CAVIGNAC & ASSOCIATES
INSURANCE BROKERS

MAR 2019

Upgrading Your Cyber Security

Article courtesy of Professional Liability Agents Network

Ransomware. Social engineering attacks. Fileless, zero-footprint assaults. Security breaches. Fund transfer fraud. They sound like perils out of a James Bond novel that even the venerable 007 would have difficulty overcoming. But in truth, these are real life dangers facing all companies, large and small, including design firms. These dangers may fall under the umbrella of cyber liability.

At the core of cyber liability is unauthorized access to or control of company computer data with malicious intent, typically seeking financial gain. Whether that data is stored in a company network, an employee's laptop, an executive's cell phone, an Internet cloud, a misplaced flash drive or any other device, it is vulnerable to highly-trained hackers and cyber thieves, disgruntled current or former employees, unscrupulous competitors or business partners, or simply high school kids looking for kicks by "cracking the code" of your computer security system. (Know, too, that paper documents are equally vulnerable to malicious acts and are covered under well-written cyber insurance policies.)

Once your private data has been compromised, the perpetrator can have a field day wrecking havoc with your information. That includes sensitive data of customers, suppliers, employees and anyone else whose information is stored in your system or accessed through your networks.

Chances are, you will be liable for any damages or losses, financial or otherwise, suffered by others due to a data breach. You might also find yourself in violation of any non-disclosure or confidentiality agreements you've entered into. Various jurisdictions, including most states in the U.S., Canada and the EU., have passed laws that impose significant financial penalties on companies that fail to report data breaches to the victims. Check your applicable laws. And you'll suffer your own losses from lost work and stolen or destroyed financial or material resources.

The Liability Grows

The latest cyber crime garnering the headlines is ransomware. Here, hackers access and gain control of your computer or entire network, typically via malware installed on your system. When launched, this malware encrypts your data and denies you access to your information unless you agree to pay a sizable ransom, typically in the form of Bitcoin or some

other nearly impossible to track electronic fund transfer. Refuse to pay, and the hacker threatens to destroy all of your data or release sensitive information regarding your employees, clients, suppliers and other third parties.

Another growing form of cyber crime is what's called a social engineering attack, which requires human interaction. Here, a perpetrator convinces one of your employees, perhaps an accounting clerk, to send electronic funds to a legitimate looking business account. The request for a funds transfer appears to be coming from a company email account, perhaps that of your CFO, and the receiving bank account may appear to be that of a supplier or other business partner. Typically, it is only after the funds are withdrawn and transferred that the scam is unveiled. And because an employee willingly sent the funds, losses may not be as insurable as when a hacker breaks into your system.

Cyber liability stretches well beyond lost, stolen, kidnapped or otherwise destroyed data. If an employee posts false and damaging information about a customer, competitor, supplier or other third party on your website, blog, email or social media account, you can be held liable for slander. If your marketing department boasts on your Website about your superior, top-notch, can't-be-beat services, and then you don't deliver on that promise, you have upped your standard of care and opened yourself to an errors and omissions claim.

Clearly, the breadth and scope of cyber liability is growing. To fight it requires a two-pronged attack and the vigilance of your entire work force. You must 1) develop and implement cyber security policies and procedures and 2) obtain the appropriate insurance coverage to protect you in the event you are a victim of such crime.

Prevention the Best Medicine

Your best way to avoid cyber liabilities is to establish and enforce a cyber privacy and security policy. Along with your IT department and/or an outside security consultant, identify your vulnerabilities, develop a plan of attack to reduce them and then train your employees to carry out your strategies.

Start by identifying the categories of information you collect and store electronically. Apply a sensitivity rating to each category (employee files, customer files, project files, financial records, etc.), and map out how this information can be accessed, who currently is authorized to access it and what, if any,

security measures are in place to protect it from intruders. Pinpoint areas of vulnerability and identify potential methods to reduce those risks -- limiting employee access, installing firewalls, tracking payments and fund transfer activities, using data encryption, and so on.

