CANADIAN CENTRE FOR CYBER SECURITY

Tips for backing up your information

June 2024 | ITSAP.40.002

Having a backup (a copy) of your organization's information is one step that you can take to improve your cyber security and your resiliency. If your networks, systems or information are compromised, a backup helps your organization minimize downtime and get back to business quickly.

Why you need backups

Unexpected incidents, like cyber attacks or natural disasters, can happen. Think of your backups like an insurance policy. If you experience an incident, your backups are critical for 2 reasons:

- **Availability:** Protecting the availability of systems and data is a key component of cyber security. Backups ensure that your employees, partners, and customers can continue to access the information they need, when they need it
- **Recovery:** Is the process of restoring your systems and information. In the event of an incident, you can:
  - use your backups to restore systems
  - get your organization up and running as quickly as possible
  - minimize the amount of information, time, and money that could be lost due to downtime

Types of backups

- **Full**: You may want to do a full backup periodically (weekly or monthly) and before any major system upgrades. A full backup is the most expensive and time-consuming option, depending on the amount of information being backed up and your storage requirements
- **Differential:** A differential backup only creates a copy of data that has changed since your last full backup
- **Incremental**: With incremental backups, you're only storing the data that has changed since your last full or differential backup. Each new backup is saved as an incremental volume. This means, if you need to restore data, you must process each increment, which can be time consuming

Your backup process should include deduplicating data so that you aren't storing excess or redundant data. By deduplicating, you can reduce the costs associated with backups and ensure that you are efficiently backing up and storing data.

When you need backups

There may be times when your organization will be glad it has backups, including some of these common scenarios.

Failure or outage

Systems and devices can fail or crash, causing downtime or outages that can impact your business processes and activities. Backups can ensure that your organization doesn't lose critical information as a result of a failure, a crash, or an unplanned outage.

Ransomware

Ransomware is a type of malicious software that locks you out of your systems, devices, and files until you pay the threat actor. By having offline backups, you will potentially mitigate the need to pay the ransom (sometimes paying won't guarantee you restored access anyway). While backups can help you restore your systems and information, keep in mind that they won't prevent a threat actor from selling or leaking any stolen data.

Denial of service attack

In a denial of service attack, a threat actor floods a target, such as a server, with traffic to crash systems and make websites and internal services unavailable. Threat actors use this attack to disrupt business activities and services or to create a distraction so they can steal data while you're trying to recover. With backups and a recovery plan, you can minimize downtime during recovery.

Natural disaster

Fire, floods, and earthquakes can happen. Most organizations have emergency plans to respond to these incidents, and backups should be a part of those plans. Natural disasters can cause damage to buildings and physical assets that may restrict your ability to access them. However, having backups stored in a secondary location (offsite or in the cloud) can help you resume your business activities.

Lost or stolen device

A lost or stolen device, such as a phone or laptop, can result in a complete loss of data that is not backed up. When your organization backs up its data, it allows you to recover quickly.

These events don't need to happen directly to your organization. For example, if your cloud or managed service provider is affected by a natural disaster or cyber incident, your organization may experience downtime that impacts your business function.

Cat. No. D97-1/40-002-2024E-PDF ISBN 978-0-660-70856-0

CANADIAN CENTRE FOR CYBER SECURITY

June 2024 | ITSAP.40.002

Where to store your backups

Having a robust backup process enhances the resiliency of your organization. Backups make it possible for you to recover from cyber threats efficiently. There are 3 options for storing backups:

- onsite (also referred to as on-premises)
- offsite
- on the cloud

These options all have pros and cons. Ultimately, you should choose the option that supports your organization's needs and security requirements. When making your decision, consider the criticality of the systems and data and how quickly you would need to restore them.

Onsite storage

With onsite storage, you store your backups within the physical space of your organization. Onsite storage is convenient and can be time-efficient. Backups are readily available should you need to initiate your recovery process.

