How to Protect Your Organization From Ransomware Attacks
Ransomware attacks can debilitate your organization’s entire information technology (IT) structure, causing disastrous effects. These attacks are only growing more common and costly—ransomware attacks have increased 500 percent since January 2019, with an average cost of more than $46,000 per attack.

Because they’re so prevalent and disruptive, it’s crucial for organizations to develop effective response strategies to minimize the impact of ransomware attacks.

The information provided here is intended as a guide to help the firm’s clients protect themselves from ransomware. It is not a comprehensive analysis of all types of ransomware activities or best practices. The client or organization is responsible for determining how to best protect itself against ransomware activities, and to select the best practices most appropriate to its needs.

“If you haven’t been a victim of ransomware or any other type of computer attack, you have to operate as if it’s just a matter of time before you are—and take the steps to protect yourself and mitigate the resulting damage or loss.”

*FBI Supervisory Special Agent Sheraun Howard*
What Is Ransomware?

Ransomware is a form of malicious software (malware) that targets critical data and systems for the purpose of extortion.

It’s frequently delivered through phishing emails that appear to come from legitimate customers, vendors or other known contacts. These messages contain links or attachments that, when clicked, encrypt the user’s computer and can potentially spread to other files on the corporate network. After the user is locked out of the system, the cybercriminal demands a ransom payment, usually in bitcoin or another cryptocurrency. The cybercriminal may also threaten to increase the ransom if payment isn’t received by a specific time frame, or threaten to delete or permanently encrypt files if the ransom isn’t paid. The cybercriminal typically promises that, upon receipt of the ransom payment, he or she will provide a decryption key so the victim can regain access to the affected files and systems.

How Much Does a Ransomware Attack Cost?

Ransom demands can range anywhere from a few hundred dollars to well over $100,000. A cybersecurity research company recently estimated the average ransom to be approximately $36,000. However, in some recent attacks, including several involving the Ryuk strain, ransom values averaged $268,000. In fact, one Georgia municipality paid $400,000 to unlock its files.

Unfortunately, the cost of the ransom is the tip of the iceberg. Ransomware’s underlying costs include lost productivity, equipment, remediation, reputational damage and possible legal fees. In a worst case scenario, ransomware may disrupt the entire spectrum of an organization’s IT infrastructure, which includes email communications, access to sensitive files and the inability to send or receive payments.

In addition, the cost of recovering from a ransomware attack can be much higher than the ransom payment. For example, the City of Baltimore experienced an attack in May 2019 demanding a $76,000 ransom, but its estimated recovery costs are $18.2 million—$10 million to repair IT infrastructure and $8.2 million in lost or delayed revenue.

Should I Pay the Ransom?

The FBI discourages companies and private citizens from paying ransom to a cybercriminal, noting that payment doesn’t guarantee data access, and further emboldens cybercriminals to target other organizations.

However, the FBI also recognizes that deciding whether or not to pay ransom isn’t always clear cut. Organizations need to consider business continuity and other obligations to their shareholders, employees and clients. In the event a client seeks to make a payment through JPMorgan Chase & Co. in connection with a ransom demand, the firm will evaluate such a request on a case-by-case basis, with consideration given, among other things, to whether processing the proposed transaction implicates any applicable laws or regulatory obligations.
How Prevalent Is Ransomware?

A recent US government interagency report estimates that more than 4,000 ransomware attacks have occurred every day worldwide since the beginning of 2016.

The threat is so widespread that FBI Supervisory Special Agent Sheraun Howard advised, “If you haven’t been a victim of ransomware or any other type of computer attack, you have to operate as if it’s just a matter of time before you are—and take the steps to protect yourself and mitigate the resulting damage or loss.”

Furthermore, ransomware is a major threat to small and medium-sized businesses (SMBs). Considering the cost and the recovery time involved, many SMBs cannot afford to experience an attack.

Also, organizations can fall victim to repeat ransomware attacks, depending on the organization’s risk profile. This is especially true if the organization doesn’t remedy vulnerabilities after an initial attack.

How Do I Enhance My Organization's Resiliency?

Many organizations falsely believe they won’t experience a cyberattack or can draw on their comprehensive cybersecurity plan to quickly recover from one. A cybersecurity plan, however, is only a good first line of defense, not an exhaustive set of safeguards.

The best protection against ransomware is to anticipate and plan for a worst case scenario. Since a ransomware attack could bring about a catastrophic stop to operations, organizations should prepare for a ransomware attack like they would any other disaster that would disrupt business continuity. To help promote organizational resiliency, it is important to have a robust incident response plan (IRP) and disaster recovery plan (DRP).

Although cybersecurity incidents can be significant, they do not always approach disaster levels that threaten to cease all operations. An IRP is designed to help your organization recover from cybersecurity incidents that don’t halt operations. Ransomware, however, is designed to cripple an organization’s IT infrastructure. It’s imperative to also have a DRP to restore IT functions after a ransomware attack.

