CAVIGNAC & ASSOCIATES
INSURANCE BROKERS

NOV 2019

Cyber and Other Risks of the Work-From-Home and Remote Employee

article courtesy of
Professional Liability Agents Network (PLAN)

Much has been written in the press lately about cyber security risks. The bulk of the attention has been focused on large multi-national organizations that have exposed millions of their customers and business partners to potential cyber crimes. These liabilities can be huge and large organizations are spending millions if not billions of dollars to strengthen their cyber security.

Small firms are far from being immune to this threat as well. In fact, one insurer's business owner survey found that over half of all businesses have been the victim of cyber crimes such as virus attacks, fund transfer fraud, phishing, and ransomware schemes.

Indeed, companies large and small are recognizing the cyber crime threat and arming their company computers and networks with antivirus software and other forms of protection. They are bringing in security experts to conduct tests to identify potential threats and then mitigate them.

Yet there is one area often overlooked when combating cyber crime at company offices. It's a backdoor into your computer network that is often left unguarded. We're talking about the vulnerabilities that exist when employees are working out of their home offices or from other remote locations and tapping into the company computer network.

More and more companies are allowing employees to work from home on a full-time or part-time basis. It's a growing trend and not one that will be going away anytime soon. The proliferation of wireless mobile devices and work-related software and applications will make sure of that.

There are a number of reasons for this growth in work-from-home employees. First, employees are demanding it. The current generation of 20-, 30- and 40-year olds see working from home as a highly desirable company perk for balancing their work and personal lives. Offering such set-ups often becomes mandatory to attract talented professionals. If you don't provide the ability to work from home to a top job candidate, chances are one of your competitors will.

There are advantages to the employer for offering the work-from-home option, too. Employers can attract a larger pool of job candidates from a larger geographic territory. Also, demands on company office space and, in turn, leases and rents are reduced. Employee productivity and loyalty have shown to increase while turnover lowers when employees can work remotely.

Not Safe At Home

Allowing employees to work from remote locations has its potential pitfalls, however, and the lack of cyber security is a big one. Employers would be wise to conduct a cyber security review of each work-from-home office to identify and eliminate exposures.

Have an IT professional visit each home office and examine the connection to the company's network. Is it adequately protected by robust ID/password combinations, and are these updated regularly? How much access does the remote employee have to company servers, clouds and other databases? Are these adequately protected by firewalls and other defenses? Can access to sensitive information be restricted to a need-to-know basis? Can activities be tracked and alarms sounded in the event of an attempted cyber breach? Are files backed up regularly to a secure location? Your goal is to make the home desktop, laptop, tablet, cell phone and other devices that have access to company servers and networks as secure as any computer in the home office.

It's a good idea to investigate the employee's internet service provider (ISP) as well. You'll likely want the ISP that serves your company headquarters to serve the remote home offices. If that's not feasible, make sure the ISP each employee uses offers the latest generation of security enhancements.

You'll also want to establish policies for the use of company computer equipment in the home office. It is almost impossible to stop employees from accessing company computers and internet connections at their home office for personal use, but you should set limits and guidelines as to what is allowable and what is strictly prohibited. For instance you should prohibit employees from visiting any websites that contain offensive content. Set guidelines for how to handle suspicious email attachments. And prohibit anyone other than the employee from using the company computer or network.

Educate all remote workers (indeed all employees) on cyber threats and how to address them. Discourage employees from using laptops or other devices attached to the company's network on public Wi-Fi connections at airports, hotels, coffee shops and other vulnerable places.

Enter Cyber Insurance

More and more insurers are developing cyber insurance policies that provide a broad range of coverages, most of which apply to remote office exposures. Specific coverages and policy language will vary by carrier. When reviewing policies, look for and discuss the value of the following coverages and how they apply to remote offices:

- Network and data security breach
- Loss of income
- Business interruption and extra expense

- Electronic media liability
- Security breach remediation and notification expense
- Computer program and electronic data restoration expense.

Beyond the insurance coverage, some innovative insurers now offer 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 and companywide Webinars on specific cyber liability topics. Insurers can also assist with assessments of your current vulnerabilities. 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.

