Let's Talk About Information Security

In this age of data breaches, fraud, hackers, (and yes, maybe even competitors willing to steal your book of business), the term "information security" is being heard more and more. Indeed, with so many criminals out there ready to steal your information—if not your profits—businesses need to protect themselves.

But What Does Information Security Really Mean?

The definition of information security, sometimes called InfoSec, is "the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording, or destruction of information."

That being said, what exactly are the key concerns and accompanying processes and measures that will ensure your company's information security?

Key Concerns:

- **Data Privacy**

  Businesses and individuals have a right to expect data privacy. The collection and dissemination of data involves the public's expectation of privacy and the legal issues surrounding it.

  To be considered is the information shared when users visit websites—how that information is used, who that information is shared with, and if that information is used to track them.

  Another consideration is a business' right to privacy of their financial data and other confidential files, such as legal, medical, or other information. They need to protect their data from those with malicious intent.

What Does the Law Say About Data Privacy?

Data privacy is not highly legislated or regulated in the U.S. Access to private data contained in, for example, third-party credit reports may be sought when seeking employment or medical care, or when making credit purchases like automobiles or housing. Although partial regulations exist, there's no all-encompassing law regulating the acquisition, storage, or use of personal data in the U.S. But any existing regulations are difficult to enforce—all the more reason to take steps to protect your data.

- ### Data Storage

Data storage is of the utmost importance when it comes to information security. Choices include DVDs, compact disks, external hard drives, flash drives, in-house servers, magnetic tape backup, and web-based (cloud) backup.

DVDs, compact disks, external hard drives, and flash drives are easy to use for storage, but not the most secure. Electronic media doesn't last forever, and can be lost, damaged, or stolen.

In-house servers take up space and require much technical support. But they're very secure because they generally only connect to the computers that back up to them.

Magnetic tape backup is outdated and the amount of tapes you must buy to back up a business can be overwhelming, but it's secure because it's not hooked up to the Internet and not susceptible to cybercriminals. Like any electronic media though, they're vulnerable to fire, flood, and other physical damage.

Cloud-based backup services are now very popular and are some of the most secure and convenient methods of storage. Files can be sent over the Internet to a secure server for a monthly fee. But choose your cloud-based backup service carefully, as all are not highly secured. For very sensitive files, encrypted cloud storage is probably the most secure.

(Encryption is the process of converting data into code to prevent unauthorized access.)

We recommend varying your storage and having more than one storage device/service.

Information Security Management: What Do Businesses Need to Do?

According to McAfee (and other industry experts), the following tips will protect you, your computer(s), and your business:

1. **Invest in trusted, multi-faceted security software**—comprehensive, multi-faceted PC security software that protects you from viruses, spyware, adware, hackers, unwanted emails, phishing scams, and identity theft.
2. **Always access the Internet from behind a firewall**—it adds a security layer between your PC and the Internet, and helps stop hackers from stealing your identity, destroying files, or using your PC to attack others.
3. **Use a PC you know is secure**—hackers can easily retrieve sensitive data sent over unsecured Internet connections. When sending sensitive information or making online transactions, use a PC you know is secure and remember there are many flavors of security. Some computers have bare minimum; others have comprehensive security.
4. **Watch out for phishing scams**—fraudulent emails and websites, masquerading as legitimate businesses, which lure unsuspecting consumers into revealing private account or login information. Even with PC security, you might visit malicious websites unknowingly. Legitimate businesses never ask you to update your personal or business information via email. Verify Web addresses before submitting such information.
5. **Secure your wireless network**—if you access the Internet from a Wi-Fi network you're at risk. Wireless network's radio waves travel through walls, and hackers with antennas can attack you from miles away to steal your information and use your wireless network for their own communication. Use additional Wi-Fi security protection.

6. **Never install potentially unwanted programs (PUPs) like spyware or adware**—many seemingly harmless free programs are downloaded via the Internet, specifically designed to be malicious and monitor your keystrokes, track Internet logins, transmit confidential information, or redirect browsers to fake sites. Some can be installed on your machine by clicking on an Internet ad's link. Security software stops installment of these programs. Never install programs unless you're familiar with the website and program and have read the end-user license agreement.
7. **Monitor your business credit reports**—check your credit history once a year. This is a good way to find out if someone is using your finance information without your knowledge.
8. **Make regular backups of critical data**—keep a copy of important files.

For businesses, an outsourced IT provider such as Tech Solutions can ensure your information security with their experienced staff of expert technicians. Many companies find it difficult to find the time or expertise within their own staff to keep up with the demands of information security's constantly changing technology.

Tech Solutions can handle all your workstations, servers, network, and other devices. Our goal is to work hard to prevent problems from occurring, but when problems arise, our expert IT Support team provides a quick response.

Contact Tech Solutions at (888) 225-2672 or info@tsboston.com. Visit our website at www.tsboston.com.