Cybercrime in the COVID-19 World

By: Tom Owens, Professional Liability Agents Network

The following material is provided for informational purposes only. Before taking any action that could have legal or other important consequences, speak with qualified legal and insurance professionals who can provide guidance that considers your own unique circumstances, including applicable employment laws.

It is often in the darkest hours that we discover the best in people. The ongoing Coronavirus (COVID-19) pandemic is a prime example.The courage, compassion and persistence shown by medical staff, caregivers, first responders and others who put themselves in the line of fire is nothing short of heroic. Individuals willing to sacrifice their and their loved ones' personal safety to help others are true angels in our midst.

Unfortunately, such dark times also bring out the worst in a small minority of individuals seeking to prey (not pray) on others. They take advantage of the fears, uncertainties and compromised states of mind to try to gain monetary wealth through trickery, threats, deceptions, falsehoods and outright crimes. Among these "bad actors" are cybercriminals who lurk in the dark recesses of the Internet and take advantage of companies large and small who are trying to navigate the treacherous and unfamiliar Coronavirus/COVID-19 world.

Vulnerability Grows

The human and financial turmoil caused by the Coronavirus pandemic is unprecedented.

Businesses grapple to find a new normal to cling to, as the global community seeks signs of a slowing of the deadly virus and a return to some degree of stability. Companies, including design firms, have had the economic rug pulled out from under their feet. They desperately try to find their footing. Governments worldwide, at all levels, are understandably putting human health and safety first by issuing shelter-in-place and social-distancing orders that can effectively shut down all companies but those deemed to be providing "essential" services. That has led to countless design and construction projects being ground to a halt. Tragically, this idleness has resulted in mass layoffs, furloughs and unemployment numbers not seen since the great depression.

Due to this economic and employment turmoil, companies are increasingly vulnerable to cybercrimes.

When income dries up due to work stoppages,

businesses are pressured to reduce expenses. Support staff, including IT professionals, are often the primary target for cost cutting. Those IT professionals who remain on staff are often overworked or thrown into new roles in a sink-or-swim manner with very little guidance or formal training.

Compound this problem with an unprecedented increase in work-at-home employees. Shelter-in-place and social-distancing dictates may force employees to work from home on a full-time basis. As a result, servers and other hardware, software and additional critical components of the company's computer network (once fairly secure behind tightly maintained company firewalls) are all of a sudden being pieced together with company and employee equipment by a short-handed and inadequately trained IT staff.

In such an environment, company practices and procedures regarding Internet use and security protocols become shortchanged and incompletely thought through. Vital knowledge and information regarding the security of internal and external networks have been lost with the layoffs and furloughs. And, third-party consultants you try to hire to bolster your network security efforts may not be available for weeks if not months.

Meanwhile, your clients, vendors and other third parties are experiencing similar problems. This can leave vulnerable backdoors into your network for cybercriminals masquerading as your long-trusted business partners to enter and cause havoc.

Cybercrime had been on the rise well before the COVID-19 pandemic began. Phishing excursions, malware-ridden emails and ransomware attacks have all been on the increase despite heightened security efforts.

Far too many firms have fallen for elaborate schemes where criminals impersonate vendors, customers or members of company management in an attempt to convince someone to wire company funds to a new external account.

With the COVID-19 crisis, cybercriminals are now adding new weapons to their arsenals. For instance, malicious Websites and emails offering advice on how to survive the pandemic are being used to snare and infect networks of those companies visiting the rouge sites. Similarly, phishing emails made to look like they come from the World Health Organization and other government and charitable bodies ask for donations and try to get access to your electronic funds.

What To Do

The COVID-19 world presents significant challenges for all businesses. large and small. Here are some general guidelines to keep in mind when planning your cyber security.

Keep cyber security in the forefront. The current economic turmoil is putting a lot of pressure on businesses to reduce expenses. When making those difficult cost-cutting decisions, consider cyber security a primary usiness objective. Key IT staff (or, alternately, specialist outside consultants) are essential to maintaining a secure operation, particularly if you are dealing with an increase in work-at-home employees

Think long and hard before significantly reducing your IT staff.

***Be wary of the Cyber Con*.** Businesses are seeing a rise in cases of their employees parting with funds due to fraudulent instructions. Commonly known as phishing or social engineering, the cybercriminal impersonates a fellow employee, vendor or customer, and tricks the recipient into sending money where it shouldn't go. Any wire transfers should be verified verbally and any mailing instructions that differ from current addresses should also be confirmed. Coverage for this exposure can be included on a Cyber Insurance policy but can also be provided on a crime policy.

Secure at-home offices. Moving staff into remote home offices can create numerous inroads for cybercriminals to invade your network. This is especially true when a decentralization of company staff isn't part of a long-term strategic plan but is forced upon businesses via an emergency situation calling for shelter-in-place and social-distancing dictates. Each employee's home office will require a security review designed to identify and eliminate cyber exposures. You'll need to inventory all employee home office hardware and software as well as mobile devices in use.

Preferably, you'll want employees to use only company-owned equipment. If you do allow employees to use their own equipment and software, you'll need to make sure they are up to date and protected with state-of-the-art antivirus software and the appropriate level of encryption.

