CYBER READINESS
INSTITUTE

CYBERREADINESSINSTITUTE.ORG

Ransomware Playbook

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

By 2021

“every 11 seconds”

a new organization will fall victim to ransomware, according to market researcher Cybersecurity Ventures.[1]

Ransomware Playbook

To Pay or Not to Pay? This question is often the first one many organizations consider after they are hit with a ransomware attack.

Unfortunately, the choice is not simple. Many organizations simply don’t know how to protect against ransomware. This guide is intended to provide a roadmap for organizations (e.g., small and medium-sized businesses, state and local governments) to secure themselves against this growing threat.

[1] umbrella.cisco.com/blog/2019/12/17/ransomware-defense-for-dummies-2nd-edition

All organizations are at risk of having their valuable data – about customers, employees, operations – encrypted by a malicious actor so that the organization loses access to it. **A ransomware attack is conducted by a malicious actor to hold an organization's data hostage for a ransom.** Malicious actors can gain access to an organization's data through various means, including phishing and unpatched software. Patches are issued by software companies for vulnerabilities they find in their programs; many users fail to download the patches, which means the vulnerabilities can be exploited.

An organization that builds a culture of cyber readiness can be resilient against a ransomware attack by taking preventative actions (e.g., creating a backup of critical data) and developing and testing a ransomware incident response plan. An organization should focus on three steps: **Prepare, Respond, and Recover.**

STEP 1

Prepare

STEP 2

Respond

STEP 3

Recover

Prepare

Make sure your company regularly backs up its data; storing dating in the cloud is a common tool used for backups. If your employees save important business information on their own computers, your organization should also provide clear instructions to your employees on how to back up their data on a regular basis. Key elements to protect against ransomware include:

- Prioritize the data that is 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.
- Early detection is important, so make sure your workforce knows how to report a possible ransomware incident or unusual network behavior.
- Contract, if possible, with a vendor that can provide response support if an incident occurs. Establish a contract, pre-event, so you have access to the vendor immediately.

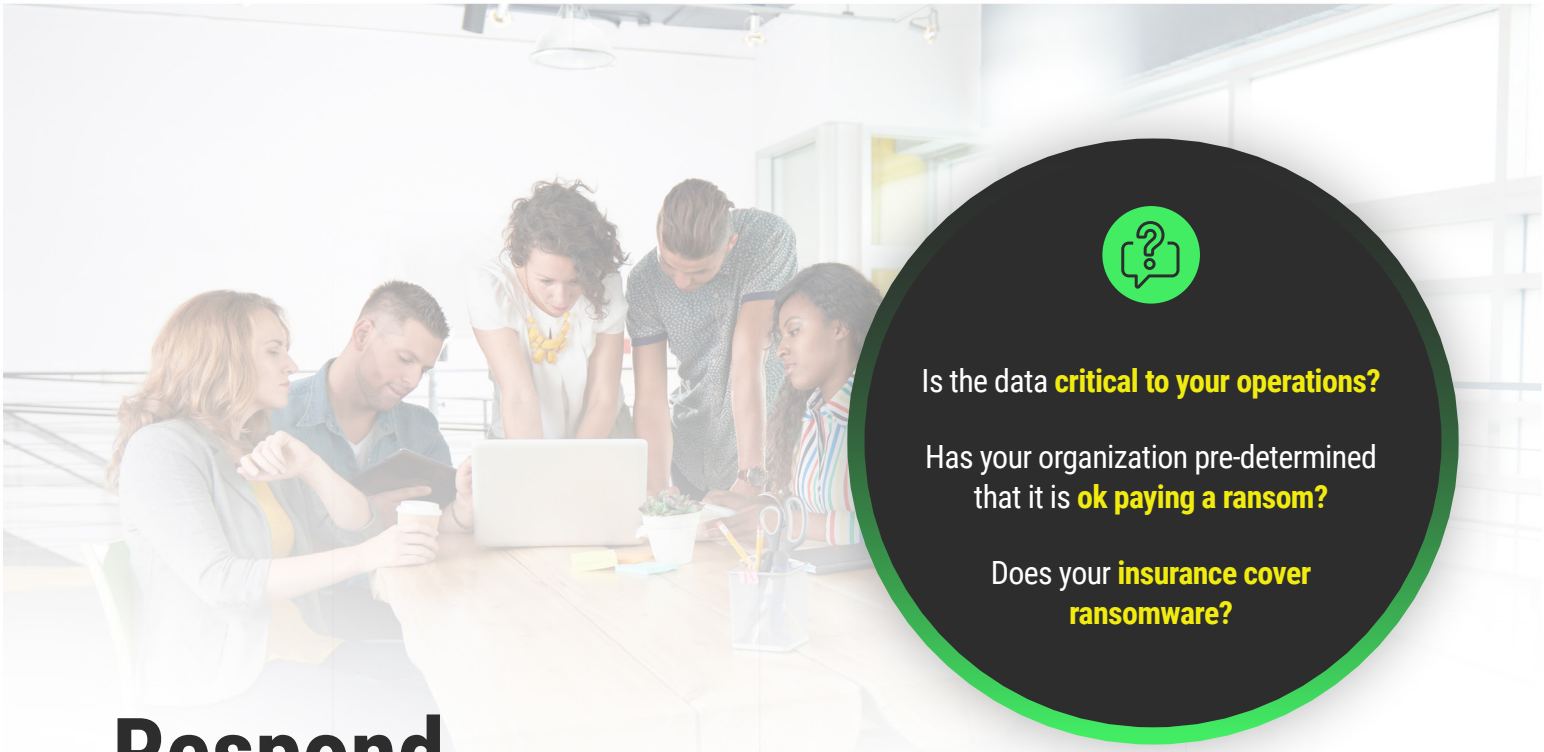
Since malicious actors often use phishing to infect a system with ransomware, it is crucial to have a phishing policy. Conduct routine phishing tests so employees will be able to detect a phishing email before clicking on any dangerous links or attachments and, when possible, use an anti-phishing software program.