A DRP is a plan to restore IT functions in the event of a major disruption, whether caused by a fire, flood or malicious attack by cybercriminals. A DRP outlines procedures and instructions an organization must follow in the face of such disasters. It covers business processes, assets, recovery times and more. An effective DRP should consist of the following four stages:
4 Stages of Disaster-Recovery Planning

1. **Conduct** a business impact analysis (BIA):

   Whereas a **risk assessment** identifies potential loss scenarios, a BIA predicts the consequences of a business disruption, and gathers information to develop recovery strategies. The BIA is the foundation of your DRP. So make sure your BIA considers a wide range of potential impacts, including:

   - Delayed and lost sales and income
   - Increased expenses (e.g., overtime labor, outsourcing or expediting costs)
   - Regulatory fines
   - Contractual penalties or loss of contractual bonuses
   - Customer dissatisfaction or defection
   - Delay of new business and operational plans
   - Reputational risk

2. **Identify** critical systems

   Using the BIA as a guide, identify and prioritize the systems and operations your organization needs to resume after a disaster. This will allow you to prioritize response resources on the systems with the greatest impact on your operations.

   Remember that as you work to resume normal business operations, your organization won’t be able to use its usual communication channels and internet connectivity. Your DRP should outline how the organization will perform critical functions (such as vendor payments and payroll) without these systems. The outline should also identify alternate communication channels and include a pre-executed memo addressed to your bank, which details how employees can contact the bank and the actions they’re authorized to perform to prevent unnecessary delays in critical financial transactions.

3. **Develop** the plan

   Once you’ve prioritized systems for recovery, it’s time to address the specifics. How will you restore systems? What’s the expected time frame for system restoration? What resources are necessary? Who will implement recovery efforts? Once you answer those questions, codify and update the DRP. This will ensure the plan remains relevant as operations evolve, and better ensure applicable systems and data receive priority during a disaster.

4. **Test** and exercise

   A disaster isn’t the time to learn you’re unable to restore critical systems within a designated time period. That’s why it’s so critical to test your DRP by conducting tabletop drills and live rehearsals. The outcomes of these tests and exercises can then be used to update the plan and better prepare for a disaster.
How Else Can I Protect My Organization?

What Should I Do If My Organization Is Targeted by Ransomware?

If you discover that your organization is being targeted by ransomware early—before it has spread—you should immediately initiate your organization’s IRP.

From there, containment is paramount, as it will help you limit the ransomware’s damage to only a few systems. For instance, if your security stack identifies an employee opening an email containing ransomware, your Security Operations Center (SOC) can quarantine the system to prevent it from communicating with the internet and other systems, thereby limiting its destructive activity.

Once the computer has been quarantined, your SOC can analyze the system to gather information, attempt to recover any important data, and re-image the system before putting it back into service. Concurrently, the SOC should conduct scans of your network to ensure no other systems have been infected. Based on the indicators of compromise gleaned about the ransomware, the SOC should put additional countermeasures in place to protect your organization against future attacks.

Lastly, your organization should conduct a post-incident analysis. In addition to reviewing details of the incident to determine its cause and evaluating the effectiveness of your response efforts, the analysis should include identifying actions to prevent the incident from reoccurring and updating your response strategy, if necessary.

Unfortunately, many organizations only learn of a ransomware attack after it reaches disruptive levels. If this is the case, enact your DRP to restore operations as quickly as possible. When conducting recovery operations, it's imperative that your organization identifies the ransomware's cause, removes any system that can transmit the malicious files and installs a clean replacement system. If the ransomware is still in your network during your recovery operation, it may infect and destroy your new or re-imaged infrastructure.

Invest in End-User Training

Employees are usually the weakest link in the cybersecurity chain. So it’s critical to educate end users on proper cybersecurity hygiene, including how to spot phishing emails.

Examine Cyberinsurance Policies

Cyberinsurance cannot prevent cybersecurity incidents. Instead, it acts as a safety net for your organization after an attack to offset potential loss.

Consider Professional Incident-Response Services

Responding to cybersecurity incidents can be overwhelming. Professional incident-response services can help ease the burden by augmenting your organization’s response capabilities and speeding up recovery operations.

Practice Good Cybersecurity Hygiene

Your organization can maintain the health of its IT systems by employing preventative measures to help reduce the instances of ransomware attacks. (See next page.)
Elements of Good Cybersecurity Hygiene

Conduct Regular Backups
Back up data regularly and store it in a secure location not directly connected to the network. This helps prevent your backups from being corrupted by ransomware. You should also confirm that you can restore your data from your backups.

Segment Your Network
Separate portions of your organization’s network for different business functions, which limits ransomware’s ability to move through your IT infrastructure. Network segmentation also protects data and other parts of the network from unauthorized and unnecessary access.

Update and Patch Systems and Software
Be sure to install all system patches and software updates, as the latest versions have been updated to mitigate known security vulnerabilities.

Whitelist Applications
Only allow specified programs to run on your IT systems. Deny all other suspicious, questionable or untrusted applications permission to run, unless you whitelist them after thorough vetting.

Protect Your Email
Scan incoming emails and their attachments for malicious software and links. Block suspicious emails with attachments that originate from unknown or blacklisted sites, and indicate that an email is external when it comes from outside the organization.

Safeguard Your Endpoints
Antivirus solutions alone aren’t sufficient to protect endpoints. Organizations should also adopt endpoint security that includes malware and ransomware protection, device firewalls, intrusion prevention and internet content filtering.

Prevent End Users from Installing New Applications
End users should only be granted the minimum privileges necessary to perform their duties and shouldn’t be able to download and install unapproved software or make changes to the operating system.

Test Yourself
Conduct regular penetration tests and vulnerability scans, and incorporate any significant findings into your DRP.
CONTACT

For additional information or questions about how to protect your organization from ransomware attacks, contact cyber.exercise@jpmchase.com.