However, if you are only storing backups onsite, you may still experience data loss. For example, if your entire facility is affected by a fire or flood. We recommend storing a copy in another location, offsite, to prevent data loss.

There are various types of storage devices you can use for onsite storage.

Removable storage media is convenient and relatively inexpensive. That said, this media and your data must be protected against damage, theft, and loss. The media should be removed from your device after the backup has occurred to safeguard it from any attacks on your network. Examples of removable storage media include:

- tapes
- CDs
- DVDs
- USB flash drives
- external hard drives

Network-attached storage (NAS) devices connect directly to your network and allow authorized users to access the stored data via your network versus a direct connection to the media itself. However, threat actors can attack NAS devices, or ransomware can spread to the NAS, and compromise your backups.

Regardless of the type of storage devices you use, you need to ensure you protect them and the data contained on them. The storage device should have security controls, such as:

- encryption
- malware scans
- proper sanitization and disposal

Offsite storage

Storing backups of critical data in a separate, offsite facility can help your organization prevent data loss. If you require more storage space, and you have the budget for it, offsite solutions may be a good choice for your organization.

If you plan to contract a vendor for offsite storage, make sure that they have the following:

- security measures, like data encryption
- incident management processes
- a disaster recovery plan

Cloud-based storage

Cloud-based storage can be beneficial in many ways. Having a service provider take care of your backups frees up resources for your organization. You can also benefit from the expertise of the cloud service provider. Many providers offer enhanced security features that you might not have in-house.

Note that your organization is always legally responsible for protecting its data. You should ensure that the service provider you select can support your security requirements with proper safeguards.

You should also consider data residency, which refers to the geographical location where your data is stored. Your organization may have regulatory and policy requirements that require data to be stored in Canada.

Cat. No. D97-1/40-002-2024E-PDF ISBN 978-0-660-70856-0

Tips for backing up your information

Online and offline backup storage

We recommend having a backup stored offline. Online backups are stored on a remote server or computer that is connected to your network. Unlike online backups, offline backups (sometimes called cold backups) remain unconnected to your organizations' systems and are only connected when they are required. Because these offline backups are not connected, they remain unaffected by many cyber threats, like ransomware, that can compromise all systems and devices on your network.

What else to consider

When backing up your systems and data, there are a few considerations to account for.

- Develop policies and procedures that address backups, such as:
  - identifying the frequency of how often backups are done (daily, weekly, monthly)
  - developing processes and policies that outline how your backups are implemented and managed
  - testing the process of recovering from your backup
  - outlining how your recovery process will be performed including roles and responsibilities
- Consider your organization's information management policy and requirements when managing your backups
- Identify and prioritize your business-critical data (data that you need to function to keep the lights on)
- Encrypt sensitive data to protect it
- Adopt the 3-2-1 rule for data storage and have 3 copies of your information (1 original and 2 backups), saved on 2 different media types, with 1 copy kept offsite
- Keep your backups separate from your computer by storing them on an external device onsite or in a cloud-based storage solution that uses a strong password or passphrase and multi factor authentication
- Know your solution providers' security measures and protocols, ask questions and make sure they can support your needs and requirements
- Test your backups to make sure they work

Learn more

Use the following guidance to grow your knowledge of backups and storage:

- Protecting your organization against denial of service attacks (ITSAP.80.100)
- Best practices for passphrases and passwords (ITSAP.30.032)
- Secure your accounts and devices with multi-factor authentication (ITSAP.30.030)
- Sanitization and disposal of electronic devices (ITSAP.40.006)
- Benefits and risks of adopting cloud-based services in your organization (ITSE.50.060)
- Ransomware: How to prevent and recover (ITSAP.00.099)
- Baseline cyber security controls for small and medium organizations
- Top measures to enhance cyber security for small and medium organizations (ITSAP.10.035)

Cat. No. D97-1/40-002-2024E-PDF ISBN 978-0-660-70856-0