What's Your *Cyber Risk Exposure* Score? Take the Test to Find Out Instantly (see page 3)

Anthea & Douglas Present:

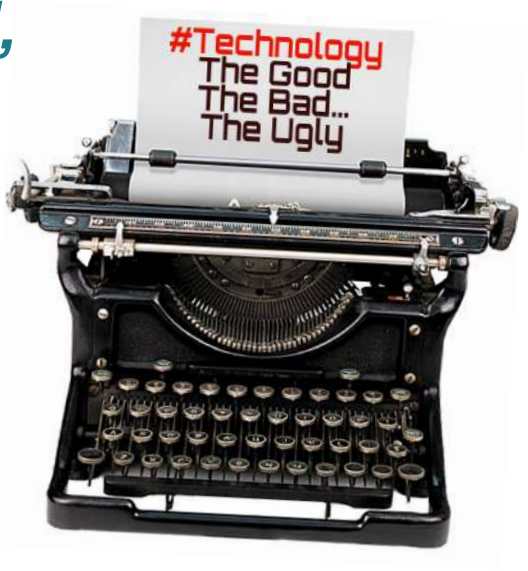
BUSINESS BY DESIGN

GREAT Rates * Award-Winning Service * For Design Professionals Only

From: Anthea Mumby, Monday 12:02pm, Mumby Insurance

April 2017 VIP Clients Edition

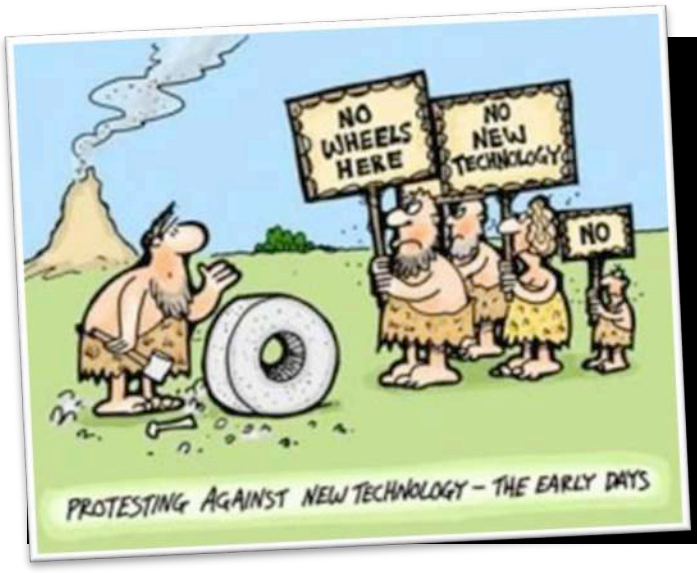
New Technology: The Good, the Bad, the Ugly



This year we are making a big push to take advantage of many new types of technology that will help serve our clients better while also helping our office run more efficiently. It's exciting to see the possibilities, but it's a little scary too. What will the learning curve be? What glitches will we face along the way? How quickly will we have to adapt as these technologies change and evolve?

Maybe you're in a similar spot with your business?

While technology has a lot to offer your business and ours, there certainly are downsides we have to look out for. One of the most prevalent has been the onslaught of ***cyber attacks*** *that have taken down big companies and small. That's why we are dedicating this newsletter to cyber protection – what should you be doing to utilize the best technologies for your business while protecting yourself from cyber attack and costly liabilities that come with it?* *(see p.2)*



What % of all computers are infected by a virus?

(Find out on page 4)

YOU SAID IT!

"We are very pleased! Douglas provides a professional and responsible liaison with his annual reviews. The hands-on is EXCELLENT, which is generally not experienced in the industry. As face-to-face is a part of our business, we appreciate it when we get it from you. The great rates are just an added bonus!" - Randy

How "Spear Phishing" Can Affect Your Business

"Phishing" is a type of cyber attack in which a hacker disguises himself as a trusted source online in order to acquire sensitive information. However, more resourceful criminals are resorting to a modified and more sophisticated technique called "spear phishing" in which they use personal information to pose as colleagues or other sources specific to individuals or businesses.