Physical "Real World" Liabilities

In addition to having cyber liabilities, remote workers present real-world liabilities for material and financial losses as well as physical injuries. Consider these risks associated with remote work-from-home employees:

Safety issues. As an employer, you have an obligation to provide a safe working environment for your employees, including remote workers. It is recommended that the home office be restricted to a defined space, preferably one that is used solely for conducting company business. Once defined, the home office space should be examined by an ergonomic and safety consultant. Consider:

- Furnishings and equipment should be ergonomically designed to help prevent injuries, including repetitive motion and carpal tunnel injuries. The chair and its relation to the desk should provide both comfort and support.
- Lighting should be designed to provide ample illumination of the employee's work and to avoid eye

Risk Management Seminar Series

Human Resources Legal Update

Wednesday, Nov. 6 - DOWNTOWN
7:30am Registration
8:00am - 10:00am Program

Sexual Harassment Prevention Training WEBINAR

Wednesday, November 13 - Webinar
8:00am - 10:00am webinar

Sexual Harassment Prevention Training

Wednesday, December 4 - 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.

strain due to glare and shadows.

- Electrical, phone and computer wiring should be safe and secure. Make sure there are no trip-and-fall or fire hazards and that surge protectors and other electronic safety equipment is properly installed.
- Smoke, fire and carbon monoxide detectors should be installed in and around the home office and tested on a regular basis.
- Walkways and outdoor entrances should be kept clear and clean and the surface designed to prevent trips, slips and falls.
- Home workers should be trained in proper use of equipment and basic ergonomic principles. Such training should be documented and updated as necessary.

Security. In addition to having sound cyber security, home offices need to be physically secured as well. Consider these added measures:

- Install locks and alarms that enable the employee to secure the home office from the outside and the rest of the home.
- Establish rules, such as the use of locked and fireproof files and safes, to secure sensitive business property.
- Set procedures to have all electronic files backed up regularly at the main company office or a secure offsite location.

Insurance. Remote offices raise insurance concerns beyond cyber insurance for both the company and the work-from-home employee. It is crucial that the employee's personal homeowners coverage and the company's business policies be carefully melded to ensure there are no significant gaps that create uninsured liabilities for either party. Consider these insurance scenarios:

- Should a client, supplier, or other business associate become injured while at the home office, the employee's homeowners insurance will likely provide the primary coverage.
- Should the work-at-home employee become injured at the home office, the company's workers compensation policy likely covers the incident.
- If company equipment at the home office is damaged or stolen, the company's general liability policy may provide primary coverage for the loss. However, the equipment and its location would likely have to be identified on an endorsement to the company's property insurance schedule. Alternately, the company's policy form (BOP or PKG) may provide limited coverage for company equipment.
- If the employee's personal office equipment becomes damaged or is stolen, it would likely be covered by the employee's homeowners policy.
- If an employee is involved in an automobile accident with his or her personal car while traveling from the home office to the company headquarters or to a client or supplier, his or her personal auto policy likely provides primary coverage. If the company has a "non-owned vehicle" endorsement on its general liability policy, that may provide excess coverage.

Clearly, insurance issues can be quite tricky when it comes to work-at-home offices. When there is a mixture of employee and company property involved it becomes even more confusing.

Ask to see a copy of the employee's up-to-date homeowners policy. Sometimes, the employee has, in the company's mind, inadequate limits of coverage. If that's the case, who would pay for raising the coverage limits on the homeowners policy?

It is also advisable to alert the employee's homeowners insurer regarding the business activities taking place at the home office. It is best to clear up any coverage questions before a loss occurs.

Please contact us to discuss your remote worker situation and develop an insurance plan, including cyber insurance, that can provide you and your employee necessary coverages, security and peace of mind. ■

Live Well, Work Well

November 2019

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

It's That Time of the Year Again: Flu Season Is Here

The arrival of the fall and winter months signals many things, including the beginning of flu season. According to the Centers for Disease Control and Prevention (CDC), flu activity peaks between December and February.

Flu Symptoms
Seasonal influenza can cause serious complications for people of any age, but children and the elderly are more vulnerable. The flu is most often associated with the sudden onset of fever, headache, fatigue, muscle aches, congestion, cough and sore throat. Most people recover within a few days to less than two weeks. Occasionally, complications such as pneumonia, bronchitis or other infections can occur.

