next I.T.
technology solutions
that make business sense

Are You Prepared If Your Data Is Lost?

If disaster struck your hometown or a ransomware attack impacted your business, could you be up and running again within minutes?

- 200,000 – Number of hard drives that crash every week in the U.S.
- $50 Billion – Yearly virus damage to businesses in the U.S.
- 1 out of 5 – Small to medium-sized businesses that suffer a major disaster causing loss of critical data.
- 60% of companies that lose their data will shut down within six months of the disaster.
- 70% of companies have experienced or will experience data loss.

Primary causes are:

- 78% Hardware or system malfunction.
- 11% Human error.
- 7% Software corruption
- 2% Computer viruses
- 1% Natural disasters
- 1% other

- $18.2 Billion – Annual estimated data loss to businesses.

Downtime can lead to reputation impairment such as stock downturns, marketing man hours and media dollars required to reboot and polish up an organization's profile.

Downtime costs in this regard include:

- Lost business with customers (both short term and long term)
- Employee time diverted from other tasks to get IT systems running again
- Employee overtime expenses (if applicable)
- Emergency maintenance fees (particularly if the outage occurs during off hours)
- And additional repair costs

There are a Few Fundamental Steps You Can Take to Keep Your Data Safe:

Educate Your Staff on Social Engineering Attacks

Social engineering attacks trick people into giving up sensitive information usually by posing as someone within the company or a vendor. Educate your staff on what to look for and how to protect themselves and your company from these malicious attacks. Phishing is one of these social engineering attacks that disguise a virus within the email. Once the attachment opens, the virus goes to work attacking data and sending information back to the hacker. Phishing scams are already surfacing for the Meltdown and Spectre flaws, so make sure your team knows about these potential risks.

Backup Your Files

Keep copies of your data separate from your original files. Whether online in the cloud or offline at a separate site from the original, always backup your data. It is best to have it backed up on the cloud as well as offline in another location. This way, if hacked, or data gets lost, you will have a much better idea of what is missing and be able to get it back.

Use Up-to-Date Anti-Virus Software and Firewalls

Check for updates periodically and install them automatically. Cybercriminals will happily exploit any unsecured system for a one-time breach or even an ongoing theft. Now, with Meltdown and Spectre, it is even more crucial to keep your system updated.

Establish Company Policies for Handling and Storing Sensitive Data

Restrict who has access to your sensitive data and make sure they are changing their passwords every ninety days at least. Also, don't keep more data on a client than you need, and don't hold it any longer than you must. The less data you have on hand, the less you lose during a breach.

Establish Guidelines for Companywide Computer Use

Your employees should not be using company computers or devices for family or personal use. It prevents them from inadvertently sending out sensitive data. But it goes the other way too. Employees should not be allowed to use their devices to download business data. Include items such as thumb drives, tablets, and phones.

Institute a Mobile Device Policy

Set up a protocol so that employees may access data from a secure location on their phone, but without having to download that data. Enable access codes, encryption and remote wipe software on all company devices, then keep a log of all issued and approved devices.

Stay Up-to-Date on Software Patches

Make sure you are installing every hardware, software, and operating system update. It keeps hackers from being able to take advantage of vulnerabilities. Be sure that these updates take place across the board. Have every computer in your organization updated and make sure it gets done to avoid any breaches. The best thing you can do for hackers is not to update.

Use Passwords

Using passwords may seem obvious but can easily be overlooked. Use the built-in password functions of the laptops and other devices. Don't allow employees to store passwords on their work computers or devices. And make sure they are using a combination of letters, numbers, and symbols in their passwords to make strong passwords. You also want them to change it at least every three months.

Encrypt Sensitive Files

You want to keep out unsavory types and those meddling hackers, so encrypting your files is a must. This way, even if they get ahold of your data, they can't view it or alter it. Encrypting data that is being sent over the internet or to the cloud for storage is also a good idea. So even if the data or files get intercepted mid-stream, they are still unable to be read or changed.

Dispose of Old Files and Devices Properly

Simply deleting a file on your hard drive does not mean that it is gone forever. Deleting tells the hard drive that space is freed up and usable. The data can still be retrieved. The only way to ensure that hackers or anyone else can't get at the deleted files is to destroy the physical drive. When you upgrade equipment, such as computers, remember to destroy the old drives. But computers aren't the only drives that you should worry about. The copier has a hard drive as well. Think about what else in the office might have data on it and secure it.

Next I.T. can help alleviate the stress of lost revenue or customers by getting you back up and running with backup and disaster recovery solutions regardless of location, operating from a secure cloud.

Most disaster recovery solutions allow backups, but they don't allow you to operate from the cloud. You can only restore the backup image to your hardware but what if your hardware is destroyed, inoperable, or inaccessible?

Next I.T. makes your business virtually invulnerable to ransomware attacks and natural disasters. We store your backups remotely, so you're ready for the worst. Recover data, even virtualize your machines and re-create your network in a cloud purpose-built for disaster recovery.

Trust your company's security and survival to the experts at Next I.T.

Let's have a talk.

Contact us at 866.388.6398 or www.next-it.net.