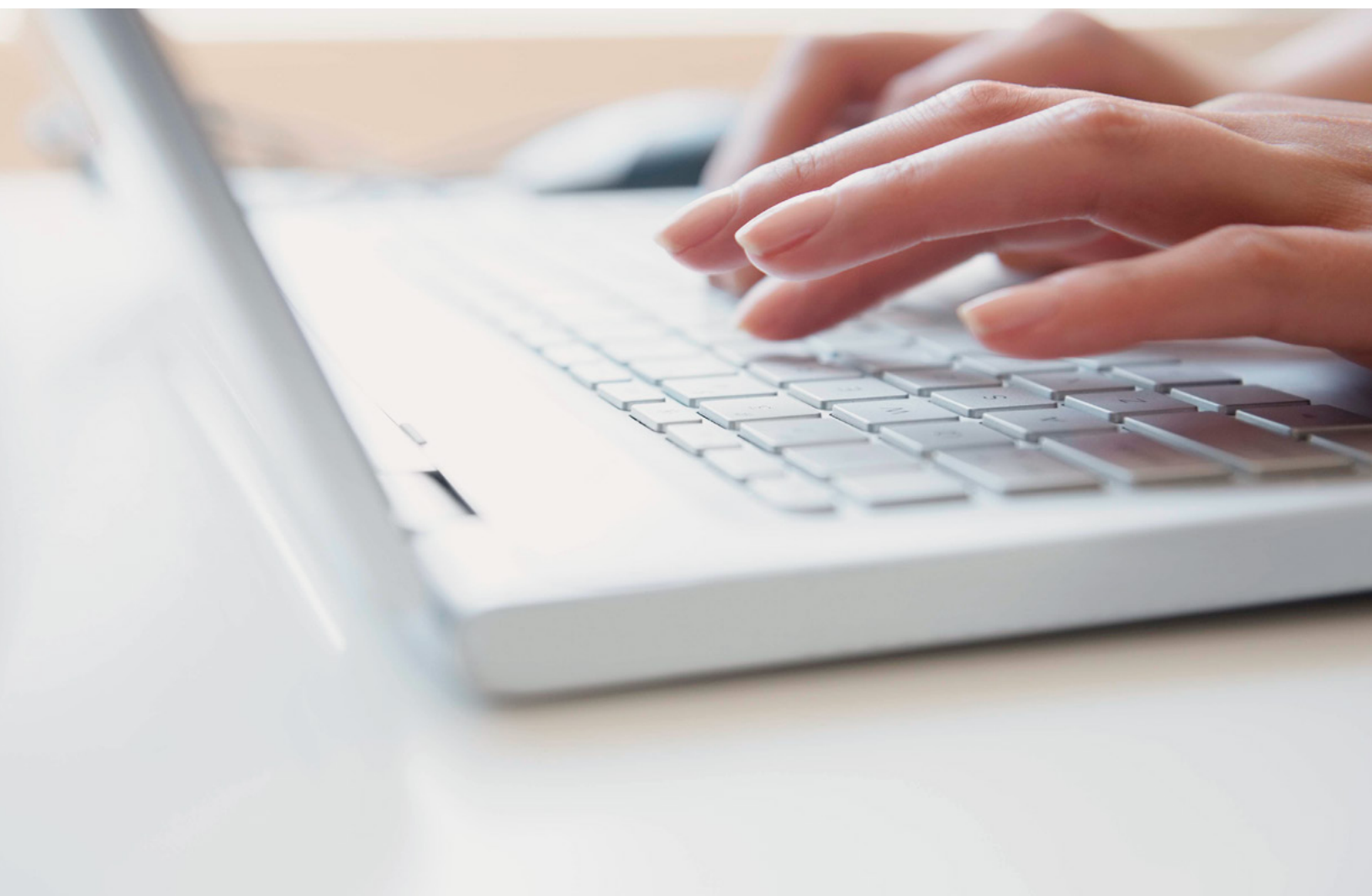


CYBERSECURITY

How to protect your organization from ransomware attacks



Ransomware attacks can debilitate your organization's IT structure, with disastrous financial and operational effects. As attacks become more aggressive, more frequent and more costly, organizations must develop specific response strategies to minimize ransomware's impact.