Also, tighten your general computer-use, email and Internet policies. Install and regularly update antivirus software. Have employees update their passwords at least twice a year. Limit personal use of company equipment. Prohibit employees from loading personal software onto company computers.

Establish protocols for taking company-owned laptops, tablets, phones, etc., off premises, and set limits on the types of data that can be taken offsite on company or personal equipment. Instruct employees to avoid using unsecured public Wi-Fi networks or opening email attachments from unknown sources, which could be malware.

Limit who has authority to post on the company's Website and social media platforms. Have content regularly reviewed from a liability perspective.

Remember that data can be altered or destroyed accidentally as well. Back-up batteries and surge protectors should always be in use, and prohibit overloading outlets with multiple extension cords. Regularly back-up data, preferably to a secure, offsite location.

Despite your best efforts to protect your data and computer equipment, it only takes one innovative hacker or one disgruntled employee to cause wide-spread damage and substantial losses. That's why insurance is such a critical protective when it comes to cyber security.

Trends in Cyber Insurance

Great strides have been made in recent years to increase the protective power of cyber insurance. More and more insurers are developing cyber insurance policies that provide a broader range of coverages. As companies become more and more reliant on computer power and hackers and other perpetrators increasingly look for new methods to inflict damages through data destruction and theft, insurers have responded with evolving security services that provide protection beyond the policy limits of their policies.

For example, some insurers are now offering suites of robust risk management resources and services that strengthen your cyber security measures, both pre- and post-breach. These may take the form of Web-based risk management portals as well as companywide Webinars on specific cyber liability topics such as developing effective password protocols and techniques for recognizing and combating phishing emails. Insurers can also assist with assessments of your current vulnerability, including staging sophisticated hack attacks to test your defensive measures. And should you suffer losses, you'll likely receive assistance from your insurance company in tracking the infiltration, identifying the perpetrator and notifying those whose data has been compromised.

Risk Management Seminar Series

Performance Management for Supervisors

Wednesday, March 27th - DOWNTOWN

Thursday, March 28th - *NORTH COUNTY*

7:30am Registration

8:00am - 10:00am Program

Cal-OSHA Heat Illness Prevention for Indoor Workers

Wednesday, April 3rd - DOWNTOWN

Wednesday, April 10th - *NORTH COUNTY*

7:30am Registration

8:00am - 10:00am Program

Sexual Harassment Prevention Training

Wednesday, April 24th - DOWNTOWN

7:30am Registration

8:00am - 10:00am Program

To register, click on the 'register now' button in the announcement email, or contact Bethany Mongold at Mongold@cavignac.com or call 619-234-6848.

Specific coverages and policy language will vary by carrier. When reviewing policies, look for the following coverages:

Network and Data Security Breach

Covers damages to third parties due to compromised data, privacy leaks, transmission of computer viruses, “denial of service” for authorized users, and failure to notify third parties of a security breach (where required by law). Cyber policies can also cover paper documents as part of data security.

Loss of Income, Business Interruption and Extra Expense

This covers income lost and expenses incurred due to a disruption or shutdown of your computer operations caused by a hacker attack, viruses or other covered cyber perils.

Electronic Media Liability

Covers damages from personal injury, domain infringement, copyright violation, and similar claims due to information published on a company Website or via email or social media.

Security Breach Remediation and Notification Expense

Covered costs include forensic investigations and legal fees incurred to determine whose information was affected, notification of damaged parties, establishment of a call center for third party inquiries, and credit monitoring.

Computer Program and Electronic Data Restoration Expense

This coverage applies to expenses incurred to restore or recreate your data and equipment lost or damaged due to perils such as computer viruses, rogue employee theft, or hackers.

Funds Transfer Fraud

Policies cover your direct loss of funds, securities or other property due to someone gaining unauthorized access to your computer system and withdrawing funds.

Cyber Extortion

This covers costs incurred due to a credible ransomware or similar threat from a third party to destroy

your data or computer system, disclose third-party information, etc.

