VISIT MAGAZINE WEBSITE

Are You Prepared for a Ransomware Attack?

A road map to strengthen your organization's ransomware readiness

Ransomware and data theft continue be a major threat to government agencies and businesses, regardless of size or industry. In 2020, the FBI's Internet Crime Complaint Center (IC3) received more than 2,400 complaints identified as ransomware, costing $29.1 million in adjusted losses. Those figures don't account for lost business revenue or other operating losses to recover systems.

continued on next page >

With the availability of ransomware toolkits now on the dark web, threats to small business are increasing as novice hackers launch attacks against smaller targets.

The disruption to business operations and loss of personal information can be costly to your organization. The data loss can be far-reaching as criminals may threaten to sell stolen data, post it on the dark web or use it to attack business partners and vendors.

"We have seen a significant increase in the number of attacks against Commercial Banking clients this year," said Anne Davis, Head of Cybersecurity & Technology Controls for Commercial Banking at JPMorgan Chase. "In some cases, there are incidences of 'double extortion' style attacks where criminals issue a ransom demand for the return of stolen data then threaten to publish or share the data with competitors."

The federal government is treating ransomware as a major national security threat, and the Biden administration has called on the private sector to do its share to protect against attacks.

In a message to corporate executives and business leaders in June 2021, the White House wrote that "companies that view ransomware as a threat to their core business operations rather than a simple risk of data theft will react and recover more effectively."

To minimize losses and disruption as the result of a ransomware attack, prepare now by gathering reliable intel, documenting a response plan, testing that plan and educating employees. This road map can help you get started.

In addition to the steps outlined below, the White House recommends organizations implement multi-factor authentication, end-point detection and response, encryption, network segmentation, and prompt system patching and updating. Visit the Cybersecurity & Infrastructure Security Agency (CISA) website at cisa.gov/ransomware for more information.

Before an Attack

1 GATHER RECENT, RELEVANT AND RELIABLE INTEL.

The frequency and sophistication of ransomware attacks is increasing, so it's important to guard against ransomware attempts and understand how the attacks are carried out. Organizations must regularly gather and study current cyberthreat trends and advisories from primary sources.

Where can you get reliable threat intelligence?

- Commercial Banking's Cybersecurity and Fraud Protection Insights page
- Federal government agencies, including the Cybersecurity & Infrastructure Security Agency (CISA) and the FBI's Internet Crime Complaint Center (IC3)
- State and local agencies
- Industry partnerships such as Information Sharing and Analysis Centers (ISACs)

2 PLAN NOW, NOT LATER.

Resilient organizations anticipate the worst-case scenario and develop a cybersecurity incident response plan that engages all departments on how to respond when a real crisis strikes and causes your business to be offline for several days. The cybersecurity plan should define:

- Your payment process strategy if your organization is unable to process transactions or payroll for an extended period of time
- What priority systems or departments should be recovered first
- A data backup strategy that is aligned to your incident recovery plan
- How response teams will work to get backup systems running and operations back to normal and you have remediated the causes of the compromise

You should also test and enhance your plan regularly by conducting tabletop exercises.

continued on next page >

3 EVERYONE'S A WATCHDOG.

Your organization is only as secure as its most vulnerable points. Ransomware attacks are frequently delivered through phishing emails that appear to be sent from legitimate customers, vendors or other known contacts. But the messages contain links or attachments that, when opened, can result in your organization's sensitive data being encrypted or stolen—and in some "double extortion" schemes—both at once.

Ignoring or deleting suspicious emails in your inbox isn't enough. Here are a few steps to take and habits to reinforce:

- Require the use of multifactor authentication, like a one-time password, token or key, if a username-password combination is compromised.
- Develop, document and train employees on processes for handling suspicious emails.
- Regularly educate employees, including the C-suite, on cyber and fraud threats.
- Flag emails with an external banner to encourage staff to identify and quickly report emails that may be fraudulent to the Information Technology (IT) team before falling victim.
- Educate employees on how to spot red flags and respond appropriately throughout the various stages of a ransomware attack.

Despite your careful efforts, a ransomware attack gets past defenses and impacts your organization. What now?

During An Attack

4 REMEMBER THAT CYBERSECURITY INCIDENT RESPONSE PLAN?

When an organization is impacted by a ransomware attack, every minute is critical. Fortunately, your organization has prepared by developing and testing your incident response plan before an actual event. The IT team gets to work by identifying the source, location and extent of the attack and disconnecting infected systems. Legal, crisis communications and operations staff will need to assess when and how to inform employees, clients, stakeholders and regulators if there is a loss of data. Once the infection is contained and removed from the network, restore systems with secure, uninfected backups.

5 CONSIDERATIONS WHEN FACED WITH A RANSOMWARE PAYMENT DEMAND

- If you are the victim of a ransomware attack, you should immediately contact your local FBI field office and submit a complaint to the **FBI's IC3**.
- In assessing whether to pay a ransom demand, you should understand any regulatory and legal considerations.
- Contact your Commercial Banking relationship team as soon as you suspect a malware or ransomware incident. The team can work with you to implement protective controls on your payment platforms and assist with any resiliency needs relating to your relationship with us.

Key Takeaways

- Stay informed on the cyberthreat landscape.
- Develop an incident response plan for cybersecurity incidents, specifically ransomware attacks.
- Understand legal and regulatory considerations before considering payment of any ransom-related demand, and contact your Commercial Banking relationship team if you suspect a ransomware attack.

The previous article is an excerpt from Fraud + Cybersecurity Magazine: Summer 2021.

Explore the full issue