An alarming trend: In 2021, more ransomware attacks were recorded worldwide than ever before. Businesses should prepare for attacks to increase.



There were roughly 714 million ransomware attacks in 2021, according to SonicWall—a 134% increase year over year.



The average cyber insurance claim value of a ransomware attack during Q3 2021 was \$290,000, according to Corvus Insurance's Risk Insights Index.



The number of ransomware incidents reported to the FBI's Internet Crime Complaint Center (IC3) increased by 20% year over year, according to its most recent report from 2020.

Ransomware is rampant

The threat is so widespread that organizations should assume they're a target. "There's not a single organization out there that can ignore the threat of ransomware," said Adam Bulava, Global Head of JPMorgan Chase's Attack Simulation team. "Criminals will look to exploit any vulnerability they can find. When we talk about prevention,

we're really talking about mitigating the risk by building different layers of protection."

Fool you twice: Organizations can fall victim to repeat ransomware attacks, especially if they don't fix vulnerabilities after an initial attack.

"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."

Anne Davis, Head of Cybersecurity & Technology Controls, Commercial Banking at JPMorgan Chase

THE BOTTOM LINE

Every organization is responsible for determining appropriate controls and best practices to protect itself against ransomware.

How attacks occur

Ransomware is often delivered through phishing emails that appear to come from legitimate customers, vendors or other known contacts.

With the rise in remote work, cybercriminals have also exploited vulnerabilities found in remote desktop protocol and virtual private network software, which is often guarded by weak passwords.

Know the red flags: Make sure your team is suspicious of any unsolicited emails, even from familiar people, that may include:

- Poor grammar and spelling or unusual layouts
- Suspicious attachments or URLs
- Generic greetings and signatures
- A sense of urgency

Attacks are costly

Ransom demands in a ransomware attack can range from a few hundred dollars to millions of dollars. But the ransom is only the tip of the iceberg.

A study by Sophos found that the global average cost to an organization recover from a ransomware attack is [\\$1.85 million](#). However, these hidden costs often dwarf a ransom demand:

- Lost productivity
- Equipment repair and replacement
- Remediation of data
- Reputational damage
- Legal fees

The newsmakers: Most recent ransomware attacks didn't make headlines. But the ones that did affected millions of people and cost millions of dollars.

- A critical pipeline operator was knocked offline by ransomware, disrupting fuel supplies across the East Coast and triggering a run on gasoline. The operator paid hackers \$4.4 million, and law enforcement only recovered [\\$2.3 million](#).
- One of the world's largest meat processors halted operations at plants after a ransomware attack. The meat processor paid hackers [\\$11 million](#) to regain access.

- An IT solutions company was hit with ransomware, creating a fallout for nearly [1,500 client companies](#). The hackers demanded \$70 million from the IT business.
- It's not just the private sector. The city of Baltimore was attacked with a \$76,000 ransom demand, but its estimated recovery costs were [\\$18.2 million](#)—\$10 million to repair IT infrastructure and \$8.2 million in lost or delayed revenue.

Nightmare scenario: Ransomware may disrupt an organization's entire IT infrastructure, email communications, access to sensitive files and the ability to send or receive payments, such as payroll. For healthcare organizations, ransomware may mean the difference between life and death if providers are unable to access patient medical records.



\$1.85 million

the global average cost to an organization recover from a ransomware attack¹

¹ 2021 Sophos State of Ransomware in Healthcare Report



How to enhance your organization's resiliency

A cybersecurity plan is a first line of defense, not an exhaustive set of safeguards.

Plan for the worst: Prepare for a ransomware like you would any other disaster that would disrupt business continuity. It's important to have a robust [incident response plan \(IRP\)](#) and [disaster recovery plan \(DRP\)](#).

An IRP is designed as a blueprint with procedures and responsibilities to help your organization recover from cybersecurity incidents that don't halt operations.

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. An effective DRP includes:

- Outlined procedures and instructions to follow in a crisis
- Business processes
- Organizational assets
- Anticipated recovery times

4 stages to develop a DRP

Here's how to start your disaster recovery plan.



