingly choosing not to pay in situations where the primary risk of non-payment is the publication of data, as payment does not negate breach notification obligations, or potential regulatory penalties resulting from an underlying data theft," adds Burke.

While choosing not to pay means a company won't have to shoulder the cost of the ransom or run the risk of an OFAC sanction violation, there are still consequences.

Even if companies can recover encrypted data, it could be a cumbersome, time-consuming process that impacts business operations, according to Burke. Plus, ransomware gangs are likely to make good on their threats of deleting and/or publishing data. Downtime and reputational damage can be costly.

Refusal of payment may lead threat actors to up the pressure to extort the ransom, according to Burke. "These techniques can include distributed denial-of-service (DDoS) attacks on the company network, direct threats to management or other individuals in the company, slow leaks of stolen information to draw media attention, threating to contact regulators about the attack and/or contacting customers or other individuals whose information was stolen to apply further payment pressure," she explains.

Payment or non-payment both come with regulatory considerations. Incident response teams need to understand all their companies' regulatory obligations to avoid compounding the cost of a ransomware incident with fines.

"Organizations need to understand their legal and regulatory exposure before they receive a ransom demand. They need to account for every statute," says Robert Hughes, CISO at cybersecurity company RSA.

Recovery

Deciding to pay or not is just one leg of the arduous journey through ransomware response. Once the choice has been made, the incident response team must face the prospect of recovery.

If a company pays and receives a decryption key from the ransomware gang, that key needs to be vetted by forensics to ensure it does not come with malware or any other malicious code, according to Burke. "Decryptors vary significantly in their usability and time to restore data," she says. "Engagement with experts like forensics or negotiation firms who have prior expertise with the threat actor can frequently increase the speed and success of decryption significantly."

Decryption can be a lengthy process. It may take 12 to 15 hours per terabyte of data, according to Larson.

Organizations that move forward without paying will need to explore alternative means of decryption or rely on their backups. But this process will need to be completed with caution. "Care must be taken to examine backup data to ensure it does not contain malware or threat actor tools which could allow for a subsequent attack," says Burke.

Regardless of whether a company pays or not, understanding how the attack happened is vital to recovery. **Clauson Haughian** emphasizes the importance of conducting a root cause analysis to identify the ransomware variant and determine why the attack was successful.

Leadership teams also need to consult with their cybersecurity insurance carrier and legal counsel to ensure they know when and how to disclose the attack.

"The minute data leaves the door of an organization (i.e., it's been exfiltrated), businesses have requirements to notify their own customers, vendors, and any other affected parties even if they are already fully back up and running," says Ma.

Organizations may opt to work with a PR firm to guide the messaging on the breach, remediation, and efforts to prevent future incidents.

"Keep in mind that following a ransomware attack, an organization will be remembered by how well it responded and recovered from the incident," says Burke.

Preparing for the Next Attack

Making it to the either side of a ransomware attack may lead to a collective sigh of relief, but it is a lesson to be remembered. "No organization is immune from 'next time," cautions Burke.

Following a ransomware attack, spend the time to evaluate what worked in the incident response plan and what could be improved. If an organization does not have a plan in place or a sufficient data recovery program, it should develop incident response protocols and immutable backups.

Hughes stresses the importance of prioritizing identity as an organization examines how to strengthen its security. The ransomware group behind the Colonial Pipeline attack leveraged a compromised password to gain access. "Colonial Pipeline was a worst-case scenario, but it's not an outlier: cybercriminals target identity more than any other component of the attack surface," says Hughes.

He emphasizes the importance of multi-factor authentication and identity governance and administration capabilities in protecting organizations against these kinds of attacks.

Threat actors will always look for ways to exploit vulnerabilities. Defending against these threats necessitates continuous improvement. Following a ransomware attack, this improvement is vital for building a more resilient future and for navigating regulatory scrutiny. Burke points out that regulators want to see organizations demonstrate improvements following an incident.

"It's hard to avoid being thought of as a victim following an attack, However, with the right assistance, an organization can come out better prepared than before they were challenged," says Larson.