Regulatory Defense Expenses

This coverage applies to any fines imposed as a result of your company violating government rules regarding identity protection and security of third-party information.

Public Relations Expenses

Such coverage offsets costs you incur for PR services needed to mitigate negative publicity and reestablish the public’s trust following a cyber breach.

A Problem for Big and Small

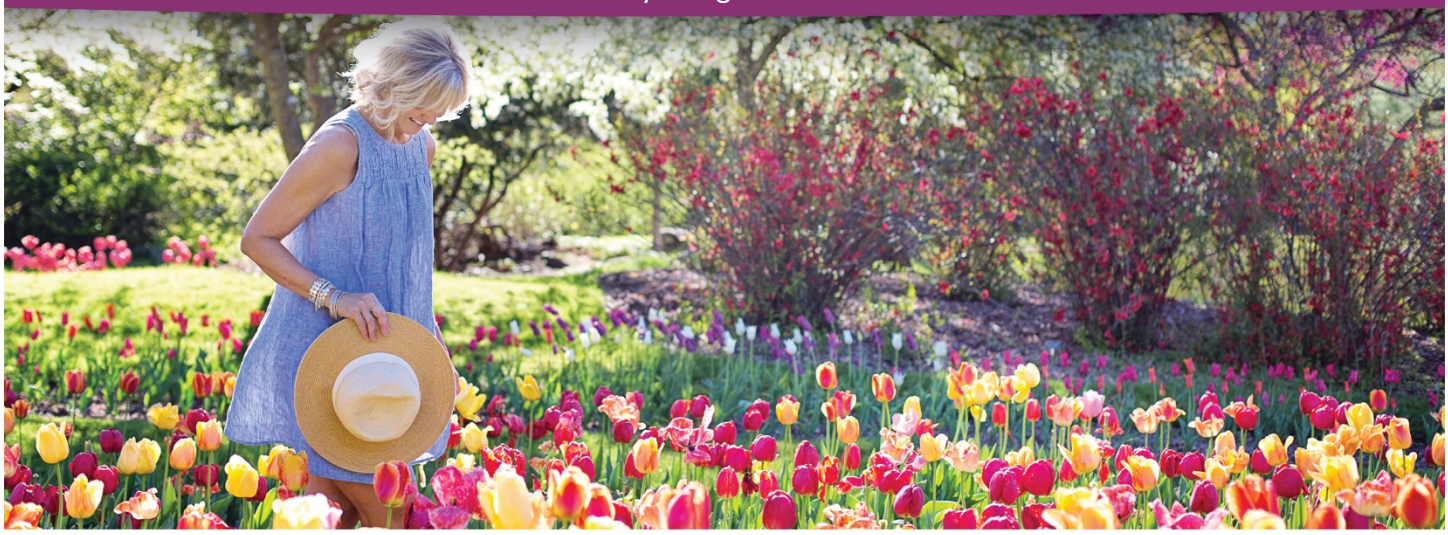
When it comes to cyber crimes, the headlines typically focus on large organizations, victims such as Target or Equifax. Yet it is estimated that half of all cyber attacks target small firms, with losses often exceeding $100,000 and sometimes reaching the millions of dollars. That’s because small companies typically lack sophisticated cyber security, owners are apt to pay ransoms and small firms often serve as vulnerable access points into larger companies.

Fortunately, cyber insurance is more available, affordable and robust than ever before. It may be available as a standalone policy or as an extension on a professional liability policy. You owe it to yourself to strengthen your cyber security and minimize your exposures to this very real 21st century liability. Contact your agent or broker for details.■

Live Well, Work Well

March 2019

Health and Wellness Tips for Your Work and Life
Provided by Cavignac & Associates



Don’t Let Spring Allergies Bring You Down

More than 50 million Americans suffer from allergies every year. In particular, springtime allergies are an annual nuisance for many people. As plants begin to bloom and neighbors start to cut their grass more frequently, allergy sufferers nationwide start sniffling and sneezing. What’s more, mold growth blooms both indoors and outdoors, making it almost impossible to escape allergy triggers.