1. Conduct a business impact analysis (BIA)

A BIA predicts the consequences of a business disruption and gathers the information necessary to develop recovery strategies.

Why it's key

This is the foundation for your entire DRP. Consider a wide range of potential impacts, including:

- Delays, lost sales and revenue
- Increased expenses (e.g., overtime labor, outsourcing or expediting costs, contractual penalties and regulatory fines)
- Customer dissatisfaction or defection and reputational harm



2. Identify critical systems

Identify and prioritize the systems and operations your organization will need to resume after a disaster.

Why it's key

In a crisis, you'll need to focus on recovering the systems with the greatest impact on your operations.

After an attack your organization may not be able to use its usual communication channels and internet connection. Your DRP should outline:

- Work-arounds to perform critical functions such as vendor payments and payroll
- Alternate communication channels
- A pre-executed memo addressed to your bank detailing how certain employees can contact the bank and the actions they're authorized to perform.



3. Develop the plan

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.

Why it's key

In the wake of an attack, you want the plan to be relevant and up-to-date.



4. Test and exercise

Test your DRP by conducting tabletop exercises and live rehearsals.

Why it's key

You don't want to learn of gaps or shortcomings in your plan during an actual attack. Simulations give your organization a chance to practice.



Steps to protect your organization

End-user training: Employees are usually the weakest link in the cybersecurity chain. Educate all users how to spot phishing emails.

Cyber insurance: It won't stop attacks, but it can help offset potential losses.

Professional incident response services: These can ease the burden by augmenting your organization's response capabilities and speeding up recovery operations.

Practice good cybersecurity hygiene with preventative measures, including:

- **Regular backups:** Store immutable copies in a secure location not directly connected to the network.
- **Segment your network:** Separate portions of your organization's network for different business functions, which limits ransomware's ability to move across your entire IT infrastructure.
- **Updates and patches:** These will close any known security vulnerabilities.
- **Safelist applications:** Only allow specified programs to run on your IT systems.
- **Protect your inbox:** Scan incoming emails for malicious software and links and attachments. Block suspicious messages and indicate when an comes from outside the organization.
- **Safeguard your end points:** Antivirus solutions alone won't sufficiently protect end points. Adopt security tools that include malware and ransomware protection, device firewalls, intrusion prevention and internet content filtering.
- **Limit privileges:** End users shouldn't be able to download and install unapproved software or make changes to the operating system.

What to do after your organization is attacked

Containment is paramount: Immediately initiate your organization's IRP. The goal is to limit the damage to only a few systems.

For example, after an employee opens an email containing ransomware, your business should:

- Quarantine each infected system to mitigate additional risks.
- Analyze each infected system to gather information, recover important data and re-image it before putting it back into service.

- Conduct scans of your network to ensure no other systems have been infected.
- Implement new countermeasures based on the indicators of compromise gleaned about the ransomware.
- Prepare a post-incident analysis.

Should you pay the ransom?

The [FBI](#) discourages paying ransoms to cybercriminals. Paying a ransom is no guarantee an organization will get any data back, and it emboldens future criminal acts.

Before paying a ransom, organizations should consider:

- Business continuity
- Obligations to shareholders
- Impacts on employees and clients

Do not make a ransom-related payment through your JPMorgan Chase account unless the firm provides written advanced approval for you to process such a payment. This includes payments that don't originate from your account but may originate from your intermediaries using accounts with JPMorgan Chase.

There is no way to completely ensure you will not be a victim of ransomware or another cyberattack, so heightened diligence and ongoing review of controls with your internal and external partners is of paramount importance.

© 2023 JPMorgan Chase & Co. All rights reserved. Chase Connect is a registered trademark of JPMorgan Chase Bank, N.A. JPMorgan Chase Bank, N.A. Member FDIC. [Visit \[jpmorgan.com/cb-disclaimer\]\(https://www.jpmorgan.com/cb-disclaimer\)](https://www.jpmorgan.com/cb-disclaimer) for full disclosures and disclaimers related to this content 1184551