# 4.3. Security Toolkit: Backups and Securing Backups

## What Everyone Needs to Know

A “backup” is, in general, one or more copies of important data stored on your devices or servers, including virtual servers or virtual machines, as well as by your cloud-based service providers (email, case management, documents, fundraising, etc.) and is used in potential data loss situations to restore the original information. Data loss can occur for several reasons, including hardware failures, human error, ransomware attacks, or theft. Protecting backups from corruption, deletion, and unauthorized access is a critical task for IT administrators since backups help us restore from all kinds of disasters.

Creating backups of essential data can ensure that attacks do not interrupt service. Backups can include:

- User data, such as individual user profiles and files.
- Organizational data, such as databases and configurations of your office’s case management systems or Windows login infrastructure.
- Full server images, which can make restoring from a cyberattack or system failure much less painful.

Backups are only as good as when and how they are created, so your organization should have a plan on how often to store backups and where to store them.

Most cloud-based services (e.g., email, documents, case management, donor management) backup your organizations data to help the service provider recover if their server or network environment is damaged or attacked.  It is worth investigating what each cloud provider backs-up, how long the back-up data is preserved, and how you may recover data that is damaged or lost by your users or through a cyber incident.  Your organization may decide that it wants to back-up some or all your cloud-based service data in addition to the backups provided by the

service vendor.  These backups might help programs meet their data retention policy requirements and protect against data that was lost or corrupted but not discovered until after the point at which the cloud service provider can recover the data itself.  These backups might also make it easier and faster to recover specific data or make it practical to turn off accounts for users who have left the organization but who created data that needs to be retained.

## What IT Needs to Know

Backups should be stored in a secure location, physically and logically separate from the original data. During ransomware attacks that involve encryption of your current data, backups are a primary target for attackers since the attackers want to prevent you from being able to recover your data without paying the ransom. There are multiple storage options, including external hard drives, tape drives, and cloud-based storage.

There are critical considerations when planning for and storing backups.  They include:

- How often should you perform backups? The timing of backups can greatly impact their usefulness. For instance, if you need to recover data but you only store backups once a day overnight, you could potentially lose a full day of work.
- What data is being backed-up?  How do you ensure that the right data is being backed-up over time?  Typically, organizations quickly evolve the systems they use and the locations of where the current data reside.  Documentation and auditing are important to ensuring the right data is being protected with your backup solution.
- Does your backup solution allow for you to recover your data on a file basis as well as a server or virtual machine basis?  It is very valuable to have a backup solution that allows both file-based and server-based recovery.
- How long will it take to restore your data? If you have a large amount of data, you may need local faster storage for faster recovery times. During a cyber incident, your organization may need to run one or more massive data restoration.  The speed of recovery system is a very important factor to restoring services.

- If your backup is stored in the cloud, is there an option to recover to a temporary cloud server environment?  How fast can that be done?
- How long will it take to restore your entire system if it is affected by an attack, a hardware failure, or a corruption? The extent of a breach will determine the time necessary to restore backups.
- What are the ongoing cost of the backup solutions (labor, hardware, subscriptions, cloud services, etc.)? Storage costs money, and so does IT staff time spent on maintaining backup systems.  How does your firm limit the growth of its data backup needs?
- How will you monitor backups to make sure they are working and backing up all the required data? Consider ways to do this automatically as part of your backup system.
- Is the backup data encrypted in case the backup is accessed in an unauthorized fashion?
- How will your firm secure access to your backup system or systems? You should ensure that backups are only accessible to authorized personnel, that the systems are protected with MFA, and that the data cannot be changed once it is backed up. This might mean limiting access to which human and service accounts have access to the backups, limiting the ability of those accounts to delete data before a certain date, and certainly working with the backup solution provider to explore further how to protect the data from cyber incidents.
- How often will you fire drill small, medium, and large recoveries?  Testing your recovery processes at least annually will typically reveal important information that your organization will want to act on promptly.
- Who is able to manage the recovery if your primary IT person(s) is not available?
- If your firm needs to maintain some period of time its compromised servers or systems for forensic analysis purposes, does your firm have a plan to recover to alternative hardware or cloud servers with sufficient capacity and performance?

Costs for implementing and maintaining a backup protocol can vary widely.  It is worth shopping around to find the right mix of features and cost. There is a significant investment of time to setup and do some initial testing of your backups. For smaller, simpler technology environments, this might be in the tens of hours. For larger, more complex environments it might be over 100 hours to implement and fully test.

## Solutions to Consider

- For backup of on-site servers, virtual machines and cloud backups of accounts, such as Microsoft 365 Email or SharePoint)
    - Datto: Website
    - Acronis: Website
    - Veeam: Website
- Microsoft Azure Site Recovery (Backups): Website
- Keepersecurity: Website

## Resources

- "Backup & Secure" (USGS)
- “Data Backup – What is it?” (Acronis)
- "Azure Backup service documentation" (Microsoft)

Last updated on December 15, 2023.

Print

Table of Contents

NEWS

**News & publications**

The news about recent activities for needed peoples.

More News

24 Mar 2023


Project Spotlight: UpToCode

Because everyone has a right to a safe home, Northeast Legal Aid (NLA) is...

Continue Reading

28 Feb 2023


Member Spotlight: Josh Lazar

We are heading south to Florida today to meet community member Josh Lazar, the...

Continue Reading

**Our Partners**

MAP | MICHIGAN ADVOCACY PROGRAM

LSC | America's Partner for Equal Justice

LEGAL SERVICES CORPORATION