Spring Allergy Alleviation Tips
To reduce your allergies, be sure to take the following steps:

- Wash your bedding every week in hot water to help keep pollen under control.
- Wash your hair before going to bed, since pollen can accumulate in your hair.
- Limit the number of throw rugs in your home to reduce dust and mold.
- Wear an inexpensive painter’s mask and gloves when cleaning, vacuuming or painting to limit skin exposure and dust and chemical inhalation.
- Vacuum twice a week.
- Make sure the rugs you have are washable.
- Change air conditioning and heating air filters often.

Treating Allergies
Treatment for most allergies is available both over-the-counter and by prescription. Talk to your doctor to find out what treatment method is right for you. If your allergy symptoms are severe or chronic, you may need a series of allergy shots. Contact your physician or allergist to determine which treatment option is best for you.

CAVIGNAC & ASSOCIATES
INSURANCE BROKERS

Veggie Chow Mein

6 ounces rice noodles
4 tsp. oil
1 onion (medium, finely chopped)
2 garlic cloves (finely chopped)
1 cup carrot (grated)
2 tsp. chicken bouillon
1 tsp. hot pepper sauce
1 cup broccoli (cut into small pieces)
1 cup celery (chopped)
1 cup bell pepper (finely chopped)
4 tsp. soy sauce

Preparations

1. Prepare noodles according to package directions. Drain and set aside.
2. Sauté onion and garlic with oil in a skillet for 1 minute over medium/high heat.
3. Add carrot, chicken bouillon and pepper sauce. Stir.
4. Add broccoli, celery and bell pepper and continue to stir.
5. Reduce heat to low, and add noodles and soy sauce. Mix well over low heat for 3 to 5 minutes.
6. Add salt and pepper to taste.

Makes: 6 servings

Nutritional Information (per serving)

Total Calories	163
Total Fat	4 g
Protein	2 g
Carbohydrates	30 g
Dietary Fiber	3 g
Saturated Fat	1 g
Sodium	399 mg
Total Sugars	3 g

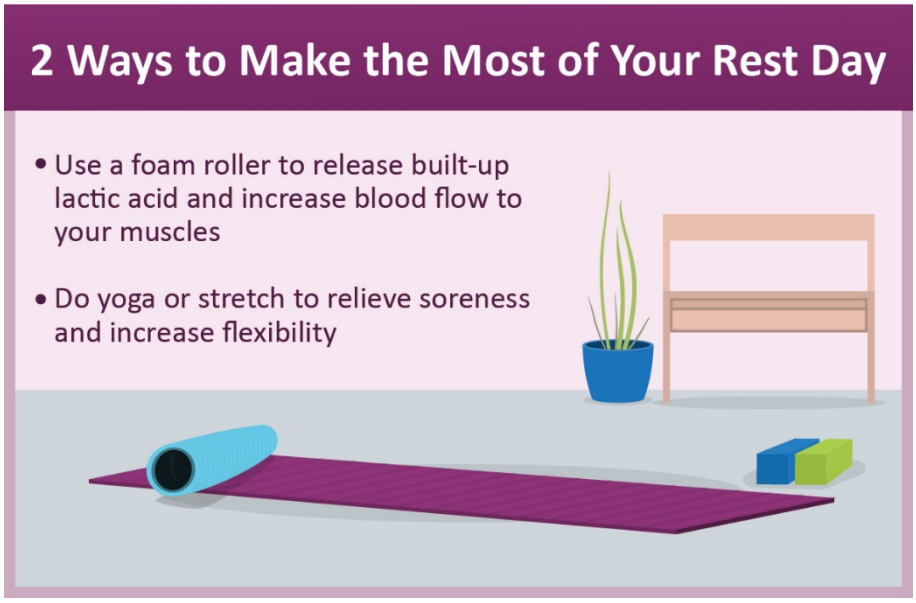
Source: USDA

Your Body May Need a Break, Here's Why

When it comes to exercising, there's a difference between pushing yourself to your limits and overexerting yourself. Oftentimes, this difference is very small, which is why it's so important to know when your body needs a break:

