CHASE J.P.Morgan

CYBERSECURITY

Your guide to ransomware preparedness

Your guide to ransomware preparedness

Ransomware attacks are among the most serious cybersecurity threats facing organizations today, including JPMorgan Chase Commercial Banking clients. The goal of a ransomware attack is to disrupt your business, usually by encrypting your own data so you cannot use it. The cybercriminals behind the scheme demand payment in exchange for a decryption tool and a promise not to release stolen data—a vow that is not honored in many cases. Ransomware victims most often lose the ability to perform even basic business functions. The disruption is determined by the victim's ability to recover. It's not uncommon for this to last anywhere from several days to weeks, carrying long-term financial, operational and reputational consequences, which can be life-or-death for healthcare organizations or hospitals.

We've created this guide to help your organization prepare for and protect against a potential ransomware attack. We also cover what to do in the event you are hit by an attack, because every minute counts when responding to an incident, especially as the rate of ransomware and zero-day attacks continues to rise.

CONTENTS

PREPAREDNESS:

How does a ransomware attack happen?

There are several ways ransomware attacks can occur. Criminals may take advantage of an organization's poor cybersecurity hygiene, including a lack of authentication protocols, use of outdated software or infrequent or absent employee cybersecurity awareness training. Ransomware can be launched from several different attack points, but the three most common vectors are:

Phishing email campaigns:

Criminals send an email to your employee encouraging them to click on a malicious link or open a document containing hidden malware, which infects the computer and allows the criminals to further penetrate your computer network.

Remote Desktop Protocol (RDP) vulnerabilities:

RDP is a technology used by many organizations that enables employees and vendors to remotely connect to a computer network. Criminals can access these networks by stealing a victim's credentials or through brute-force attacks that attempt to find the right password by continuously trying passwords until the correct one is entered.

Software vulnerabilities:

Poorly written or unpatched applications (such as RDP or other operating platforms) present criminals with easy entry points to gain access to an organization's systems. Applications that are designed to be accessible from outside a client's network are particularly vulnerable to exploitation. Keep in mind, these methods of attack are not limited to just your network. Ransomware or zero-day attacks can impact third-party vendor and cause a ripple effect across the entire supply chain.

CONTENTS

PROTECTION:

Best practices

Protecting your business against ransomware attacks is a team effort. Preparedness starts with developing and following good cybersecurity hygiene. Below are some basic best practices that your organization may consider adding to your existing internal security protocols.

Technical Best Practices

- Require employees to use multifactor authentication—like a one-time password, token or key—when accessing the network or email. This helps safeguard your operations in case a username-password combination is compromised.
- Consider using network segmentation to help limit the scope of an attack.
- Utilize immutable backups to safeguard information and enhance business resiliency.
- Keep your network up to date with the latest software patches.

Operational Best Practices

- Assign regular mandatory employee training and testing on email phishing, password protection and other cybersecurity practices.
- Hire or create your own cybersecurity "Red Team" to routinely test and evaluate your incident response plan and network systems to find any potential gaps.
- Leverage public resources—like this guide to incident response from the National Institute of Standards and Technology (NIST) or incident response training from the U.S. Cybersecurity and Infrastructure Security Agency (CISA) —to develop robust resiliency, response and recovery plans.
- Consider purchasing a cyber insurance policy to help reduce the financial impact of cyberattack.

These best practices also extend to other organizations and vendors you do business with. You should continuously validate third-party compliance and conduct annual reviews to make sure vendors are maintaining their own cybersecurity protocols.

We also offer additional resources, including:

- Cybersecurity and fraud prevention training and education sessions for your employees via modules on J.P. Morgan Access® and Chase Connect®.
- Simulated real-life ransomware tabletop exercises for qualifying organizations.
- Thought leadership articles to stay cyber prepared published on our CB Insights webpage.

CONTENTS

RESPONSE:

What to do if you're hit by a ransomware attack

We understand how devastating an attack can be to your organization—and we're here to help. In the event of a malware or ransomware attack, it is important to respond quickly by:

- Taking immediate action to stop the spread of malware; this should include disconnecting from the network.
- Executing your incident response and business continuity plans (which should be stored in a place that is completely separate from the network, like cloud file storage).
- Communicating with your own advisors, stakeholders, legal counsel, etc.
- Filing a report with the FBI's Internet Crime Complaint Center at IC3.gov and contacting your local FBI field office.
- Notifying your Commercial Banking relationship team. We can assist you with implementing financial controls and can assist with various resiliency options even if your network is completely down.

Do not make a ransom-related payment through your JPMorgan Chase account unless we provide written advanced approval for you to process such a payment. This includes payments that do not originate from your account but may originate from your intermediaries using accounts with JPMorgan Chase.

Contact your Relationship Team if you want more information on how to improve your defenses.

CONTENTS

CHASE J.P.Morgan