For businesses, the potential risk of spear phishing is monumental. The Internet Security Threat Report released in 2015 states that 5 out of every 6 large companies were targeted in spear phishing attacks in the previous 12 months!

How Exactly Does Spear Phishing Work?

Any personal information that is posted online can help a criminal seem more trustworthy during an attack. Once the apparent source gains the victim's trust, and there is information within the message that supports the message's validity, the hacker will usually make a reasonable request, such as following a URL link, supplying usernames and/or passwords, or opening an attachment.

Even if spear phishing perpetrators target just one of your employees, it can put your entire business at risk.

How to Protect Your Business

Though it is difficult to completely avoid the risk that spear phishing attacks pose, there are ways to prevent further damage to your business. Make sure that your employees are aware of these simple techniques:

- Never send financial or personal information electronically, even if you know the recipient well.
- Be cautious when you are asked to divulge personal information in an email. Even if it appears to be from a trusted source, it could be a hacker impersonating another person or group.
- Only share personal information on secure websites or over the phone. When in a Web browser, you can ensure a website is secure when you see a lock icon in the URL bar, or when an "s" (i.e. "secure") is present in the "https" of a URL.
- Some spear-phishing schemes use telephone numbers, so be sure to never share information over the phone unless you initiate the call to a trusted number.
- Never click on links or open attachments from unknown sources.
- Ensure that your company's security software is up to date. Firewalls and anti-virus software can help protect against spear phishing attacks.
- Encourage employees to think twice about what they post online. Spear phishing hackers often attain personal information through social media sites.
- Regularly check all online accounts and bank statements to ensure that no one has accessed them without authorization.

In addition, there are specific ***cyber liability insurance*** policies that will protect you from damages that result from a potential attack. This coverage is often quite inexpensive and is therefore very worthwhile investigating. **Call us today at 1-800-446-5745** to discuss what your cyber liability insurance could look like.

CYBER RISK EXPOSURE SCORECARD

You know that cyber risks exist each and every day, but just how vulnerable is your business?

INSTRUCTIONS: Begin by answering the questions below. Each response will be given a numerical value depending on the answer:

- **YES:** 5 points
- **UNSURE:** 5 points
- **NO:** 0 points

After completing all of the questions, total your score to determine your organization's level of cyber risk using the scale below.

EXPOSURE	YES	NO	UNSURE	SCORE
1. Does your organization have a wireless network, or do employees or customers access your internal systems from remote locations?	☐	☐	☐	
2. Does anyone in your organization take company-owned mobile devices (e.g., laptops, smartphones and USB drives) with them, either home or when travelling?	☐	☐	☐	
3. Does your organization use Cloud-based software or storage?	☐	☐	☐	
4. Does your organization have a "bring your own device" (BYOD) policy that allows employees to use personal devices for business use or on a company network?	☐	☐	☐	
5. Are any employees allowed access to administrative privileges on your network or computers?	☐	☐	☐	
6. Does your organization have critical operational systems connected to a public network?	☐	☐	☐	
7. Does anyone in your organization use computers to access bank accounts or initiate money transfers?	☐	☐	☐	
8. Does your organization store sensitive information (e.g., financial reports, trade secrets, intellectual property and product designs) that could potentially compromise your organization if stolen?	☐	☐	☐	
9. Does your organization digitally store the personally identifiable information (PII) of employees or customers? This can include government-issued ID numbers and financial information.	☐	☐	☐	
10. Is your organization part of a supply chain, or do you have supply chain partners?	☐	☐	☐	
11. Does your organization conduct business in foreign countries, either physically or online?	☐	☐	☐	
12. Has your organization ever failed to enforce policies around the acceptable use of computers, email, the Internet, etc.?	☐	☐	☐	
13. Can the general public access your organization's building without the use of an ID card?	☐	☐	☐	
14. Is network security training for employees optional at your organization?	☐	☐	☐	
15. Can employees use their computers or company-issued devices indefinitely without updating passwords?	☐	☐	☐	
16. Has your IT department ever failed to install antivirus software or perform regular vulnerability checks?	☐	☐	☐	
17. Can employees dispose of sensitive information in unsecured bins?	☐	☐	☐	
18. Would your organization lose critical information in the event of a system failure or other network disaster?	☐	☐	☐	
19. Can employees easily see what co-workers are doing on their computers?	☐	☐	☐	
20. Has your organization neglected to review its data security or cyber security policies and procedures within the last year?	☐	☐	☐	
TOTAL SCORE:				

