CIO Security Insight :

Why your backup solution is crucial to defending your organization from ransomware

cbts

Consult Build Transform Support

The best defense against ransomware has two central components: learning how to diagnose and prepare for attacks and creating robust backup and recovery programs that can bring your critical data back online as soon as possible.

The prudent response to the ransomware threat is a holistic program combining cyber defense and backup/recovery planning. Alas, many IT organizations lack the skills, training, and experience to dovetail these disciplines into a comprehensive solution, leaving many enterprises vulnerable to cyberattack.

That's why so many organizations partner with a managed-backup provider to cover these vital operations. This eBook from CBTS, leaders in managed backup and recovery services, will help you understand why outsourcing is a savvy business decision. The appeal of outsourcing has four pillars:

- The ransomware threat persists and keeps evolving.
- Ransomware usually attacks onsite backups.
- Cloud backups are safer, but they also have vulnerabilities.
- The complexities of cyber defense and backup/recovery require substantial know-how.

This eBook will focus on the current reality that many organizations face today, as well as why backup is an essential component of recovery from a Ransomware incident.

Part 1: Ransomware is not going away

Ransomware exploded in 2017 thanks to the global wave of WannaCry exploits, but cybersecurity experts noted that the attacks started to wane in the second half of the year. "In 2016, the profitability of ransomware led to a crowded market," Symantec said in its *2018 Internet Security Threat Report*[1]. "In 2017, the market made a correction, lowering the average ransom to $522 and signaling the commoditization of ransomware."

Alas, the risks of ransomware endure—they've just shifted in new directions. Industry insiders says cybercriminals have started using ransomware as a decoy to distract defenders from more insidious intrusions. Moreover, ransomware techniques are rapidly evolving in ways that make cyber defense more complicated.

A report at *CIOOnline.com*[2] noted emerging changes in ransomware techniques, including:

- **New delivery media.** Cybercriminals have moved beyond email and started implanting malware in documents and image files.
- **Disk drive locking.** Instead of freezing individual files, the malware attacks the master boot record of a disk drive—making everything inaccessible at once.
- **Targeting older operating systems.** It's getting tougher to hack the latest versions of Windows and MacOS, so cybercriminals are going after earlier versions of system software.
- **Expanding the time frame.** Another tactic is to hide malware on a system and set it to attack months or years in advance.

[1] https://www.symantec.com/security-center/threat-report
[2] https://www.csoonline.com/article/3267544/ransomware/11-ways-ransomware-is-evolving.html

In March 2018, ransomware attackers cost the city Atlanta, Georgia, $2.6 million and disrupted a host of services to residents, *Wired*[3] magazine reported. The cybercriminals initially sought a ransom worth about $50,000 before shutting down their payment portal and forcing the city to clean up the mess.

These threats give organizations no choice but to create backup systems that can withstand ransomware attacks. The key is to ensure you have a backup program in place that you know, in fact, will recover your data. If you have not tested it, you are putting your business at risk.

Part 2: Attacks will target onsite backups

The nature of ransomware code is to seek out every device on a network, encrypt everything, and demand payment in exchange for a decryption key. Ransomware authors understand that backup systems undermine their efforts, so their code typically targets backup capabilities.

"Several ransomware programs—such as the recent WannaCry (WannaCrypt0r) and the newer version of CryptoLocker—delete the shadow volume copies created by Microsoft's Windows operating system. Shadow copies are a simple method that Microsoft Windows provides for easy restoration," cybersecurity expert Rod Mathews said in an article at *Dark Reading*[4], a news website that covers IT security.

Mathews noted that the structure of network file servers makes it easy to connect to users' PCs, centralize data, and streamline the backup process. All these benefits, however, create inherent vulnerabilities.

"Most ransomware programs encrypt connected drives, so the victim's home directory would be encrypted as well," Mathews said. "In addition, any server that runs a vulnerable and highly targeted operating system like Windows could be infected, which would lead to every user's data being encrypted."

When the ransomware threat started making headlines worldwide in 2016, observers wondered why targeted hospitals and other organizations lacked the backup resources to prevent major disruptions. While it makes perfect sense in theory to back up everything, in practice, large, sophisticated IT operations had to make tough decisions about where to allocate funding and invest in the necessary hardware to replicate their systems.

