THE NATIONAL CYBERSECURITY SOCIETY

HOW TO CREATE A BACKUP PLAN

Most of us want to store and protect our irreplaceable assets (business data) and media (photos, movies, music). What often stands in our way is the lack of understanding about how to do it; how often to conduct a back up; and how to recover data. These are all important questions in determining your business continuity strategy and preparing for ***when*** not ***if*** an incident occurs.

An inventory of your data should be conducted to identify all your files on network servers, desktop computers, laptop computers and wireless devices. Include in this inventory whether it is stored digitally or on paper. The inventory plan should also include data owner, type of file, date of origin, how it is stored and its sensitivity.

DID YOU KNOW?

- ✓ 50 percent of the nation's small businesses were victims of hacking in 2016, according to *The 2016 State of SMB Cybersecurity report*.
- ✓ Ransomware attacks target your data and prevents you or your customers from reaching your website or other critical data.
- ✓ Creating a backup plan and exercising recovery will reduce your risk of losing your data to a ransomware attack.
- ✓ The average 2017 cost to recover from a cyber incident was $880K.

STEP 1: CREATE A BACKUP STRATEGY

Try to think about your company's backup in three parts: 1) a local copy, 2) a local backup, and 3) an offsite backup. For further detail:

1. Local Copy. Users continue to rely on their local data as their primary access.
2. Local Backup. A local backup gives you immediate, instant access to whatever data you might need back, regardless of whether it's deleted, overwritten, or lost.
3. Offsite Backup. Businesses rely on offsite backup as an insurance policy against an event at their primary work location. A backup at a remote site could be in another state or county. These backup services typically copy all data after the end of the business day and many use tapes. However, today many businesses are using cloud-based providers who guarantee reliability and recovery. An example is Backblaze.

STEP 2: HOW TO BACKUP

Once you have completed an inventory and determined what needs to be backed up, the next step is to determine how to backup. As an example, employees can be instructed to keep a local (working) copy on their desktop and save their work

Still have questions, need help?
Contact us at our **"Ask-an-Expert"** service,
web@thencss.org or visit us at the link below.

JOIN THE NCSS

Become a member of **The National Cybersecurity Society** today and learn more about how to protect your business from a cyber attack.

Back Up Plan continued...

on a local server in the office at the end of the workday. This process ensures two copies are kept locally. Adding a backup service provider at an offsite location would provide protection from a local event – such as a fire or electrical outage that might impact the two local copies. The backup service provider will provide you options on how often to back up your critical files – daily, weekly or biweekly, depending on cost and other considerations. So backing up is just that – establish a policy and execute.

Back up Devices. An external USB-based hard disk drive is good method to store backups for a small business. These devices can be used either as storage for the local copy or for storage as the local backup (just make sure there are two copies). Just bear in mind that hard drives wear down and stop working, so don't rely exclusively on this one option.

Network Attached Storage. Unfortunately, USB-based drives tend to fall into the pile of more things to keep track of and more to have compromised by theft or loss. Another more stable option is to use a Network Attached Storage (NAS) system like those made by Synology, QNAP and other companies. NAS systems live on your network, providing pooled storage so everyone on the network can use. Software that resides on your computer or software on the NAS can be used to back up the computer to the NAS. Using a NAS system ensures that everyone stays backed up and in sync when they're connected to the network.

Many NAS devices and even some large desktop drives incorporate RAID storage. RAID ("Redundant Array of Inexpensive Disks") systems distribute data across multiple hard drives.

STEP 3: WHAT TO BACKUP

Completion of your company's data audit will identity all critical data that is essential to daily operations. Any data that's critical to keeping your business running should be backed up. Financial records, customer records, tax forms, sales records, websites files, software, and project plans are all examples of critical data to back up. During the data audit, your team should identity all sensitive data that needs to be maintained and backed up. This data will need to be encrypted whether it is stored locally or offsite. Access to these files should also be controlled through access control procedures – like identity authentication and verification (login in name, password, as well as two factor authentication).

Also bear in mind that a lot of data is stored in the cloud. Take email, for example. Many small businesses rely on Gmail and other services to handle email for them — that data is already on Google's servers (and in a cloud).

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service,
web@thencss.org or visit us at the link below.

Back Up Plan continued...

Remember that having your business data only in the cloud is a single point of failure. Five years is usually the maximum time required to keep data. The “Data Protection Act” requires personal data processed for any purpose “shall not be kept for longer than necessary for the purpose.” This act states the maximum period of retention is regarded as 5 years. For this reason, it is critical to capture the date of origin of the data when you complete the data audit so that data that is no longer needed can be removed.

STEP 4: WHEN TO BACKUP

The best time to backup is whenever data changes, so a continuous backup system is the best. Most backup systems work by backing up all of your data once, and then incrementally updating only what’s changed or new. Also think about whether you need a backup of your backup. Some businesses make a point to rotate their backups periodically to make sure that even if one backup fails, another can take its place. How much redundancy you want or need is dictated by how much time, money, and equipment you’re willing to invest. Your backup service provider can assist in determining your best strategy.

STEP 5: RECOVERY

The best time to recover your data is before an incident occurs. Schedule a day at least once a year, to test your recovery procedures. Keeping the data audit/inventory as well as the recovery plan on paper, in an offsite location is an industry best practice. Train your staff on how to use the plan and who will be in charge. The recovery plan should be a step-by-step outline of: 1) what systems to bring on line first; 2) what data files need to be restored and in what order: and 3) testing of the system and data files through each phase.

STEP 6: THINGS TO CONSIDER

Not all data is created equal. Consider creating data retention schedules that align to the various data elements you require to run your business. Do you need to retain all your email messages since the beginning of time? Did you know that if you were sued, any correspondence related to the lawsuit would be required to be turned over as evidence? If you don’t need it, get rid of it.

RESOURCES:

- Backing up for Small Business, September 2nd 2016: https://www.backblaze.com/blog/backing-up-for-small-business/

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service,
web@thencss.org or visit us at the link below.