THE ONLY THING WORSE THAN A RANSOMWARE ATTACK? MISHANDLING ONE

Kevin Beasley, CIO at VAI, oversees the corporation's overall technology strategy.

March 10, 2022 • Forbes • Kevin Beasley

Imagine starting your workday and your screen suddenly goes dark. It turns out a hacker has encrypted the files on your device and the only way to stop them from leaking the information is to pay up — fast.

While you hope to never see your business fall victim to a ransomware attack, organizations experienced 17% more incidents in 2021 than they did in the previous year. Using a form of malicious malware, a hacker encrypts the files on an organization's device and threatens to leak the information unless the victim pays a ransom. And no one is safe from these attacks: Organizations of all sizes and industries are at risk.

In addition to the ransom itself, ransomware attacks pose an added risk of disruption, downtime, lost revenue and customer distrust. Now, more than ever, you need to prioritize security. But you also need to know what to do in the event of an attack.

The Aftermath Of A Ransomware Attack

The world's largest meat supplier, JBS Foods, fell victim to a ransomware attack in May 2021. The company recovered with the help of consultants and government officials, but not before the attack wreaked havoc on the entire organization's operations.

The incident unleashed a domino effect, causing plant shutdowns, increased wholesale prices and, ultimately, an $11 million loss in ransom. This type of attack also has a negative impact on customer trust. On average, more than two-thirds of consumers lose trust in an organization after a data breach.

This is just one example of the millions of ransomware attacks that occur every year. In 2021, ransomware attacks climbed 158% in North America alone. And more than just the frequency is increasing — ransom demands are also growing.

What does this mean for your organization? Simply put, cybersecurity cannot be an afterthought. You need to proactively shore up cybersecurity measures, prioritize security in all business initiatives and ensure your cybersecurity coverage is in place. To get started, consider these tips:

- **Ensure** an enterprisewide understanding of security measures through training.

- **Require** multifactor authentication (MFA) and complex passwords for login.

- **Implement** network

segmentation.

- **Update** software and scan for vulnerabilities regularly.

- **Administer** endpoint and detection response tools.

- **Ensure** that your cyber insurance policy is in place.

Operating under cybersecurity best practices can significantly reduce the likelihood of falling victim to an attack, but there are no guarantees. Considering the rise in frequency and severity of these attacks, you also need to have a thorough response plan in place.

Your Data Has Been Compromised. Now What?
In the event of a data breach, an agile and informed response can go a long way. Fast action not only helps mitigate the consequences of the breach — it can also help you regain affected customers' trust more quickly. Contact authorities such as CISA and contact your insurance company.

The Federal Trade Commission (FTC) provides regulatory guidelines explaining the steps businesses should take in the event of a breach. Your actions may vary slightly depending on the severity of the incident, but in most cases, you should follow these steps:

- **Take equipment offline**. To avoid further data loss, pull all affected equipment offline immediately — but do not turn any devices off until a forensic expert is present. If viable, replace affected equipment, update credentials, and carefully monitor entry and exit points.

- **Secure systems.** The next thing you need to do after discovering a ransomware attack is to fix vulnerabilities that could have led to the breach. Change computer passwords and secure physical areas, including switching access codes if needed.

- **Call in a team of experts.** In all instances, but especially when dealing with a severe data breach, you need to work with a team of experts to create a comprehensive response plan. This may include forensics, IT, information security, human resources or legal teams. Also, consider hiring a third-party investigator to identify the source of the breach. Refer to your legal counsel to ensure compliance with regulations that may be connected to a breach.

- **Remove posted information from the web.** Bad actors often post stolen data on the victim's website or other sites. Search your company's name and the exposed data to ensure the information is not located anywhere else. You may have to contact the administrator of another website if the information needs to be removed.

- **Interview and investigate.** Speak with the person who discovered the breach and anyone else who may have knowledge about the incident. If your organization has a customer service center, communicate with staff so they know where to relay important information regarding the breach. Most importantly, do not destroy evidence during the investigation.

- **Address vulnerabilities.** Consider the service providers you work with. What personal information do they have access to? Ensure your providers have appropriate access privileges, and if they were involved in the breach, make sure they are taking the required steps to prevent a future breach. Verify that they fix their own vulnerabilities before continuing the partnership. Additionally, evaluate whether your network segmentation was successful in containing the breach and make changes accordingly.

- **Communicate clearly.** All states have regulatory guidelines in place regarding who you should notify in the event of a breach (e.g., other businesses, stakeholders or customers). Check federal, state and local laws for additional requirements. Prepare a thorough communication plan, because after discovering a ransomware attack, people will have questions and concerns. Explicitly state how the breach happened, what information was stolen, what actions you are taking to address the breach and what actions you will take to protect victims of the attack (e.g., offering free credit monitoring services).

With the number of ransomware attacks on the rise, it is essential to practice safe computer habits and understand the steps to take in the event of a breach. Ensure all members of your organization are aware of cybersecurity best practices and policies and consistently remind people to remain vigilant. Preparation is key, so start today to minimize the chance of falling victim to a ransomware attack.