McCurdy Group
All your insurance needs under one roof.

May 2017

The best insurance is protection!

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

A Message from Dennis

In a recent article entitled "How to Mess Up a Business Without Breaking A Sweat," the marketing guru John Graham stated that to keep a business on track and growing, there's only one question that gets the wheels moving, that generates fire, not smoke. There's only one question that gets results: "Who's going to do what, why, and when?" Nothing else matters. It's nailed down. No loose ends. Some call it taking responsibility, while for others it's accountability. It's all the same; it's what it's all about.

Failing to educate customers is a good example of how businesses mess up. A recent American Consumer Satisfaction Index indicated that consumers view Facebook, Twitter, and LinkedIn "more negatively" than in past years. It set off alarms at Twitter. The company found 90% of people worldwide know the Twitter name, but only those who use it get what it's all about. That's a 40-point gap. In response, Twitter developed a campaign to educate people on how the platform works and the benefits of using it.

Have you educated your customers about what you do for them and how to use your services? Every company faces the same problem. Satisfied to drink their own Kool-Aid, they fail, often miserably, at telling their story consistently. And it always catches up with them.

~ Dennis

BOP It!
Not Just A Game Anymore

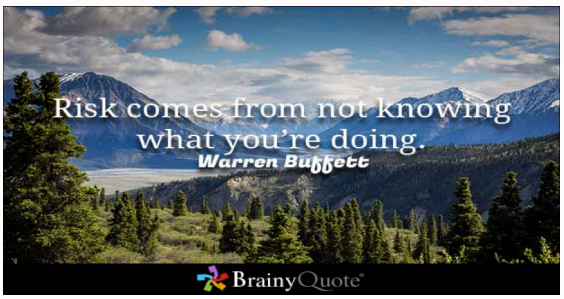
Maybe your kids (or you) have a Bop It toy, one of those audio games where you follow a series of commands telling you to pull handles, twist cranks, spin wheels, etc., with pace speeding up as play progresses.

But in the insurance world, a BOP can make the difference between solvency and total loss should a damaging event occur. All too often we hear stories like the one where floor installer tossed combustible rags in the trashcan on a hot day and the rags spontaneously combusted, burning down the house and four other homes in the neighborhood.

Or how about the delivery driver who lost control of the truck and took out a electrical pole causing business owners in the effected area to lose power thereby losing thousands of dollars in revenue, even product loss if the effected business is a grocery store or restaurant.

Having a BOP — a business owner's policy — usually includes property, casualty, liability, and business interruption coverage. By bundling these types of insurance together you're likely to pay less expensive premiums rather than buying the policies separately.

Unsure if you are fully protected? Give us a call. We'll talk with you about what exactly your business does (and doesn't do)as well as its future direction. This will enable us to assess the risks and suggest the types of coverage we think are best for your business.



Cyber Liability Insurance
By Justin Bellinger

In this high tech world we live in where every-thing is just an "app" away, consumers have become much more tech-savvy. Therefore, your business faces many more tech-related exposures.

If your business stores any customer data, accepts credit cards, sends customer information via email, has a website, or any social media platform, then you have potential liabilities that are not covered under a standard business owners insurance policy. Any data
breach could cost your business thousands of dollars — an out of pocket expense if you do not carry cyber-liability insurance.

Cyber insurance can make the difference between staying in business and closing the doors after a cyber-attack. Whether you have two hundred customer records or twenty thousand, your bottom line could be impacted by lost business, notification costs, legal defense expenses, and settlements.

Data breaches* affect businesses of all sizes:

- 55% of small business owners experience at least ONE data breach
- 72% are unable to fully restore their company's data
- 30% of cyber attacks target small businesses with 1-250 employees.

The general consensus is that most data breaches are caused by malicious attacks or hackers. But more than half of data breaches are a product of human error or system glitches. Examples may be:

- While on a business trip you lose your tablet, which has sensitive customer information stored on it.
- An employee mistakenly sends personal files to the incorrect email address.
- Credit cards used at your business were compromised via your point of sale system.

At McCurdy Insurance we understand cyber exposures and how to protect you and your company from the crippling costs associated with them. The McCurdy team works diligently to make sure your business insurance coverage doesn't have any gaps, including gaps related to data breaches. We will look at your exposures, assess your risks, and then get you the coverages you'll need to address the devastating impacts of various cyber-attacks.

Remember: Cyber insurance can't stop data breaches from occurring. But it can help you prepare and respond when a breach does occur!
(Source: *2014 Symantec Internet Security Threat Report ** Small Commercial Study by Ponemon Institute, Hartford Steam Boiler)

Justin Bellinger recently joined the team in March of 2017. Enthusiastic and eager are two words that best describe Justin. Whether it's answering the phone in reception or quoting a policy as Commercial Lines Account Manager, Justin is up for the job.

Goin' Phishing

In the April newsletter we explored password protection. This month, we draw your attention to another mode of cyber theft called phishing — collecting via email sensitive information, e.g., login credentials and credit-card information through a legitimate-looking (albeit fraudulent) website. Phishing messages, websites, and even phone calls are designed to steal your money.

There are several ways cybercriminals do this. One includes installing malicious software, aka malware, on your computer that harms your system in the form of worms, viruses, trojans, spyware, etc., and which steals protected data, deletes documents or adds software not approved by you. Or malware may be designed to steal personal information off of your computer, without your knowledge.

Social engineering is another cybercriminal tactic. The goal is to manipulate you into divulging, via downloads or links to another web site, confidential or personal information that may be used for fraudulent purposes.

How can you recognize phishing email messages and/or links? One way is to look for a mis-matched URL. While the URL in a phishing message will appear to be perfectly valid, if you hover your mouse over the top of the URL, you will see the actual hyperlinked address. If it is different from the address that is displayed, the message is probably fraudulent or malicious.

Another thing to look for is if the message contains poor spelling and grammar. Messages sent on behalf of a company are usually reviewed for spelling, grammar, and legality, among other things. So if a message is filled with poor grammar or spelling mistakes, it likely did not come from a corporation's legal department.

Next month we'll explore other cyber tactics, so stay tuned!