Ransomware Readiness & Recovery: Do's and Don'ts to Safeguard Your Data

If you wait till an attack occurs, it will be too late. Get ready now. Today.

By Bryce Austin

If you think your organization is safe from a ransomware attack, think again. It's happening to many nonprofits, and the results are devastating. Even if you're able to pay the ransom, you may still lose some or all of your data, and it may take months afterward to assure that your systems are safe.

Stopping ransomware includes three key areas: cybersecurity hygiene of your employees, proper practices by your IT department, and a solid data-backup strategy. Here are ways to prevent a ransomware attack and to recover if you fall victim to one:

Add Multi-Factor Authentication (MFA) to all your organization's e-mail accounts and to all external access to your network (VPN, TeamViewer, WebEx, and so on). This will help prevent a cybercriminal from taking over an e-mail account using a compromised username or password.

If your organization uses Windows Active Directory, do *not* log in to computers with Domain Admin accounts. There is an attack called "Pass the Hash" that will steal encrypted (hashed) credentials left behind. If you must log in with a Domain Admin account, change the password.

Patch your PCs, workstations, servers, and networking gear. Every month. No exceptions. That includes your phone systems, firewalls, switches, conference-room PCs, loaner PCs, HVAC computers, and so on. (To patch means to update and fix any bugs or security vulnerabilities; there's patching software available to help you do so.)

Geofilter your internet traffic and e-mails. Geofiltering means to block access to internet content that's not relevant based on your geographical location. In other words, if you don't do business with a foreign country, you want to block traffic and e-mails to and from that country. Geofiltering will keep out lazy cybercriminals. No, it won't keep out the cybercriminals that VPN into your country before attacking you, but it's surprising how many cybercriminals don't take the time to do that. (VPNs, or "Virtual Private Networks" encrypt your internet traffic and disguise your online identity, making it harder for cybercriminals to steal data.)

If your organization has many workstations, use the Microsoft Local Administrator Password Solution (LAPS) to randomize the local administrator password on all PCs. If you have the same initial local admin username/password for every workstation, then if one machine gets compromised, it's very easy for them to all get compromised.

Don't give local admin credentials to your users. If cybercriminals compromise a computer, they normally inherit the permissions of the user for that computer. If that user is a local administrator, the bad guys are going to use that access to do more damage.

Perform OFFLINE backups. These are backups that are kept off your network. Cybercriminals try to delete your backups. If your backups aren't on your network, the bad guys can't destroy them.

Test your restore procedures. If you try to restore your backups only when you need them, you're rolling the dice every time you're in a real bind.

Keep 35% free drive space on all network drives. Ransomware often bloats the data on the drives it encrypts. As soon as a drive fills up, the encryption process will keep

trying to move forward, but every file it encrypts after the drive is full will be unrecoverable.

Find a cyber-incident response company and get a contract in place. That way you'll know how to "call in the cavalry" very quickly as opposed to going through contract negotiations in the middle of a crisis.

If you've been the victim of an attack, don't begin to restore your data with your network still attached to the internet. In many ransomware cases, the cybercriminals still have hooks into the organization's network, and they destroy the used-to-be-offline backups as soon as the restore process begins.

If you have cybersecurity liability insurance, call your insurance company as soon as an incident occurs. Many insurance policies state that customers must inform their insurance company of a suspected cyber attack within 24 hours of the initial discovery. If you take a few days before reporting the attack, it can be an expensive mistake.

If everyone followed the recommendations in this article, ransomware cybercriminals would become a thing of the past. With a solid plan and cybersecurity-awareness training for your employees, cybercrime is a solvable problem.

Bryce Austin (bryceaustin.com) is the CEO of TCE Strategy, an internationally-recognized speaker on emerging technology and cybersecurity issues, and author of Secure Enough?

Don't Be a Victim

Take care to prevent not only ransomware attacks but other common risks that can devastate your organization. For more ways to keep your data safe, turn to these articles at NonprofitWorld.org:

- **Nine Surefire Steps to Lock Down Your Cybersecurity** (Vol. 36, No. 3)
- **Mitigate Cyber Risks with the Right Security Controls** (Vol. 36, No. 1)
- **Hacking People: Why Your Biggest Vulnerability Isn't in Your IT Department** (Vol. 37, No. 1)
- **Are You Prepared for a Cybersecurity Incident?** (Vol. 38, No. 4)
- **Can Your Organization Afford to Lose $100,000? Safeguards Every Nonprofit Needs to Implement** (Vol. 30, No. 3)
- **Don't Get Caught by Phishing Schemes** (Vol. 35, No. 2)
- **Avoid Catastrophe by Addressing Cyber Risk** (Vol. 33, No. 3)
- **Wire Transfer Fraud: It Could Happen to You** (Vol. 35, No. 3)
- **What to Do When an Employee Becomes a Cybercriminal** (Vol. 39, No. 4)
- **Keep Your Online Identity Safe** (Vol. 35, No. 4)

please get in touch...

We would love to hear your response to anything in **Nonprofit World**, your comments about any aspect of the nonprofit sector, and your concerns about your daily work. Please get in touch in any of the following ways:

Drop us a note at: Letters to the Editor, Nonprofit World, P.O. Box 44173, Madison, Wisconsin 53744-4173.

E-mail to: muehrcke@charter.net

Please include your name, organization, address, phone number, and e-mail address. If you'd like your comments to appear anonymously, please let us know. We look forward to hearing from you!

WHAT'S UP ONLINE?

Would you like to discuss some of the issues addressed in ***Nonprofit World*** with other nonprofit professionals? Do you have questions to ask or expertise of your own to share?

Society for Nonprofits is actively engaged on LinkedIn, Facebook and Twitter. Find us on your favorite social media platform by visiting **social.snpo.org**

If you have any questions, contact Jason Chmura at jchmura@NonprofitWorld.org