Update your software with the latest security patches. This critical preventative step will make it harder for malicious actors to compromise your system.

Develop an organization-wide policy regarding ransomware attacks. It is much easier to have these discussions when the pressure of response is not looming. Questions to consider: What data is most critical to your organization? Does your insurance cover ransomware? Are you OK with paying a ransom? If so, do you understand how to use bitcoin and other crypto-currencies?

Discuss and agree to an organization-wide policy regarding ransomware attacks.

It is much easier to have these discussions when the pressure of response is not looming.



Is the data **critical to your operations?**

Has your organization pre-determined that it is **ok paying a ransom?**

Does your **insurance cover ransomware?**

Respond

If an employee or the organization is confronted with a ransom request, your organization must first assess the legitimacy of the ransom request by contacting your IT manager. If it is legitimate, two possible scenarios are presented:

1. **Your organization has backups that work.**
   You don't need to worry about the ransomware.
   You restore your data completely and get back to work.

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

   a. Check if the data exists somewhere else in the organization (e.g., cache files, email) so you can "tape" together the data to replace 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 organization pre-determined that it is ok paying a ransom?
   - Does your insurance cover it?

Recover

The fire is out and it's time to return to business as usual. The scope of the ransomware attack and the severity of its impact on your daily operations will determine how much time and effort is needed to recover. Use the incident as a learning experience to reinforce the importance of cyber readiness principles like patching and phishing awareness.

Ensuring that your software is always updated with the latest security patches will make it harder to penetrate your system. Likewise, enforcing routine phishing training minimizes human error and the potential entry points into 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 especially important to ensure patches are updated following the attack. If data has been restored, sometimes vulnerabilities that were patched, pre-ransomware, can reappear.

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 **BeCyberReady.com**.

To read about real examples of how companies and municipalities responded to a ransomware attack, please visit **Cyber Readiness News.**

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

Have you prioritized your data and systems so you know what is most critical to your business operations?

PREPARE

Do you have an incident response plan that covers ransomware?

Identify what is most valuable. Go to **BeCyberReady.com** to access a prioritization checklist.

Develop an incident response plan that covers ransomware. Go to **BeCyberReady.com** to access an incident response plan template.

Do you have a current backup?

Back up your system and all data.

Have you tested it in the last month?

Test your backup to make sure you can recover your data – especially the most critical to your business operations.

Congratulations. **You're prepared.**

You better hope you don't get a ransomware attack. **You are REALLY unprepared.**

Ransomware Incident Occurs

RESPOND

Isolate the incident and remove the infected computer(s) from the network. Then proceed.

Great job. **Go directly to Recover!**

Do you have an IT support to contact?

Can you or your IT support back up in real time?

Is the data being held hostage valuable to your business?

Do you have cyber insurance?

Does your policy cover ransom events?

Your data is unrecoverable… **decide whether or not to pay.**

RECOVER

Go into the real time backup and clean out the malware.

Reset user IDs and change passwords

Do a clean install from your backup

Update your software

Selectively reinstall data

You are back in business!!
Sign up for the free Cyber Readiness Program at **BeCyberReady.com** to prevent more ransomware attacks in the future.

guide@cyberreadinessinstitute.org