Security is Everyone's Responsibility

Today's cyber security threats are real, and you don't have to look far to see the big headlines. What you rarely hear about are the small companies that are compromised. This creates a false sense of security for all of us. It's out of sight and out of mind. Unfortunately, small companies are faced with the exact same problems and threats as the big guys. Everyone is a target.

Attacks range from very simple approaches to ones that are highly-sophisticated, well-coordinated and well-timed. All in an effort to steal information, disrupt your business, or separate you from your hard earned dollars. Here are some of the sobering statistics*:

- **58% of cyber-attacks target small businesses with less than 250 employees.**
- **60% of those small businesses targeted are out of business in six months.**
- **Small business cyber breaches increased 424% last year.**

So what can you do?

1. **Validate the threats and risks to your company – get your head in the game.**
2. **Realize there's no easy fix – this requires a multilevel approach and everyone to pitch in (see guide).**
3. **Don't wait for tomorrow – get started on developing your plans today.**

Once you've decided to act and you have a plan, the biggest challenge you'll likely face is end user adoption and compliance — getting your employees to do what you ask. Generally speaking, employees perceive anything that can potentially slow them down in one of two ways. Either the change to workflow or process becomes an excuse why the job cannot can done the same way, or they'll find it as a reason to circumvent the process and technology you have worked hard to put in place. Neither is a good reason for allowing your company to be exposed. So be prepared for some pushback. A good way to tackle this is to explain why the changes are important for your organization and how you need their help. It also helps to include an acceptable use of technology policy, with employee signoff, in their HR folder as a great way to document the organization's expectations of them. Then there's training. We suggest the wash, rinse, and repeat method.

Developing a great cyber security strategy doesn't need to break the bank, but it is going to take some time and effort to implement and adopt. A great way to get started quickly is to realize there is a lot of help out there and you don't need to recreate the wheel. Ask other business leaders or partners of yours who you know and trust to share their plans with you. There are also lots of cyber security-focused firms out there to get you in good shape too, and the cost is generally a small fraction compared to the cost of a breach or ransomware event.

There is an old proverb that says, "the best time to plant a tree was twenty years ago, the second best time is today." Additionally, General Patton is quoted as saying, "a violently executed plan today is better than a well thought out plan two weeks from now". The moral of these two quotes? Don't put this off. Today is the day to start planting your trees.

*https://www.forbes.com/sites/ivywalker/2019/01/31/cybercriminals-have-your-business-their-crosshairs-and-your-employees-are-in-cahoots-with-them/?sh=5382dd1b1953

What end users can do:	Ideas and alternatives:
Be skeptical and vigilant	• A skeptical end user is your best defense • Think before you click • When in doubt ask • Don't hide the mess under the rug, tell someone
Stop emailing files	Utilize professional files sharing service, also known as Enterprise Data Management (EDM) systems.
Discontinue public WiFi	Use your phone mobile hot spot instead.
Use encrypted USB drives	They are inexpensive. Buy these and assign them to employees.
Change passwords often	Make this part of your normal process, for everyone. Every 90 days.
Use Password Keeper Apps	There are great tools available that are secure and simple to use.
What IT can do:	**Ideas and alternatives:**
Backup data & test periodically	Validate this independently, or at least get it in writing.
Disaster Recovery Plan	Doesn't need to be overwhelmingly complicated
Network Security Appliance	Use current equipment and technologies right-sized for your business.
Deploy updates & patches	Know who, what, how, and when for all devices (pc's, servers, network appliances, tables, mobile phones).
Use malware protection	Use paid products. The free versions are free for a reason.
Utilize email security protection	Same as malware protection. Look for something that protects you against viruses, phishing, URL redirects, file level scanning, quarantine.
Employ guest & private wireless networks	Make certain you have segmented wireless networks for guests and employees, and Splash pages for guests to accept your Internet use terms.
Pin protect mobile phones	This is simple for everyone in the organization to do.
Utilize strong passwords	Use a combination of upper and lower case letters, numbers, and symbols.
Secure Web Browsing	Keep your browsers up-to-date and protected.
Failed attempts lockout	Enact lockouts to systems after so many failed login attempts.
Two-factor authentication	If your application providers offer this feature, use it, it's a way to really tighten up your security.
Utilize SSL certificates	This is a small investment that goes a long way in providing in-flight encryption.
Dispose of old equipment properly	Find a partner who will ensure the proper disposal of old IT equipment, and will give certification of reclamation, EPA sign off — specially those printers of yours.
What Leadership can do:	**Ideas and alternatives:**
Cyber Liability Insurance	Purchase a policy for your organization and read the fine print.
Employee HR documentation	Incorporate IT policies into your normal process, items such as acceptable use of technology, acceptable internet use, mobile phone, breach notification.
End User Training	End users can be your greatest weakness and your greatest strength. Talk about these subjects and train, train, train.

Glossary of Common Cyber Threats

Adware
Hides on your device and serves up advertisements to you, or monitors your online behavior so it can target you with specific ads

Backdoor
Any method to get around normal security measures to gain access to systems & data, may be authorized or unauthorized access

Cyptojacking
Hides on your device and steals your system resources to mine online currencies such as Bitcoin

DDoS Attacks
Hackers maliciously overwhelm a website or service with requests or false web traffic from numerous devices

Emotet
A type of malware aimed at stealing financial data, originally a Trojan to exploit banks but it has now evolved to become a threat to all users

Hacking
Refers to activities conducted by individuals that seek to compromise digital devices such as computers, phones, tablets, networks, and servers for their own personal gain

Keylogger
A piece of malicious software installed on your device that secretly records your keystrokes, and may also be able to capture what you are viewing onscreen

Malvertising
Online ads that distribute malicious malware, little or no user interaction is required for installation

Malware
This is a general term for any type of software with malicious intent, most online threats constitute some form of malware

Phishing
A malicious attempt to trick you into sharing passwords, credit or bank information, or other sensitive information by posing any someone else or as a trusted institution

Ransomware
This is malware that locks the user out of their device and/or files, and then the perpetrator demands an anonymous online payment to restore access

Scam Call
What SPAM is to email, robo-calls are to your phone. Unwanted, annoying, & automated. Can be used to steal your information

Software Exploits
Cybercriminals take advantage of software vulnerabilities, hidden within the code of the OS or application, to gain illicit access to your systems

SPAM
Unwanted and unsolicited digital communication generally sent out in bulk by malicious senders

Spoofing
When someone pretends to be someone else to gain your confidence, access systems, steal information, steal money

Spyware
A form of malware that hides on your device, monitors your activity, and then steals sensitive information

SQL Injection
Used by malicious cyber criminals to exploit vulnerabilities in web applications to gain access to data

Trojan
Software that claims to do one function but actually does another nefariously; hidden in downloads, attachments, videos, or programs

Virus
A piece of code which is capable of copying itself and typically has a detrimental effect, such as corrupting the system or destroying data – often depends on a host application to replicate

Worm
A piece of code very similar to a virus, which is also capable of replicating itself for detrimental effect, but worms operate more of less independently of other files to spread