E-COMP NOW!
Business Insurance Simplified

5 Steps to Proactively Address Ransomware Threats

Ransomware attacks are skyrocketing, impacting large & small businesses and disrupting entire supply chains such as oil distribution (Colonial Pipeline in May 2021) and the national food supply (JBS in May 2021). No business, no industry is immune to ransomware attacks.

As an insurance brokerage, we believe that it is our duty to provide information not only to our current policyholders but to all organizations that are threatened by this criminal activity. E-COMP strives to provide the best available resources and advice to keep everyone protected from these kinds of attacks.

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. It can provide protection against unlawful access even when user IDs 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.

Need Live Expertise? Call: 888-493-2667 or email us: service@goecomp.com

E-COMP NOW!
Business Insurance Simplified

3 **Prepare your organization to respond to a cyber incident with an incident 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 know *before* a ransomware attack takes place. You should have a ransomware incident response plan in place to 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 should be clear, with key personnel identified to carry out specific tasks and responsibilities 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 further sensitive assets and infrastructure on your network.**
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 your organization's ability to comply with many regulations.

5 **Know your backups.**
Having ready-to-go backups for systems and data will give the response team negotiating power and will most likely give you the option to not 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

E-COMP partners with security providers (product and services) to help you strengthen your company's cybersecurity or even run a cybersecurity program for you. Contact us for a recommendation.

Need Live Expertise? Call: 888-493-2667 or email us: service@goecomp.com