FIVE STEPS TO BETTER DATA PROTECTION NOW

claritech

This eBook is written to provide you with simple and inexpensive steps you can perform today that will immediately improve the protection and security of your important data. Continue reading for our exclusive free offer near the end.

STEP 1 IDENTIFICATION

The first step in protecting your data is to detail your important applications and the locations of the associated data. Email is probably one of the most complicated and important applications for any business. There are many places where email is stored: Google and Microsoft typically keep email on their servers, but your configuration can vary widely. If you don't know where your email is stored, you can't properly back it up. Ask your provider, or Claritech can assist.

If you have a customer relationship management application, it likely holds the contact information and notes for many customers and prospects. Similar to email, the data for the CRM may reside on a database server, as a file on a standalone PC or it could be hosted by a third party as a cloud application.

The above process is repeated for all the other corporate applications to ensure all information is accounted for.

Take Action :

Identify your critical data and where it's stored

STEP 2 BACK THAT DATA UP

Once the important applications and data have been identified, everything should be backed up as soon as possible This is particularly critical if you can't remember or haven't backed up for a long time.

The type of backup and tools you can use depend on where and how the data is stored. Server backups should be handled by an expert. Whether you do it yourself, or rely on an expert, it is important that the owner of the data, usually you, is confident that the data is protected. If you're not sure, be sure to ask.

Here are some of the things to consider about your backups:

- All your data should be backed up regularly and checked. Never assume that backups are working.
- The decision to backup hosted data, such as Office 365 or G-Suite, may depend on how important the data is to you. Microsoft and Google only keep your deleted files for about 30 days, so that might not be sufficient to recover old files. There are always options to backup hosted data. If it's important, you'll want to look into it.
- User desktops are sometimes not part of a backup strategy. If that's the case, make sure the users are aware that their local data is not being backed up and that they are responsible for protecting their own (non-network) files.
- Email is a tricky application to backup. Make sure you have your email configuration and your backup reviewed by an expert to ensure your important emails are protected.
- To protect against things like ransomware, the best strategy is to have offline backups, that are physically disconnected from your computers and not accessible by malicious software. Offsite backups can protect against a total disaster where local backup media is destroyed, and can also help recover in extreme ransomware cases where even the local backups are encrypted.

Take Action :
Buy a 2 TB or 4 TB USB drive (~$100) and hook it up to the computer with the most data. Run Windows Backup or Time Machine if you're on a Mac. Repeat for every computer that stores critical data. Call Claritech if you need assistance.

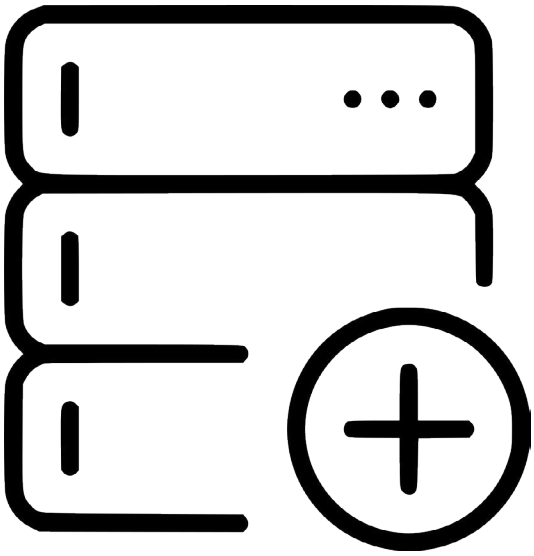
STEP 3 TEST YOUR BACKUPS

Good recovery plans involve testing a full recovery at least once each year. Ideally, all of the critical applications should be recovered to a test environment and functionality confirmed. The testing plan and results should be documented and kept secure in an off-site location to be relied upon in the event of a disaster.

If you're a small business with only one or two PCs, the recovery plan could include the above documentation of where data is stored as well as how all of the information is backed up. The testing plan could be as simple as performing a test restore of a key document or application, such as QuickBooks, to ensure the backups are performing as expected.

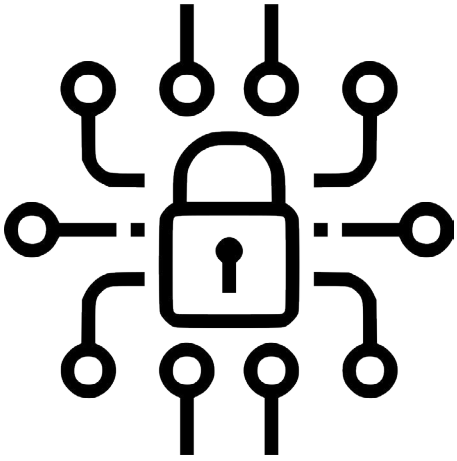
Larger businesses should have a more comprehensive disaster recovery plan that includes key stakeholders, including vendor and employee contact information that's kept in a secure off-site location that can be referred to in any disaster scenario. Checklists and recovery procedures for each of the applications identified above should to be included. The procedures should be tested in a test recovery scenario at least once per year.

Take Action
Pick one of the applications that you backed up above and try to restore it to a different location. Try to run the application and read the information. If you run into issues, resolve those, document the process and try again. Repeat until you are comfortable your backups are working correctly.



STEP 4 SHORE UP YOUR NETWORK

Network security should be part of every data protection strategy. Traditionally, the most common configuration is to stop all inbound network traffic to prevent hackers from accessing your information. Newer attack methods have challenged those assumptions. You should consider immediately blocking all outbound traffic except what is absolutely necessary to run your business. The only outbound traffic typically necessary is web and email traffic.



Tweaking firewall settings is a complicated and important role that should only be performed by qualified experts.

Take Action
Have a qualified expert reconfigure your firewall to block unnecessary outbound traffic.

STEP 5 TRAIN YOUR USERS

One of the biggest risks to the loss or theft of corporate information is company staff. Social engineering is a method of tricking users into installing software or going to a link that provides critical information, granting a hacker access to confidential information and potential access to internal systems. To effectively prevent social engineering attacks, the staff must be trained on the techniques hackers use and how to properly avoid them. Test phishing emails can provide an excellent insight into the level of security awareness of corporate users and is a simple and inexpensive addition to a security program.

Here are some of the tricks that hackers use to fool you into releasing private information or giving them access to your computer:

- Formatting a fake email that looks like it came from Microsoft containing a malicious attachment or link that they want you to install. This could allow them to take complete control of your computer.
- Send an email that appears to come from your bank asking you to click a link and login. This could provide them with your bank account login information.
- Sending you an email that appears to come from your boss or from the CEO. They usually request some sort of funds transfer to a bank account. These scams may even involve a two-way email conversation with the hacker confirming that the request is legitimate, urgent and confidential.
- Other fake emails usually take the form of something that looks concerning to you, such as iTunes, your credit card, a delivery attempt, etc, and compels you to take action right away. Often users who have been duped had a feeling that something was up but were compelled to click and proceed with the instructions anyhow.

The best protection against these types of attacks is to first know about them, and then to think before you click any links or attachments. If in doubt, check it out.

Take Action
Claritech provides training, phishing testing as well as suspicious email review for our clients.

We hope this eBook has helped you to understand some simple steps you can take right now to better protect your important information. If you would like help with any of the ideas introduced, you are invited to book a free 30 minute telephone consult with Dan at: claritech.ca/bookdan

Thank you for reading. If you haven't already subscribed, be sure to sign up at claritech.ca/protectme for our regular weekly tips.