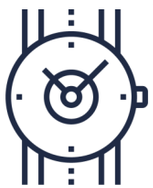
TIPS FOR BACKING UP YOUR INFORMATION

OCTOBER 2020 | 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 as a business. If your networks, systems, or information are compromised by a threat, such as a virus, or damaged due to a natural disaster, a backup helps your organization minimize downtime and get back to business quickly.

WHY DO I NEED BACKUPS?



You never hope for natural disasters and cyber attacks, but they can happen. Think of backups like insurance. If something does happen to your organization, your backups are critical for two reasons:

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

WHEN WILL I NEED MY BACKUPS?

There may be times when your organization will be glad it has backups, including some of these common example 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 backups, you don't 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 (e.g. a server) with traffic to crash systems and makes websites and internal services unavailable. Threat actors use this attack to disrupt business activities and services or create a distraction; while you're trying to recover, they may be stealing data. With backups and a recovery plan, you can minimize downtime during recovery.

NATURAL DISASTER

Fire, floods, and earthquakes can happen. Most businesses 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.

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 functions.

TYPES OF BACKUPS

Data can be backed up in different iterations:

- **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 increment is saved as an incremental volume. However, if you need to restore data, you must process each

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.

Communications Security Establishment | Centre de la sécurité des télécommunications

Canada

WHERE SHOULD I STORE MY BACKUPS?

Having a robust backup process enhances the resiliency of your business; backups make it possible for you to recover from cyber threats efficiently. There are three options for storing backups: **onsite** (also referred to as on-premises), **offsite**, or on the **cloud**. These options all have pros and cons. Ultimately, you should choose the option that supports your business 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. You should also have more than one copy of your backups and store these copies in two different locations to reduce the risk of data loss.

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 if your entire facility is affected by a fire or flood, for example. We recommend storing a copy in another location to prevent data loss.

Different storage devices include the following examples:

Removable storage media (e.g. tapes, CDs, DVDs, USB flash drives, and external hard drives) is convenient and relatively inexpensive. However, this media and your data must be protected against damage, theft, and loss.

Network-attached storage (NAS) devices connect directly to your network and enable users whose devices aren't connected directly to removable storage media to access the stored data. However, ransomware can attack NAS devices and affect your backups.

Regardless of the type of storage devices you use, you need to ensure you protect them, and the data contained on them, with other security controls, such as encryption, malware scans, and proper sanitization or 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 security measures, incident management processes, and a disaster recovery plan in place.

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 benefit from the expertise of the cloud service provider; many service provides 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.

ONLINE OR OFFLINE BACKUPS?

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 SHOULD I CONSIDER?

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

- Develop policies and procedures that address backups (e.g. frequency, process, testing, recovery).
- Consider your organizations' information management policy and requirements when managing your backups.
- Identify and prioritize your business critical data. What do you need to function and keep the lights on?
- Encrypt sensitive data to protect it.
- Keep your backups separate from your computer. Store them on an external device onsite or on a cloud-based storage solution.
- Have more than one copy of your backups and store these copies in two separate locations (e.g. one in the cloud and one on an external hard drive).
- 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!

WHERE CAN I LEARN MORE?

Visit the Cyber Centre website (**cyber.gc.ca**) to learn more about cyber security topics and find our entire collection of publications, including:

- *ITSE.50.060 Benefits and Risks of Adopting Cloud-Based Services in Your Organization*
- *ITSAP.00.099 Ransomware: How to Prevent and Recover*
- *Baseline Cyber Security Controls for Small and Medium Organizations*

Communications Security Establishment | Centre de la sécurité des télécommunications

Canada