Organizations that scrimped on backup and recovery planning often found themselves in a serious pinch in a ransomware attack. Some may have created only partial backups that replicated their most mission-critical systems but opted not to restore systems fully, suffering a painful outage when ransomware struck.

The advent of cloud computing, which slashed the costs of mass storage, has reduced the pressure on companies to make those kinds of compromises. Indeed, off-site backup to the cloud can be a pillar of sound security policy that can help you recover your data in the event of a breach or ransomware attack.

Part 3: Even cloud-based backups are vulnerable

MIT Security Review[5] predicts the cloud will become an attractive target of ransomware perpetrators because of the massive volumes of data stored in the cloud. "The biggest cloud operators, like Google, Amazon, and IBM, have hired some of the brightest minds in digital security, so they won't be easy to crack," Martin Giles of the *Review* said. "But smaller companies are likely to be more vulnerable, and even a modest breach could lead to a big payday for the hackers involved."

[3] https://www.wired.com/story/atlanta-spent-26m-recover-from-ransomware-scare/
[4] https://www.darkreading.com/endpoint/ransomware-will-target-backups-4-ways-to-protect-your-data/a/d-id/1330029
[5] https://www.technologyreview.com/s/609641/six-cyber-threats-to-really-worry-about-in-2018/

Of course, cloud backups can be placed beyond the reach of ransomware. For instance, a dedicated offsite backup solution can copy files and data to a secondary cloud storage site where malware cannot find it.

Deploying a secondary offsite cloud backup service seems like a straightforward solution to the ransomware menace, but it may not be that simple. To prepare for and fend off ransomware attacks, organizations need a robust backup and recovery program that accounts for the needs of their business and their customers while protecting vital data and keeping key systems online.

Many organizations are choosing to partner with experienced managed backup providers to ensure their data is safe.

Part 4: Fighting ransomware requires specific expertise

Ransomware defense poses a twofold challenge—understanding the peculiarities of malware threats and building programs to recover encrypted files. Most organizations are short on time and resources, so addressing these challenges can be difficult. That underscores the appeal of partnering with an experienced managed backup expert.

For example, ransomware often encrypts files one by one, increasing the size of each file. Malware detection software can identify sudden bursts of file-size increases and flag them as possible cyberattacks. Human experts must monitor the detection software to decrease the odds of false alarms. Multiply this challenge by the dozens of malware variants infecting systems—with new ones arriving every day—and you start to see the scope of expertise required for ransomware defense.

The backup component is similarly complex. To work effectively in a ransomware attack, backup operations must be:

- Well designed to account for operational needs, budget resources, IT workloads, customer demands, supplier pipelines, and other critical business issues.
- Designed with security measures and employee training.
- Encrypting data on site, in transit, and at rest to ensure that even if the data is stolen they can't do anything with it.
- Strategically configured to ensure that organizations can fail-over to backups that can keep serving users and customers even while the primary system is under attack.
- Comprehensively tested to ensure backups restore as expected.
- Thoroughly documented so the absence of critical personnel doesn't disrupt the restoration.

The evolution of cloud computing, virtualization, and replication software enables organizations to create mirror systems that can deploy rapidly in a ransomware attack—if they have the talent, training, experience, and budget to make it all happen.

Many companies don't. That's why they choose to partner with an experienced IT solutions provider who can tackle each of these diverse technical challenges.

Partnering with CBTS for backups, recovery, and cyber defense

CBTS has decades of experience configuring and managing enterprise data centers. We also partner with top cloud and security providers to deliver the latest, most powerful technologies to our managed services and backup clients.

We take the time to learn your unique business challenges, and our people have the training, expertise, and certifications required to provide comprehensive protection against downtime and cyberattacks.

A few years ago, tape backups were sufficient for many organizations. These days, however, digital technologies connect every corner of a business, making downtime a much more severe threat you cannot afford to ignore. Meanwhile, cybercriminals keep dreaming up new ways to attack organizations' networks and critical data.

These trends oblige organizations to beef up their cyber defense and develop thorough backup and recovery programs that will be there in a crisis.

If you need help with your data protection and backup programs, talk to CBTS today.

Contact us today at cbts.com