



5 Steps to Proactively Address Ransomware Threats

No business, no industry is immune to ransomware attacks. As a cyber insurance provider, we believe that it is our duty to provide our policyholders and all organizations that are threatened by such criminal activity with information and resources to prevent ransomware incidents.

Here are 5 steps that are critical to maintaining secure business operations online:

① Understand your third-party risk.

- Do you conduct a thorough cybersecurity vetting of third parties and supply chain partners?
- How often do you revalidate the security measures of third parties?
- Do you have visibility into fourth parties (the suppliers of your suppliers)?

② Ensure deployment of Multi-Factor Authentication (MFA) on all systems.

MFA is the first line of defense against cybercriminals as they attempt to breach your network or applications. MFA can provide protection against unlawful access even when user credentials (usernames and passwords) have been compromised.

Nowadays, most cloud-based applications and services offer MFA out-of-the-box, with the ability to centrally enforce its use for all accounts.

- Do you require MFA for all employees, contractors, and third-party service providers to use your organization's network or systems?
- Is MFA deployed on all systems and for all users: email, cloud services, SaaS applications, collaboration tools, remote desktop access, etc.?

If you are new to MFA, we have put together [an FAQ on MFA](#) to get you started.



③ Prepare your organization to respond to a cyber incident with an incident response plan.

Knowing whom to call, what steps to take (or to not take, like engaging directly in ransom negotiations), and what information to collect, is important to have at hand before an attack takes place. An incident response plan will help you recover as quickly as possible.

Cyber incidents are times of crisis when people need leadership and clear directions. A cyber incident response plan brings clarity and specifies key personnel identified to carry out specific tasks when a cyberattack hits. Such a plan should include specific actions for ransomware events.

Here is also a summary of [quick steps to take when you discover an incident](#).

④ Use network segmentation to protect sensitive assets

Network segmentation has many benefits. By isolating segments of your network using firewall rules or air-gapped measures, you can limit the scope of a ransomware attack and prevent it from impacting critical systems and sensitive data. Note that network segmentation will directly contribute to (1) your organization's ability to comply with many regulations, (2) your insurability and the optimization of your insurance premium.

⑤ Know your backups.

Having ready-to-go backups for systems and data gives the response team negotiating power and keeps open the option not to pay the ransom.

- Does your organization have backups?
- Are they encrypted, tested, and separate from the company network? i.e. either offline/air-gapped or in a cloud service designated for this purpose.
- If you are using 3rd party applications, you need to ask them the same questions?



Access Expert Resources

Cowbell partners with security providers (product and services) to help you strengthen your cybersecurity or even run a cybersecurity program for you.