1. **You're always tired.** If you're constantly fatigued, even after getting enough sleep, chances you're working your body too hard.
2. **You're always sore.** A little bit of muscle soreness that occurs 24-48 hours after your workout isn't necessarily a bad thing—it means your workout was effective. However, extensive or prolonged soreness means you're overtraining your body.
3. **You're feeling stiff.** Doing the same exercises, particularly running on hard surfaces, can wreak havoc on your joints. This is especially true if you don't give yourself enough time to recover. That's why having a rest day is so important.

For more information, talk to your doctor.



Strengthen Your Financial Wellness Plan with These 3 Tips

Getting into the practice of saving will help you become more financially secure. Plan ahead so you have money waiting for you at retirement and can afford unexpected costs along the way. With the right preparation, you won't have to worry when life throws you a curveball.

1. Take advantage of an individual retirement account, 401(k) or other saving mechanisms.
2. Set money aside in accounts you can access prior to retirement.
3. Speak with a financial professional.

Source: IRS

Cavignac & Community

Cavignac & Associates is proud to support local and non-profit civic organizations, including the Light the Night fundraiser for the Leukemia and Lymphoma Society

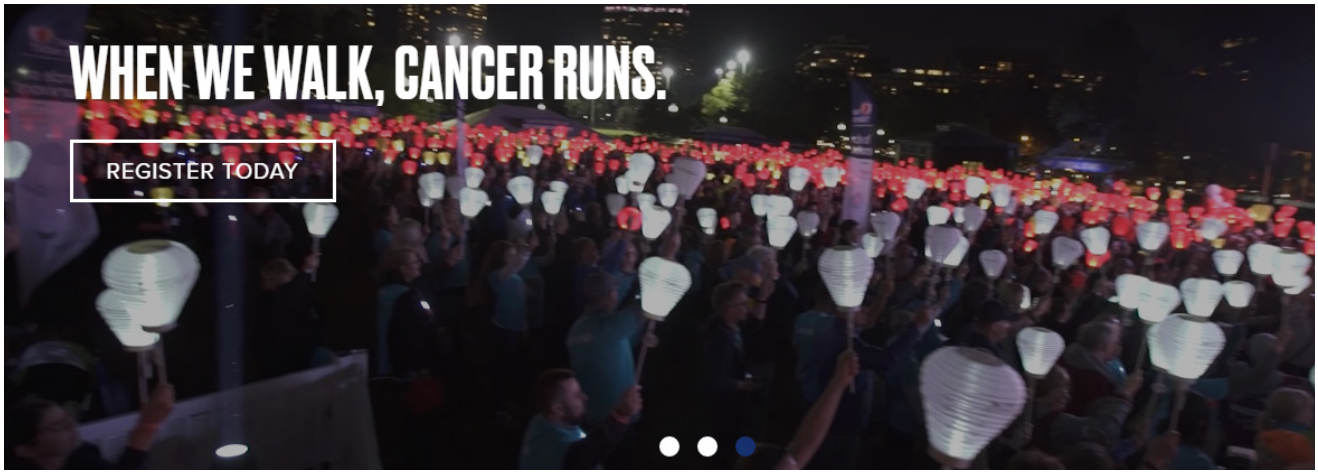
LEUKEMIA & LYMPHOMA SOCIETY®

LIGHT THE NIGHT®
bring light to the darkness of cancer

Light The Night raises funds in support of The Leukemia & Lymphoma Society.

The mission of LLS is to cure leukemia, lymphoma, Hodgkin's disease and myeloma, and improve the quality of life of patients and their families.

LLS exists to find cures and ensure access to treatments for blood cancer patients. We are the voice for all blood cancer patients and we work to ensure access to treatments for all blood cancer patients.



For more information, go to www.lightthenight.org