Social Distancing and the Risk Impacts on Employers' Cyber Security Position

While most of the world agrees that social distancing is the best risk management solution to fight against the spread of COVID-19, it does come with unintended consequences. In this article, we will discuss how companies are now at greater risk of becoming the victim of a cyber-related event and what steps they can take to protect their employees and other important assets.

The mandated quarantines across the world and specifically the United States have forced businesses to shutdown operations for an extended time period. Learning that Business Interruption insurance was not likely to cover their loss of income during this downtime, many companies hastily exercised Business Continuity Plan B, which is a Work From Home (WFH) policy for all employees. While this protects the company and their employees from the Coronavirus, it increases the chances of contracting a "virus" of another kind . . . the cyber kind. Cyber criminals are using this opportunity to prey on our vulnerabilities. Malware, phishing emails, scams, ransomware attacks are very much on the rise and will continue to spread as the weeks go on.

For continuity plans to be effective (specifically a plan that involves a greater number of employees to now work from home), they need to be carefully planned and the employees need to be properly trained. Most companies did not have the foresight, nor the resources to plan for such an event like the COVID-19 pandemic. As a result, these contingency plans are un-tested, and the employees are ill-prepared. Here are some of the issues at hand:

- Most small businesses do not have the internal personnel nor the necessary assets to execute a Work From Home plan.
- Company-issued laptops could still be vulnerable if their security software is not updated or their remote network connection is not perfectly configured.
- Employees using their own equipment that security teams cannot monitor for malicious traffic (these devices may already be infected with malware).
- Expansion of places hackers can exploit
- Hackers using the pandemic to prey on employee's fears
- Loss of personal interaction amongst co-workers leading to social engineering fraud

Businesses have focused most of their efforts thus far into continuing normal operations or close to normal; however, this has potentially come at the expense of good network security. Though it is impossible to turn back the hands of time before COVID-19 impacted our businesses, there are some steps companies and their employees can take NOW to ensure they are protected. They are as follows:

Employers

- Provide copy and require acknowledgement signature of the Information Security Policy and the Data Breach Incident Response Plan. *Both plans need to contemplate the loss of social interaction in an office environment and how you are going to mitigate that risk pre-breach and post-breach.*
- Require strong passwords and multi-factor authentication
- Implement a Virtual Private Network
- Use encrypted messaging for work communication

Employees

- Review (and UNDERSTAND!!!) the Information Security Policy and the Data Breach Incident Response Plan
- Ensure Wi-Fi is secure and Anti-virus is in place and updated
- Beware of suspicious email and avoid opening any unfamiliar links
- Verify the source of any COVID-19 news before accepting and circulating
- Never share personal or financial information over email or messaging
- Confirm any invoice or any wiring instruction is legitimate (remember you cannot walk down the hall anymore to verify and your bank may be unable to protect you in this current environment)

While most claims arising from COVID-19 are likely uncovered by insurance policies, cyber incidents arising from working from home and falling victim to COVID-19 scams are typically covered under a Cybersecurity policy. Like all insurance policies, careful consideration should be taken with the exclusionary language and the conditions of coverage to ensure adequate protection. Furthermore, not all cyber insurance policies are built the same. Coverages continue to evolve in response to the ways in which cyber criminals attack businesses – **large or small**. It takes the keen understanding of an expert to understand the unique risks of each business and to address those risks with the appropriate coverage language.

In closing, the adversity faced from the COVID-19 pandemic has taught us a lot about ourselves and the resiliency of our businesses. The best lessons learned in life are usually the ones that push us way outside our comfort zone and test our fortitude in every way (I like to call this The School of Hard Knocks). COVID-19 has put business contingency planning to the ultimate test and highlighted risk management, not insurance, as the primary solution. This pandemic will pass and those that are able to adapt and survive will be stronger and better prepared/protected as a result of it.

SOURCES:

- **Insurance Journal:** "Employers Beware: Working from Home Creates New Cyber Risks"
- **Insurance Journal:** "Watch Out for Virus-Tied Cyber Attacks on Remote Workers, Warns Tech Professor"
- **Chubb:** "Cloud Infrastructures Are Being Targeted"
- **CNBC:** "Phishing scams, spam spike as hackers use coronavirus to prey on remote workers, stressed IT systems"
- **ZDNet:** "Working From Home: Cyber Security Tips for Remote Workers"
- **ZDNet:** "With everyone working from home, VPN security is now paramount"
- **Business Insider:** "Working from home? Here are the steps all workers and companies should take to avoid cyberattacks, according to experts"

About the Author: Brian J. Courtney, RPLU, AAI

Brian Courtney has been with The Safegard Group since 2005 and has 20 years experience in the insurance industry. Throughout his years in the insurance industry, Brian has gained considerable experience in several different industries, including the Healthcare, Professional Service, and Manufacturing industries. Brian has become Safegard's expert on cyber liability exposures over the past few years with the rise of cyber security's effects on businesses and individuals.