McCurdy Group
All your insurance needs under one roof.

January 2018

The best insurance is prevention!

212 Main Street, Sturbridge, MA 01566 Tel 508-347-9343 www.mccurdyinsurance.com

A Message from Dennis

Remember the old adage, you can't see the forest for the trees? Are you caught up "in the thick of thin things" (Neal A. Maxwell), meaning things of little substance or which are trivial?

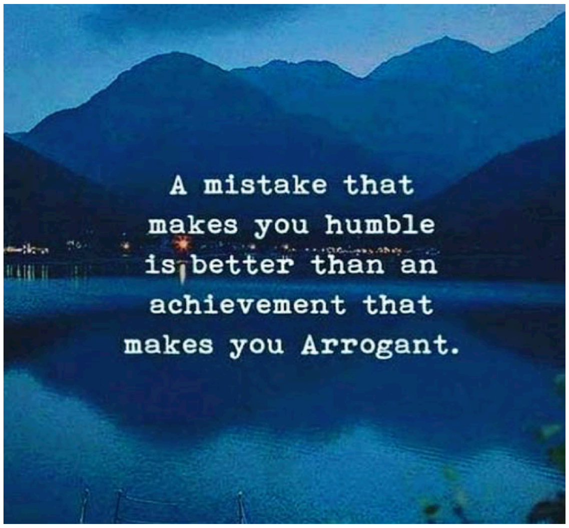
It's a new year, time for a fresh start, time to make a plan, and make a second plan, and an action plan.

How do you do this? Well, you need to step back, step outside your business for a few hours, a day, or whatever you need. Take time to THINK....

Remember another adage. Sometimes you need to "work on your business, not in your business." (Rhett Power)

And if you need help doing this, let me know....

Have a great 2018 ~ **Dennis**



The Threat of Weaponized Malware

Malware attacks pose a major threat. Cybercriminals use ransomware and malware to make money or steal identities. This new "weaponized malware" has no purpose other than to wreak havoc on an organization's data and functioning. One disturbing trend is cyber-attacks whose sole goal is creating destruction.

NotPetya was one of the first forms of weaponized malware that did not try to gain data or a ransom. And it will not be the last. Cybersecurity experts warn that more weaponized malware is coming, and it will be worse than ransomware.

Weaponized malware succeeds by stealing digital keys and certificates to gain administrative privileges. (See page 2 for types of malware and how it is spread.) Better certificate and encryption management strategies can help organizations prevent a successful attack. Monitor keys and certificates to keep them updated and secure.

What you can do:

- Train all employees on effective cybersecurity practices.
- Create unique, strong passwords for all accounts.
- Keep passwords secret and change them regularly. This may seem simplistic, but it is still one of the best ways to keep cybercriminals from accessing your network.

Because email-based malware continues to be a major risk, employees must understand that they *must never select and click* on a link or attachment in an email unless they are certain they know what it is and who it is from.

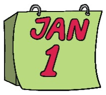
A Look At Malware by Type

Malware Type	How it spreads	Primary Purpose
Virus	Removable media (thumb-drive), download from Internet, e-mail attachments.	Various purposes for a virus. Viruses can interrupt service, delete files, capture valuable information.
Worm	Standalone malware computer program that replicates itself in order to spread to other computers.	The spread of a worm can consume bandwidth causing service interruption and possibly delete files, or send documents via email.
Trojan Horse	Spread through user interaction such as opening an email attachment or downloading and running a file.	Gives an attacker remote control over a computer. Attacker can do anything he/she wishes on the infected computer.
Spyware	Downloading and running a file from the Internet.	Software that will capture the interaction of the user on a specific computer. It can record websites visited and password entered plus other valuable information.
Adware	Downloading and running a file from the Internet.	Not harmful, but annoying. Displays unwanted advertisements to the user as you surf the web.
Bot	Bots oftentimes spread themselves across the internet by searching for vulnerable, unprotected computers.	Coordination and operation of an automated attack on networked computers, commonly used for denial-of-service attack.
Ransom-ware	Removable media (thumb-drive), download from internet, e-mail attachments.	Hijack important or critical files, encrypt those files and take them hostage. The attacker will ask for money before they un-encrypt the files and allow the owners to access those again.
Rootkit	Installed by an attacker, looking for vulnerable systems.	Take control of a system, give full access to an attacker to a system.

8 Ways to Lower Employee Driving Risks

Develop a fleet safety program. Create a written safety program and express expectations to all employees.

Hire qualified drivers. Conduct road tests, crosscheck references, call for medical evaluations and document standards.



Regularly check driving records. Make a set schedule to check employee driving records.

Train your drivers. Cover essential topics: speeding, distracted driving, breakdowns, driving under the influence.

Enforce policy for use of vehicles. Monitor who should be driving company vehicles, limit personal use.

Use the company fleet. Be aware of risks when employees use personal vehicles on the job.

Telematics - to monitor drivers. Control unsafe practices e.g., speeding, excessive braking, other aggressive behaviors.

Review every accident. Learn from the accidents how to help prevent future occurrences.

Justin's Insurance Fun Fact

The modern insurance industry developed primarily in England after the great London fire of 1666.

Like Us on Facebook

Did you know we have a Facebook page? Each week we post a blog entry that keeps you up-to-date on various insurance topics – with some surprises thrown in. LIKE us, and you'll be well connected! https://www.facebook.com/McCurdyInsurance