syncplicity by axway

8

WAYS TO HELP KEEP RANSOMWARE FROM HOLDING YOUR DIGITAL FILES HOSTAGE

Business leaders across industries are justifiably nervous about ransomware attacks. While there is no foolproof way to prevent one from happening to you, there are measures you can easily take now to better defend against this new and destructive type of malware; and, if attacked, recover quickly with a solid remediation plan in place. Here are 8 tips to sound ransomware prevention and recovery.

01 **Back up files in real time.** There's no silver bullet when it comes to stopping ransomware attacks, but if you want to play it safe, industry experts have three words for you: "backup, backup, backup." It's easier said than done because it could involve extra manual steps and backup jobs that never get complete. But Syncplicity can help make backup easy and seamless. Files and folders are backed up automatically in real time. Users sync their folders once and move on, eliminating worries about data loss.

02 **Ditch the single "magic folder."** Back up every folder on your desktop automatically with Multi-Folder Sync. It lets users and admins sync all files and folders in place without moving them to a "magic folder." In the event your company or a user is breached by ransomware, Multi-Folder Sync has your back. Every file in every folder on Syncplicity is backed up, not just the lucky few files that made it into the single "magic" folder offered by others. Educate your users to sync all their critical files and folders, including Desktop and My Documents. You can proactively specify the sync of any desktop folders to ensure that users are safe.

03 **Establish an enterprise retention policy.** Common ransomware does harm by deleting files and replacing them with renamed encrypted versions, or by retaining filenames and encrypting the contents in place. In both cases, you'll need to ensure the files can be recovered. With Syncplicity's deleted files retention policy, you can retain deleted files forever or for a specified time period, letting you retrieve your original files after an attack. You should review file-version retention policies that control how long prior versions of a file are saved after they have been edited or overwritten.

"Over the last 18 months Syncplicity has seen a significant rise in the number of incidences and we've assisted customers in healthcare, manufacturing, hi-tech, education and others with their data recovery efforts."

Brian W. Levine,
Axway Director of Cloud Security

04 **Block risky file types.** Administrators can contain or stop the spread of an attack by blocking problem file types from syncing. Syncplicity file type exclusion policy gives you the ability to pre-emptively block known crypto document types like .scry, .locky and .crypt filename extensions. You can also block files containing potentially malicious executables such as .vbs, .scr, and .exe.

05 **Think twice about email attachments.** Ransomware often enters a system via email when a user unknowingly opens an infected attachment. One way to reduce your organization's risk is to train employees to use Syncplicity to share links to files rather than opening documents directly from their email clients. The Syncplicity Outlook Add-In automatically transforms email attachments to links. Or users can simply paste a Syncplicity shared link into the body of an email message.

06 **Establish a recovery plan.** The restoration process after a ransomware attack can be time-consuming and costly, significantly impacting business. Attackers are counting on you to pay the ransom in order to get business moving again. So you'll need to protect the most critical component of your remediation strategy: recovery of the locked files. With Syncplicity retention policies and Multi-Folder Sync, users and administrators can restore files to prior unlocked versions and restore deleted files using the Syncplicity interface.

07 **Be vigilant over time.** Bad actors looking to take your files hostage do so because there's a huge payoff. Unfortunately, it will likely be some time before the current wave of ransomware attacks subsides. Stay vigilant. By following industry guidelines and smart ransomware prevention and recovery strategies over the long haul, you can avoid being the next victim in the headlines.

08 **Stay informed.** Knowledge is power. Fortunately, there's a lot of it out there, even as it pertains to ransomware prevention and recovery.

Here are links to a few resources that will help you learn more about protecting your organization's files:

- File Type Exclusion Policy
- Silently Mapping Syncplicity Folders
- Deleted File Retention Policy
- File Version Retention Policy
- File Version Recovery

syncplicity.com