GLOBAL CYBER ALLIANCE

globalcyberalliance.org
New York City | London | Brussels

GCA Cybersecurity Toolkit Backgrounder: Backup and Recover Toolbox

GCA Cybersecurity Toolkit For Small Business

Backing up data is critical from a business and personal perspective as more information is kept online. It is crucial for Business Continuity.
There are many reasons why access to your data may be lost. In this case we are considering loss or corruption of data due to a cyberattack, but backing up also facilitates recovery due to hard disc failure, equipment theft, human error, accidental damage, and flood, among others.

The heavy reliance on computers and the online world means the impact of data loss or downtime can seriously impact an organization's productivity and profitability. The loss of treasured photographs on a home computer, for example, will equally cause distress.

Consider the impact, from a financial and reputational perspective, if your business:

- Was unable to trade/use your IT systems for a day?
- Lost an important proposal that could win the next big contract?
- Was no longer able to access customer files or they were corrupted?
- Was told you could only get access to information if you paid a ransom?

Having backups is critical to being able to recover quickly and resume operations!

Ransomware:
Ransomware is a type of malware that blocks access to a system, device, or file until a ransom is paid - usually in cryptocurrency (i.e., bitcoin), which is less easy to trace than traditional transfers.
It has been gaining in popularity and has been behind a number of high-profile attacks.
Examples of ransomware attacks include:

- WannaCry: WannaCry took advantage of a vulnerability in the Windows Operating System in 2017 - NHS, Renault, and FedEx were affected.
- Petya (2016) and NotPetya (2017): Petya spread, hidden within a PDF attached to an email (i.e., a malicious CV sent to a HR department), and evolved into NotPetya which took advantage, in part, of the same flaw Wannacry did.
- At the start of 2020, TravelEx, a global currency exchange, fell victim to a ransomware attack taking it offline for over two weeks and causing chaos for millions of travelers.

While it may be tempting to pay the ransom, the recognized advice is NOT TO.

Protect Against Ransomware:

- **Ensure that all systems are up to date** – good cyber hygiene, patching, auto-updates, and real-time Anti-Virus software will help prevent becoming a victim of a ransomware attack.
- **Prevent phishing/spam messages** by enabling the appropriate filters and educating users to not click on links or open attachments from untrusted sources.
- **Regular and external backups** will help recovery should you find yourself a victim of a ransomware attack (or malware/other cause of data loss/corruption).

There are different ways to back up:

- **Offline backups** refer to data storage that is both local and offline, such as storage on an external hard drive, USB drive, memory card, or other device. These devices should be disconnected and stored separately from the device itself.
- **Online Backups** or cloud backups make copies of your important data and store them off-site on secure servers 'in the cloud.'

Consider the 'loss impact' of the data you hold; develop a backup policy that takes this into account. Encryption should be adopted to protect sensitive information.

- Implement a sensible approach (policy) to back up your data, having categorized the different types of data you hold.
- Consider the important and sensitive data - how regularly should that be backed up and how/where should it be stored?

Use the tools in the Backup and Recover Toolbox to configure backups across all systems. Use an external drive/device to perform offline backups.

https://gcatoolkit.org/smallbusiness/backup-and-recover/