You'll also need to examine how each home office is connected to the company network (including a review of the Internet service provider), which parts of the company network (servers, clouds andother databases) remote employees can access, and what access can be blocked or restricted through firewalls and other defenses. You'll also want to be able to track all traffic and receive alerts when there is suspicious activity that may signal a cyber breach.

Importantly, you must simultaneously ensure employees are not overly restricted from successfully conducting their work by an excess of security measures. Otherwise, they will look for workarounds that will defeat your network protection. Finding the "right" level of security is the challenge.

Secure unused or underused office space and equipment. In the rush to comply with shelter-in-place directives, many main offices have become scattered with office equipment no longer in use. It is crucial to secure these servers, desktops, and other hardware and, when possible, disconnect them from the company network. Strive to eliminate any risk that an intruder may enter your premises and gain physical access to your network.

Beef up employee protocols. Employees must conduct themselves properly while using the company's equipment, software and networks. You'd be surprised how lax employees can be when it comes to creating strong passwords and changing them on a regular basis. Strong, frequently changed passwords combined with multi-factor authentication are widely considered .

your best first line of defense against hackers.

You'll also need strict rules regarding what types of Internet activities, business or personal, employees are allowed to conduct in their home offices. Limits should be put on the use of public Wi-Fi in coffee shops, hotels and other public places as well. In addition, you'll need secure back-up procedures to help prevent data from being maliciously stolen or kidnapped via ransomware.

Institute security training. To avoid security breaches, employees will need clear direction and consistent guidance in the form of best practice procedure manuals and training. Company guidelines must spell out employees' role in maintaining cyber security, identify functions and activities they can and cannot perform on the company network, and teach them to identify potential attacks to the system through phishing campaigns, malware, viruses, ransomware and the ever-growing list of cybercrimes.

All security training must be actively backed and attended by top management in order to demonstrate the high priority given to this effort. Third parties such as key vendors and clients may also need training on how to correctly navigate and use parts of your company network while applying appropriate security procedures.

The Added Protection of Cyber Insurance

Cyber insurance has become more prevalent over the past decade. The backbone of any good cyber insurance policy is a robust list of perils covered. While cyber insurance policies are becoming rather standard between carriers, they can have important differences. When reviewing policies, look for these coverages:

- **Network and Data Security Coverage**. Cyber

insurance can cover damages to third parties due to issues such as compromised data, privacy leaks, transmission of computer viruses, "denial of service" interruptions, and failure to notify third parties of a security breach (where required by law).

- **Loss of Income, Business Interruption and Extra Expense Coverage.** Cyber insurance can cover your lost income and incurred expenses due to a disruption or shutdown of your computer operations caused by a hacker attack, viruses and other covered perils.

- **Electronic Media Liability Coverage**. Cyber insurance can cover damages from personal injury, copyright violation, and similar perils due to information published on a company Website or via email or social media.

- **Security Breach Remediation and Notification Expense Coverage.** Coverages can include the costs of forensic investigations and legal fees incurred determining the extent of a breach, notifying damaged parties, establishing a call center for third party inquiries, and monitoring credit.

- **Computer Program and Electronic Data Restoration Expense Coverage.** Cyber insurance can cover expenses incurred to restore or recreate your data as well as lost or damaged equipment due to perils such as

computer viruses, rogue employee theft, or hacker attacks.

- **Funds Transfer Fraud Coverage**. Some cyber policies cover your direct loss of funds, securities or other property due to an intruder gaining unauthorized access to your computer system and withdrawing funds. This coverage can also be provided under your crime policy.

- **Cyber Extortion Coverage.** Cyber insurance can also be extended to cover costs incurred due to a credible ransomware attack or similar threat from a third party to destroy your data or computer system, disclose third-party information, etc.

While coverage of cyber perils is the backbone of cyber insurance, it is in the area of added security services where carriers can differentiate themselves from the competition. Consider:

- 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 often take the form of Web-based risk management portals.

- Insurers also sponsor in-depth Webinars on topics such as developing effective password protocols and teaching employees to recognize and combat phishing emails and other cyber-attacks.

- Insurers can also assist with assessments of your current vulnerability, including staging sophisticated hack attacks to test your defensive measures.

- Should you suffer losses, you can receive assistance from your insurance company in tracking the infiltration, identifying the perpetrator and notifying those whose data has been compromised.

Some general liability and commercial insurance packages will may include a base level of cyber coverages. However, to obtain a full range of coverages and security services, you will likely need to secure a stand-alone cyber insurance policy.

The New Normal

Shelter in place, social distancing and other dictates may ease in the near future, but few expect things to return to the previous "normal" for an extended period of time -- if ever. Even if conditions improve over the coming months, new waves of infections may rise in the fall and winter seasons.

Design firms need to determine how a new normal will impact the way they conduct business and how that new reality impacts cyber security. We suggest you apply the recommendations presented here, keep abreast of new developments in cyber security and seek guidance from security and insurance advisors to provide the necessary levels of protection.

We may be able to help you by providing referrals to consultants, and by providing guidance relative to insurance issues, and even to certain preventives, including the development and application of sound human resources management policies and procedures. Please call on us for assistance. We’re here to help.

