eventus

# Ransomware Playbook

How to prepare for, deal with,
and recover from a ransomware invasion

# Cybercrime To Cost The World $10.5 Trillion Annually By 2025[1], Mentions Cybercrime Magazine In A Special Report Published On Nov. 13, 2020.

## Ransomware Playbook

Should I pay or should I not pay? This is frequently the first question that many firms ponder following a ransomware assault.

Unfortunately, the option is not straightforward. Many businesses simply do not understand how to defend themselves against ransomware. This guide is meant to give a road map for organisations (such as small and medium-sized enterprises, state and local governments) to follow in order to protect themselves against this expanding danger.

[1] https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/#:~:text=The%20latest%20forecast%20is%20for,every%2040%20seconds%20in%202016.

All firms risk the chance of a malevolent actor encrypting their valuable data — on customers, staff, and operations – so that they lose access to it. A malicious attacker conducts a ransomware assault to keep an organization's data hostage for a ransom. Several methods, including phishing and unpatched software, allow malicious actors to get access to an organization's data. Software firms release fixes for vulnerabilities they discover in their systems; however, many users neglect to download the updates, allowing the vulnerabilities to be exploited.

By adopting precautionary measures (e.g., generating a backup of essential data) and building and testing a ransomware incident response strategy, a company can be robust against a ransomware attack. A company should concentrate on three steps: Prepare, Respond, and Recover.

# I Prepare

Ensure that your organisation frequently backs up its data; cloud storage is a typical option for backups. If your workers save crucial company data on their personal computers, your firm should also give them with clear instructions on how to regularly back up their data. Key components for ransomware protection include:

- Prioritize and back up the data that is most important to your company. Always make sure your backups are tested periodically, and that you can reinstall from them if necessary.

---

- Importantly, ensure that your employees are aware of how to report a potential ransomware event or strange network behaviour.

---

- If at all feasible, enter into a contract with a vendor who can offer reaction help in the event of an emergency. Create a contract before the event so you can contact the vendor right away.

Because threat actors frequently employ phishing to infect a system with ransomware, a phishing policy is essential. Conduct regular phishing tests so that staff can spot a phishing email before clicking on any risky links or attachments, and utilise anti-phishing software when possible.

Get the latest security patches for your software and install them. This important precaution will make it harder for bad people to get into your system.

Create an organization-wide policy for dealing with ransomware attacks. It is much simpler to hold these talks when there is no imminent deadline. Consider the following: What data is most essential to your organisation? Is ransomware covered by your insurance? Are you willing to pay a ransom? If so, are you familiar with bitcoin and other cryptocurrencies?

Discuss and agree on a policy addresasing ransomware attacks across the business.

When there isn't a deadline pressing, it's much simpler to have these interactions.

**Are the data vital to your business operations?**

**Has your company already decided that paying a ransom is acceptable?**

**Does your insurance cover ransomware?**

# I Respond

If an employee or the company is presented with a ransom demand, your company must first call the IT manager to determine the authenticity of the ransom demand. If it is valid, there are two possible outcomes:

**1**

**Your company has functional backups.**

**You do not need to be concerned about ransomware.**

**You totally restore your data and return to work.**

**2**

**We need the data that is being held hostage,**
**and there are no backups that work.**

**a.** Check to see whether the data is available elsewhere in the company (e.g., cache files, email) so you may "tape" the data together to replace what is being held captive.

**b.** If you are unable to get the information elsewhere, consider the following:

- Are the data vital to your business operations?
- Has your company already decided that paying a ransom is acceptable?
- Is it covered by your insurance?

# | Recover

The blaze has been extinguished, and normal operations may resume. Time and resources required to recover from a ransomware assault depend on the scale of the attack and the extent to which it disrupted your day-to-day operations. Remind people of the significance of cyber preparation practises like patching and phishing awareness by using this occurrence as a teaching moment.

Making sure your software is updated with the most recent security updates will make it more difficult for hackers to access your device. Similar to how frequent phishing training is enforced, it reduces human mistake and possible entry points into your system. As with any security incident, after the ransomware threat has been eliminated, notify all parties impacted, reset the user IDs and passwords of all compromised devices, update the software on all devices, and reinstall your data from backups.

It is extremely critical to ensure that fixes are updated after an attack. If data has been recovered, pre-ransomware vulnerabilities that were addressed may return.

---

Develop your own policies and incident response plan to prepare for, respond to, and recover from a ransomware attack.

---

Learn more about real-world examples of how businesses and municipalities responded to a ransomware assault.

---

Eventus provides a number of ready-to-use products and assets, such as a Ransomware Readiness Checklist that covers 9 essential elements and may be used by you right away to enhance your level of readiness. Incident Response Framework and Quick Guide for the first responder are very useful assets and reference material when you are under attack.