VISIT OUR FRAUD HUB

Developing a proactive mindset on ransomware

As cyberattack threats loom large over businesses, our expert says companies should focus on prevention, detection, response and recovery.

Anne Davis
Head of Cybersecurity & Technology
Controls, Commercial Banking

Anne Davis oversees firmwide global technology control management. In more than two decades with the firm, Davis has held roles in information security, technology and business controls and technology execution. We sat down with Anne for her advice on how clients can develop a proactive mindset to prevent ransomware attacks.

continued on next page >

VISIT OUR FRAUD HUB

Q: In June 2021, the White House called on business leaders to take action and launched stopransomware.gov to help inform the public and remain vigilant. Why is ransomware a national security issue?

A: Ransomware is a leading national security topic right now because of the growing frequency and sophistication of attacks. Ransomware impacts the livelihood of all Americans and requires business and government to work together to strengthen national resilience. It's also because of an increase in attacks on businesses that provide critical infrastructure—think oil pipelines, food processing plants and hospitals. These attacks have created costly ripple effects through government and beyond to other businesses, ultimately impacting their customers too. The best way to mitigate risk is to implement baseline cyber hygiene practices and develop standards and controls that apply broadly to consumers, businesses and the government.

Q: When it comes to ransomware, what does it mean to be prepared? How can companies know whether they're targets for attacks?

A: Ransomware attacks are now so widespread that all organizations should assume they will be targeted. There is no way to completely ensure you will not be a victim of ransomware, so heightened diligence and ongoing review of your controls with your internal and external partners is of paramount importance. You should focus on four areas to prepare for threats: prevention, detection, response and recovery.

Q: Let's start with prevention. What does that entail?

A: Good cyber hygiene is key to preventing ransomware. That involves keeping systems patched and keeping them up-to-date using a risk-based approach. You also need to implement a layered defense strategy and use multifactor authentication and backup systems for your data. And you have to maintain extensive oversight and security controls over any third-party vendors that may have access to your computer network or handle sensitive data. Employee awareness is at the core of prevention. Helping them understand how attacks happen and how they can help is critical.

Q: Can you explain risk-based approaches to software patches?

A: Software providers regularly provide updates to fix newly discovered security gaps, and those gaps remain as potential vulnerabilities that criminals can discover unless those patches are added. Organizations need to consider several factors before deciding if, when and how to install patches and updates: Is the system internal or external? How critical is the system to your business? If you delay patch updates, are there regulatory or compliance considerations, such as fines?

Q: What does an effective detection strategy look like?

A: It means being able to detect anomalous activity as quickly as possible. The sooner you detect an intrusion, the sooner you can contain it and reduce the overall impact. Perform a regular review of log files and monitor outbound data. Consider using a tool that looks for encryption activity stops it immediately and sends alerts.

continued on next page >

Q: Even with sound prevention and detection strategies, some ransomware attacks will occur. What are the steps businesses should take so they can respond quickly?

A: Being prepared means having a concrete plan and proper training to respond to an attack before it occurs. In the chaotic situation following a ransomware attack, time to act is limited, stress will be sky-high and normal organizational, financial and communications tools may be offline. So create a plan. The plan contains details on identification, detection, containment and recovery. Regular testing will help your team and response time improve.

Q: How often should a business review its response plan?

A: Reviewing a plan should be a regular practice so that the details are up-to-date at the moment an attacker strikes. Perhaps employees' roles have changed, or new hardware or cloud systems have been added. Test your plan regularly to make sure everyone is familiar with it and you can identify any gaps in security protocols.

Q: What other pieces need to be part of any organization's response plan?

A: The plan should document all systems and in what order they should be restored. It should also address who needs to be contacted to begin recovery and which people or teams will handle different aspects of managing the crisis, from legal and compliance to information technology, billing and public relations.

The plan should also account for backups so that data and operations can be restored. An effective response plan will detail how to access backups and test them prior to restoration.

A response plan is about keeping the business running and mitigating your recovery time. It's up to the technology and cybersecurity teams to remain diligent and expedient.

Q: What should an organization do when it's hit by a ransomware attack?

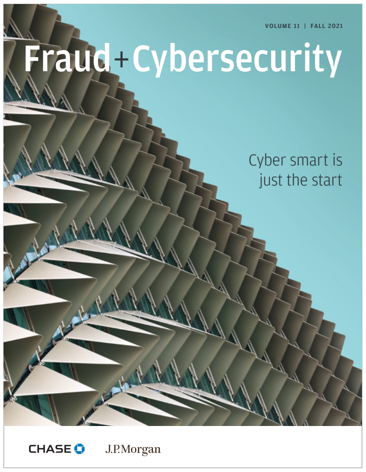
A: JPMorgan Chase has a process in place to help clients when they're impacted by a ransomware attack. Affected clients should contact their Commercial Banking relationship team as soon as they suspect a malware or ransomware incident. The firm will work with your business to implement protective controls on payment platforms and will assist with other resiliency needs. If faced with a ransomware payment demand, each business must understand the regulatory and legal implications.

You should also contact the local FBI field office and submit a complaint to the FBI's Internet Crime Complaint Center, or IC3.

Key takeaways

- Prevent attacks by patching systems and keeping them updated.
- Detect intrusions quickly so you can contain them as soon as possible.
- Develop a response plan for ransomware attacks, and keep it up-to-date.
- Understand legal and regulatory implications before considering payment of any ransom-related demand.

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



DOWNLOAD

J.P. Morgan and Chase are marketing names for certain businesses of JPMorgan Chase & Co. and its subsidiaries worldwide (JPMC). Any example of cyber or other fraud or loss in this material is for illustrative purposes only; any similarity to any actual event or person is unintended and unfounded. This document was prepared exclusively for the benefit and internal use of the party to whom it is delivered (each, a “Recipient”). The content is not intended as, nor shall be deemed to constitute or contain, advice on which the Recipient may rely; does not constitute in any way JPMC research, and should not be treated as such; and is confidential and proprietary to JPMC. The content may not be copied, published, disclosed or used, in whole or in part, for any purpose other than as expressly authorized by JPMC. This is provided for educational and informational purposes only and is not intended, nor should it be relied upon, to address every aspect of the subject discussed herein. The information provided is intended to help clients protect themselves from malicious cyber activity. It does not provide a comprehensive list of all types of malicious cyber activities and it does not identify all types of cybersecurity best practices. You, your company or organization are responsible for determining how to best protect against malicious cyber activities and for selecting the cybersecurity best practices that are most appropriate to your needs. JPMC assumes no responsibility or liability whatsoever to any person in respect of such matters, and nothing within this document shall amend or override the terms and conditions in the agreement(s) between JPMC and the Recipient.