CYBER READINESS
INSTITUTE

Ransomware Playbook 2025

How to prepare for, respond to, and recover from a ransomware attack.

CYBERREADINESSINSTITUTE.ORG

Ransomware Playbook

TO PAY OR NOT TO PAY

That's usually the first question organizations ask when hit with a ransomware attack. Unfortunately, there's no easy answer. Many organizations--especially small to medium-sized businesses (SMBs)--simply don't know how to protect themselves. Cybercriminals are now using artificial intelligence (AI) to create smarter, faster, and more deceptive attacks. It is more important than ever to be ready. This playbook provides a clear roadmap to prepare for, respond to, and recover from ransomware so your business can stay resilient no matter what comes your way.

55.8% of ransomware attacks targeted small organizations with 1-50 employees.

52.3% of ransomware attacks were caused by email/phishing attempts, making it the most consistent attack vector over the years.

Hornetsecurity Q3 2024 Ransomware Attacks Survey, October 15, 2025

PREPARE - RESPOND - RECOVER

A ransomware attack locks your systems or encrypts your data until a ransom is paid. Every organization is a potential target.

Attackers gain access in many ways:

- Phishing emails
- Unpatched or outdated software
- Malicious links, fake websites, or QR codes

Hackers are using AI to increase both the frequency and sophistication of these attacks. The best defense is a culture of cyber readiness. Every organization should focus on three steps:

Prepare

Respond

Recover

And at each step, there is one thing that matters most: current, tested backups.

Prepare

Preparation is your strongest defense. Backups are essential but so is building a workforce that knows what to do. Key elements to protect against ransomware include:

- Prioritize the data most critical to your organization and back it up. Make sure you can re-install from the backups, which are often in the cloud, and that the backups are tested frequently.
- Educate your employees to regularly backup any important company information on their own computers. Train your workforce in how to report a possible ransomware incident or unusual network behavior. Early detection is important.
- Contract with a vendor that will provide support if an incident occurs. Establish the contract, before an incident occurs, so you have access to the vendor immediately.
- Train employees how to spot and appropriately react to phishing emails – even ones that look like they are coming from someone in your organization. Use frequent phishing awareness communications and conduct routine phishing tests to reinforce the key message.
- Update all software with the latest security patches. Hackers are using AI to analyze newly released software patches and identify vulnerabilities faster than ever to exploit old software before organizations install the patch.
- Develop an incident response plan for ransomware attacks now--before the pressure is on. Questions to consider: What data is most critical to your organization? Does your insurance cover ransomware? Are you comfortable negotiating and possibly paying a ransom? Which law enforcement agency would you contact to report the crime?

AI isn't just for hackers. Use it to your advantage. A simple prompt like "Write an email to employees about how to spot a phishing email" can produce a polished, ready-to-send message in seconds.

Respond

Your organization has been hit by ransomware. Immediately isolate and shut down the infected devices or systems to stop the spread. Follow your incident response plan - if you have one - to contact the appropriate people. You've reached your first major decision point. Now is when the preparation pays off.

Scenario 1: Your organization has backups that work. No need to worry. You can restore your data completely and get back to work.

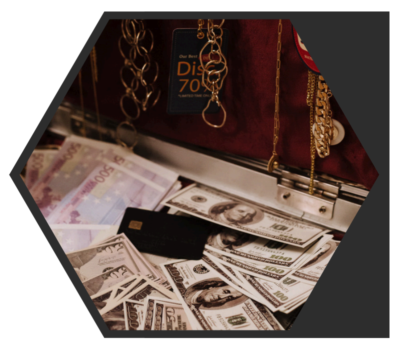
Scenario 2: Data that is held hostage is needed and there are no working backups.

a. Check if the data exists elsewhere in the organization (e.g., cache files, email) so you can piece together what is being held hostage.
b. If you can't access the data elsewhere, ask the following questions:
- Is the data critical to your operations?
- Has your leadership determined whether paying a ransom is an option?
- To what extent does your insurance cover ransomware?

Is the data being held critical to your organization?

Has your organization's leadership pre-determined whether it is ok to pay a ransom?

To what extent does your insurance cover ransomware attacks?
Are there conditions that must be met?



Recover

The speed and ease of the recovery depend on the scale of the attack and your preparation. Use the incident as a learning experience to reinforce the importance of cyber readiness principles like patching and phishing awareness.

Ensure your software is always updated with the latest security patches to make it harder to penetrate your system. Conduct routine phishing training to reduce human error and potential access to your system. As with any security breach, notify all affected parties, re-set the user IDs and passwords of all compromised devices, update the software on all devices, and re-install your data from backups once the ransomware threat has been neutralized.

It is critical to ensure patches are updated and passwords have been changed following an attack. If you re-install software from backups, check to make sure that the versions are up to date.

The Cyber Readiness Program includes detailed instructions and templates to help you create your own policies and incident response plan to prepare for, respond to, and recover from a ransomware attack. Sign up for free at CyberReadinessInstitute.org.

Use the decision tree on the next page to go through your organization's path to recovery. See how straightforward the process is if you have a current, tested back-up. If more preparation is needed, the Cyber Readiness Program includes detailed instructions and templates to help you create your own policies and incident response plan to prepare for, respond to, and recover from a ransomware attack.

Ransomware Decision Guide