Flu Prevention
The flu vaccine is your best chance of preventing the illness. Currently, the CDC recommends that anyone over 6 months of age receive an annual flu vaccine. While there are many different types of flu viruses, the vaccine protects you against the viruses that experts believe will be most common that year.

In addition to getting your annual vaccine, here are some other tips to stay healthy this season:

- Avoid close contact with people who are sick, and stay away from others when you feel under the weather.
- Wash your hands often using soap and warm water to protect against germs.
- Get plenty of sleep, stay physically active and drink plenty of water to keep your immune system strong.
- Manage your stress and eat a nutritious diet rich in healthy grains, fruits, vegetables and fiber.

CAVIGNAC & ASSOCIATES
INSURANCE BROKERS

This article is intended for informational purposes only and is not intended to be exhaustive, nor should any discussion or opinions be construed as professional advice. Readers should contact a health professional for appropriate advice.

Autumn Vegetable Succotash

¼ cup olive oil
1 cup onion (diced)
2 garlic cloves (finely chopped)
2 cups red bell pepper (chopped)
2 cups zucchini (diced)
2 cups yellow summer squash (diced)
3 cups lima beans (frozen)
3 cups corn (frozen)
2 tsp. dried sage

Preparations

1. In a skillet over medium-high heat, add oil.
2. Add onion and cook until translucent.
3. Add garlic, bell peppers, zucchini, squash, lima beans and corn. Season as desired.
4. Cook, stirring, until vegetables are tender (about 10 minutes). Stir in sage and serve.

Makes: 8 servings

Nutritional Information (per serving)

Total Calories	203
Total Fat	8 g
Protein	7 g
Carbohydrates	30 g
Dietary Fiber	7 g
Saturated Fat	1 g
Sodium	43 mg
Total Sugars	6 g

Source: USDA

An Apple a Day May Help Keep the Doctor Away

You've heard the saying, but it turns out there's truth in the statement. Apples are rich in flavonoids, which can help you reduce your risk of disease, according to a recent study published in the Nature Communications journal.

Flavonoids are a diverse group of naturally occurring plant chemicals that pack a powerful punch of antioxidants and anti-inflammation properties. There are a wide variety of foods that are considered flavonoids, including strawberries, blueberries, green and black tea, onions, kale and celery.

The research found that those who consumed at least 500 milligrams (mg) of flavonoids per day had the lowest risk of developing cancer or heart disease. Additionally, the health-boosting effects of flavonoids appeared to be strongest for smokers and those who drank more than two alcoholic beverages per day.

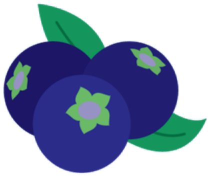
The study's authors note that flavonoid consumption shouldn't be used as a quick fix to remedy poor habits, but that when combined with living an overall healthy lifestyle, it could be useful for keeping disease at bay.

Get Your Fill of Flavonoids

It's easier than you might think to consume 500 mg of flavonoids.

Here are three simple ways to get your daily dose:

Drink 1 cup of green tea



Eat 100 g of blueberries

Eat 100 g of broccoli

This Popular Beverage Is Linked to Earlier Death

Yet another study has linked drinking soda to negative health effects. The European study, which researched the health of participants for an average of 16 years, found that drinking more than two sodas per day is linked to a risk of earlier death.

The researchers explained that the sugar in soda—regardless of whether the soda is diet or regular—can lead to obesity and can affect how your body uses insulin. Both of these conditions can shorten your life. In addition to this study's findings, soda consumption has also been linked to an increased risk for cancer and heart disease.

To protect your health, try opting for water as your beverage choice whenever possible. For more information about the health risks of soda, please consult your doctor.

Cavignac & Community

Cavignac & Associates is proud to support local and non-profit civic organizations, including I Love a Clean San Diego:

I Love a Clean San Diego

I Love A Clean San Diego leads and inspires our community to actively conserve and enhance the environment through example, outreach, and local involvement.

For more information, go to www.ilacsd.org