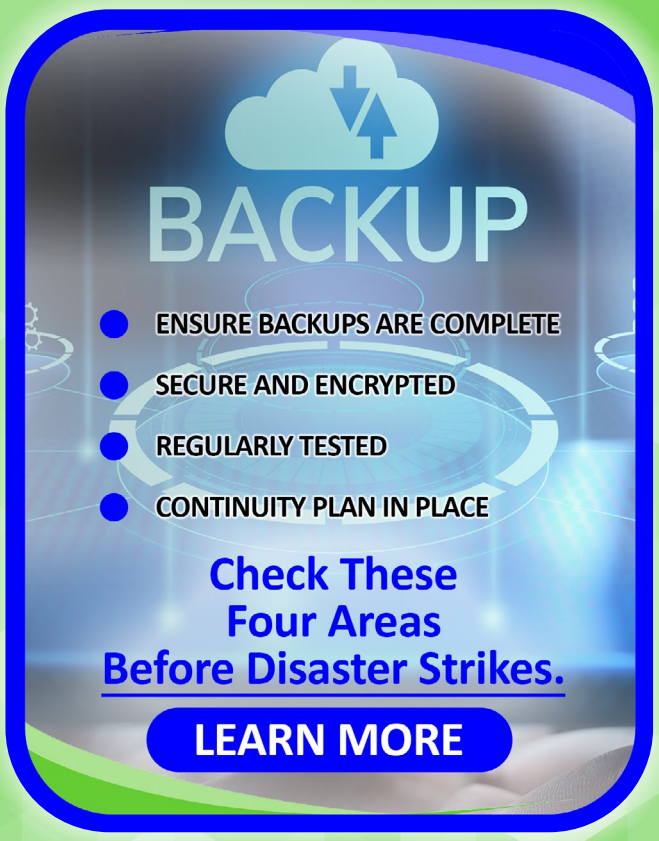
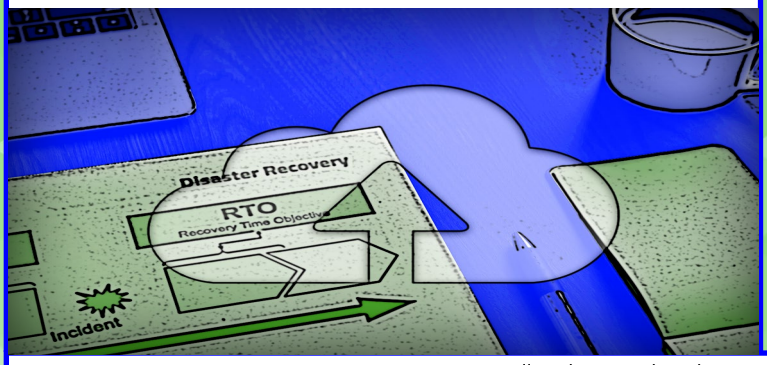
Secure Networkers®

IT NEWS BRIEF

August 2022



Backup Integrity and Malware-Free



Restoring Company Data After Any Crisis

The source of a cyber incident will be found in one of three areas:

- **Malicious activity committed by a network insider,**
- **An accident or misjudgment made by a network insider, or**
- **An attack by an outsider, who likely ferreted a way inside with the help of malware.**

All three of these security failures may lead to the loss of system files and cause corruption in system configurations. Database records may be destroyed. Application codes may be altered.

Smart businesses that plan for these kinds of attacks will have in place elaborate cyberattack prevention and incident response plans. They will make sure that their systems and data are backed up, and the backups will be scheduled at a frequency that supports their target window of recovery.

But what if the backed-up data has also been compromised? Testing the integrity of backups before restoration is the only way to ensure they are completely free of malware. So, how is that accomplished?

What If There is Malware and Mayhem in the Backup?

We have all seen the suspense thriller where the protagonist sweats over which wire to cut before the bomb goes off. A wire is chosen and cut, and the timer freezes. But just as the bomb is being dismantled, a secondary timer activates and the whole mechanism blows up anyway. Boom.

This metaphor fairly describes the experience of finding out the hard way that, recovering from a cyber attack and during the process of restoring all the data, the backed-up data also explodes in your face. Ransomware, in particular, can encrypt backed up files just like any other.

Assessing the integrity of that data, and cleaning it up before restoration, is critical. But this is easier said than done. The approach to it largely depends upon what kind of incident happened in the first place.

Let's look at three scenarios..

Cleaning Up after a Data Manipulation Attack

Data manipulation attacks are a problem that can happen well under the radar and for an indeterminate length of time if proper monitoring is not in place....

Continued...

A STRONG NETWORK

Let's connect and follow each other in business!
If you have a particular social network you use, please let us know so we can "**Like**", "**Follow**" and "**Connect**" with you. ***FIND US AT:***

EVENTS | BLOG

EMAIL QUESTIONS TO:
Service@Securenetworkers.com

CALL US:
(281) 651.2254

Backup plans can be flawed, and they can fail. When they fail, it can mean the loss of all company data. Todd Ellis addresses the importance of regular backup tests, and what works best.

Subscribe