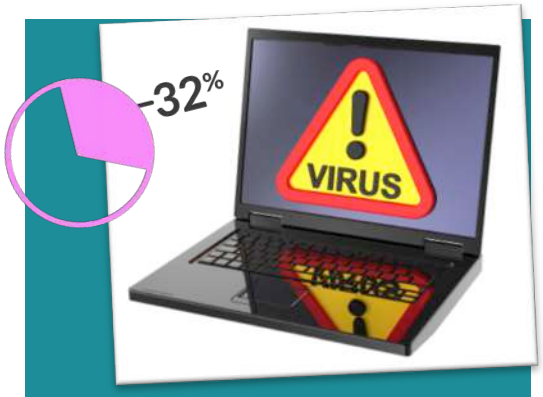
ESCALATED RISK: 55-100

MODERATE RISK: 15-25

HIGH RISK: 30-50

LOW RISK: 0-10

Did your firm score *Moderate* or higher on this scorecard? **Call us today at 1-800-446-5745** to find out if your current insurance will protect you from these cyber security risks.



Is Your Computer Infected?

Nearly 1 out of every 3 (32%) computers worldwide are currently infected with a virus or malware. This includes the machines in your office!

Most business owners don't fully understand their risks. Want help? **Call Us: 1-800-446-5745**

Do You Need a Social Media Policy?

A strong social media policy is crucial for any business that seeks to use social networking to promote its activities and communicate with its customers. At a minimum, a social media policy should clearly include the following 4 items:

1. Specific guidance on when to disclose company activities using social media and what kinds of details can be discussed in a public forum
2. Additional rules of behaviour for employees using personal social networking accounts to make clear what kinds of discussion topics or posts could cause risk for the company
3. Guidance on the acceptability of using a company email address to register for, or get notices from, social media sites
4. Guidance on selecting long, strong passwords for social networking accounts, since very few social media sites enforce strong authentication policies for users

How Are Your Employees Using the Internet?

You can't (and likely shouldn't try to) control everything your employees do online while they are at work. Your company Internet usage guidelines should allow employees the maximum degree of freedom they require to be productive. In fact, short breaks to surf the Web or perform personal tasks online have been shown to increase productivity.

At the same time, rules for behaviour are necessary to keep employees safe and to keep your company successful. Some guidelines to consider include the following:

- Personal breaks to surf the Web should be limited to a reasonable amount of time and to certain types of activities.
- If you track Web usage, employees should have clear knowledge of how and why their Web activities will be monitored, and what types of sites are deemed unacceptable by your policy.
- Workplace rules for behaviour should be clear, concise and easy to follow. Employees should feel comfortable performing both personal and professional tasks online without making judgment calls as to what may or may not be deemed appropriate.
- Businesses may want to include a splash warning upon network sign-on that advises employees about the company's Internet usage policy so that all employees are on notice.

CALL 519-885-5956 OR 1-800-446-5745 NOW!

Email Quotes: getaquotenow@mumby.com **Fax Quotes:** 519-747-2862 **Weekdays:** 8:30am-4:30pm
Mumby Insurance Brokers, 572 Weber Street N. Suite 2, Waterloo, ON, N2L 5C6

www.MUMBY.com