CAPINTECH

3 Ways to Defeat Ransomware: Plan, Prevent, Not Pay

By Lindsey P. Whinnery, Partner

Imagine you are in the middle of your workday and you double-click on one of the 50 Excel files saved to your desktop. Instead of seeing multiple columns and thousands of rows of data, you receive an error message stating your file cannot open unless you pay someone by the name of 4N0M4LY a certain amount of bitcoin. You need to access this file immediately, and you have no other copies of it since you do not back up your desktop. What do you do next?

Unfortunately, this ransomware nightmare scenario is common, and there is no indication that this type of attack will slow down. Ransomware attacks continue to dominate headlines and plague organizations of all sizes in both the private and public sectors. As with other cybersecurity attacks, no organization is immune. Your best option is to prepare for this type of attack by using a three-pronged approach: plan, prevent, and not pay.

Plan

During a ransomware attack, the general mood is panic. Time is of the essence, so having a plan is critical. Here are a few steps that you will want to define.

- **Containment:** Immediately disconnect the infected system(s) from the network — wired, wireless, and Bluetooth connections. You want to make sure the ransomware will not spread to other systems on the network. It's also important to immediately hibernate or power off the system(s).
- **Check other systems:** Ransomware can spread. Run full-system scans of all the workstations and servers on the network to help detect ransomware on other systems.
- **Format and restore:** Format the infected system(s) several times and restore the operating system. Use your backups to restore the data.
- **Retain outside IT support:** Develop a relationship with an IT forensics company, an emergency IT support company, or both. It's likely that your IT department is already overloaded and may not have the resources to recover from a large-scale ransomware attack in a reasonable time period. Being able to call upon outside help immediately could help drastically reduce the impact of a ransomware attack and the time it will take to restore your operations.

Prevent

While it's impossible to completely prevent a ransomware attack, you can implement some important safeguards to significantly reduce your risk of becoming a ransomware victim.

- **Train end users:** Your end users are your front line of defense. The majority of ransomware is downloaded when end users click on malicious links or open malicious email attachments. Systems can also be infected with ransomware when end users visit infected websites. Ransomware is frequently downloaded and installed on the computer in the background while the end user is innocently browsing. Training will reduce the risk of ransomware entering your network.
- **Use email security software:** Since a majority of ransomware attacks begin with end users clicking on links in an email, email security software will reduce the number of emails with malicious links and attachments arriving in your end users' inboxes. Systems can filter suspicious emails for review or even strip potentially malicious links from the email.
- **Anti-malware software:** Anti-malware software can prevent some forms of ransomware, so it is important for all devices to have this sort of software installed and configured for periodic full-system scans and on-access scanning.
- **Back up your data:** Backing up your data will not prevent ransomware attacks, but it will prevent you from having to consider paying the ransom. All critical data should be backed up, and it is important to have

Taking these steps now can help you avoid a ransomware attack and reduce the impact should one occur within your network.

multiple versions of data backups, such as weekly and monthly versions. Ransomware could encrypt files and go undetected for weeks, if not months. Having multiple versions of backups will increase your chances of having an uninfected backup to restore from. Also, these backups should be disconnected from the network, since ransomware attacks are notorious for specifically seeking out known backup files and encrypting those files, too.

Not Pay

If you do not have a backup to restore from, you may find yourself asking: Should we pay the ransom to get our data back? Consider the following.

- **Look for a solution:** Start by checking nomoreransom.org, which lists several known ransomware attacks and the associated decryption keys. You may be able to unlock your data without having to pay the ransom.
- **Don't fund criminals:** If you pay the ransom, you're funding criminals and unintentionally supporting the ransomware business, which will continue to grow with each ransom payment made.
- **Don't trust criminals:** As in any ransom situation, there is no guarantee that you'll receive the decryption key after paying the ransom. Even if you do receive a decryption key, it may not work and it's unlikely the criminal will provide tech support to determine the issue.

Taking the plan and prevent steps now can help you avoid a ransomware attack and reduce the impact should one occur within your network. It's important to layer controls so that if one fails, others are in place to help prevent an attack.

This article was originally published in The Journal of Accountancy.

About the Author

Lindsey Whinnery, Partner
CapinTech
lwhinnery@capincrouse.com
o 505.50.CAPIN ext. 2003

Lindsey has over 20 years of experience in information technology and information security. Lindsey provides review and consulting services with an emphasis on nonprofit organizations, higher education, financial institutions, and healthcare facilities. She stays current on changing threats, government regulations, and various organizations' security frameworks to design audit work programs and better assist clients in implementing appropriate controls to protect against cybersecurity threats.

About CapinTech

Capin Technology, a CapinCrouse company, provides information security services, including cybersecurity assessments, consulting, and training services, to financial institutions, nonprofit organizations, medical entities, professional services firms, and other organizations. Each year the firm performs hundreds of assessment, consulting, and speaking engagements with a team of experienced professionals retaining numerous certifications, including CPA, CISSP, CISM, CISA, CITP, CGMA, and CTGA. Each engagement is tailored to fit the unique needs of the organization, and information and reports are presented in a clear, concise manner intended for an audience with varying information systems (IS) knowledge. More information is available at capintechnology.com.

About CapinCrouse

As a national full-service CPA and consulting firm devoted to serving nonprofit organizations, CapinCrouse provides professional solutions to organizations whose outcomes are measured in lives changed. Since 1972, the firm has served domestic and international outreach organizations, universities and seminaries, foundations, media ministries, rescue missions, relief and development organizations, churches and denominations, and many others by providing support in the key areas of financial integrity and security. With a network of offices across the nation, CapinCrouse has the resources of a large firm and the personal touch of a local firm. Learn more at capincrouse.com.

CapinCrouse is an independent member of the BDO Alliance USA.