Freeborn

Your Future Is Our Purpose

Five Cyber Issues Companies Should Consider in the Midst of COVID-19

by Robert A. Stines

A FREEBORN & PETERS LLP CLIENT ALERT

ABOUT THIS CLIENT ALERT

Security researchers say they are witnessing nation-state hackers in China, as well as Eastern European cybercriminals, exploit the COVID-19 panic through cyber-attacks. This Client Alert details five cyber issues companies should consider as a result of COVID-19.

According to the *Financial Times*, cyber criminals and hacking groups are exploiting disruption caused by COVID-19 through a range of phishing and malware attacks. *The New York Times* reported that a series of fake websites for the World Health Organization and the CDC have started to appear. Security researchers say they are witnessing nation-state hackers in China, as well as Eastern European cybercriminals, exploit the COVID-19 panic through cyber-attacks. At a recent panel discussion on Managing Risk at the Intersection of Cybersecurity, Data Privacy and Business presented by the American Bar Association, there was discussion about the high likelihood of an increase in cyber-attacks such as ransomware.

These are valid concerns. To maintain productivity while working remotely, companies are relying on the internet and mobile applications. In other words, companies are working in a digital space. While many predicted that most companies would eventually move to a digital space, the pandemic has accelerated the process. This presents a prime opportunity for cyber criminals to prey on the unprepared and unsuspecting work force.

Under the circumstances, companies need to protect their IT systems and digital platforms. Here are five cyber issues companies should consider as a result of COVID-19.

1. Cyber Security and Hygiene

Medical experts are encouraging everyone to employ simple hygiene protocols to slow the spread of COVID-19. Cyber hygiene is also important to avoid a cyber event. Everyone should carefully review random emails requiring some sort of action, such as clicking a suspicious link or transferring large amounts of funds. If there is a link in an email, hover over the link to view the web address. Instead of clicking it, manually enter the web address to avoid clicking a malicious link. If you click on a link in an email and it asks for username and password, do not, under any circumstance, enter that information. If possible, avoid using public WIFI (such as coffee shops) for company business. Multifactor authentication is another layer that companies should implement to deter hackers from accessing digital platforms.

2. Confidential Information

Companies should treat confidential information just as they would in the office. Take precautions with the information being printed at home. Try to maintain shredding protocols for paper documents, or simply avoid printing. Personal emails are just that–personal and not for business use.

When sending confidential information through email, try to send it encrypted. Avoid using the free version of cloud storage for confidential or private information. The paid version usually includes increased security measures.

3. Personal Devices Are Risky
With the advent of Bring Your Own Device (BYOD), the division between company and personal becomes murky. As a Litigation Powerhouse®, we know that clients have difficulty preserving electronically stored information on personal devices. With this in mind, avoid having confidential or sensitive discussions over unsecure third-party instant messaging platforms. Best practice is to use company email (hopefully encrypted) or business-level instant messaging software such as Microsoft Teams. Employees should make an effort to save company-related emails in the appropriate digital folders. Additionally, the software on personal devices are sometimes out-of-date. Encourage employees to install all patches and security updates on their personal devices.

4. Is There a Plan?
What happens if there is a data breach or a ransomware event? Companies should review data breach and incident response plans to ensure they are prepared for a cyber event. If the company does not have a plan, hire a professional to assist with creating one. With an existing plan, it may have assumed everyone was in the office to react to a cyber event. Now that everyone is outside the office, there might be some unanticipated difficulties. This is the time to update the plan.

5. Cyber Insurance
Hopefully, the company already has an appropriate cyber insurance policy in place. If there are questions about the types of insurance that protects digital assets and covers cyber risks, contact an insurance broker (preferably, one that specializes in cyber). Now that companies are relying on digital communication, the internet, cloud storage and remote apps more than ever, the risk of a cyber event has increased. Having an insurer that can mitigate and defer some of the costs in such an event is critical.

Cybersecurity in the wake of COVID-19 is a rapidly evolving threat to businesses, especially with employees working in a digital space for the foreseeable future. We will continue to offer suggestions for optimal cyber health and best practices as developments arise on Freeborn's COVID-19 webpage. If you have any questions, please contact Robert A. Stines (rstines@freeborn.com; (813) 488-2928) or another member of the Freeborn & Peters LLP Emerging Industries Team.

ABOUT THE AUTHOR

Robert A. Stines
Partner
Tampa Office
(813) 488-2928
rstines@freeborn.com

Robert is a Partner in the Firm's Tampa office and a member of the Litigation Practice Group and Emerging Technologies Industry Team. Robert is focused on business litigation, commercial disputes, professional liability defense and cyber law. He has litigated contract disputes, products liability claims, legal malpractice lawsuits, unfair trade practices, employment agreements, shareholder disputes, restrictive covenants, healthcare matters, insurance professional malpractice, and business torts. He is a certified IAPP US-law privacy professional.

Freeborn

Your Future Is Our Purpose

140+ Attorneys. 5 Offices.

Freeborn & Peters LLP is a full-service law firm with international capabilities and offices in Chicago, Ill.; New York, Ny; Richmond, Va.; Springfield, Ill.; and Tampa, Fla. Freeborn is always looking ahead and seeking to find better ways to serve its clients. It takes a proactive approach to ensure its clients are more informed, prepared and able to achieve greater success – not just now, but also in the future. While the firm serves clients across a very broad range of sectors, it has also pioneered an interdisciplinary approach that serves the specific needs of targeted industries.

Freeborn's major achievements in litigation are reflective of the firm's significant growth over the last several years and its established reputation as a Litigation Powerhouse®. Freeborn has one of the largest litigation departments among full-service firms of its size – currently with more than 90 litigators, which represents about two-thirds of the firm's lawyers.

Freeborn is a firm that genuinely lives up to its core values of integrity, effectiveness, teamwork, caring and commitment, and embodies them through high standards of client service and responsive action. Its lawyers build close and lasting relationships with clients and are driven to help them achieve their legal and business objectives.

For more information visit: www.freeborn.com

CHICAGO
311 South Wacker Drive
Suite 3000
Chicago, IL 60606
(312) 360-6000
(312) 360-6520 fax

NEW YORK
230 Park Avenue
Suite 630
New York, NY 10169
(212) 218-8760
(212) 218-8761 fax

SPRINGFIELD
217 East Monroe Street
Suite 202
Springfield, IL 62701
(217) 535-1060
(217) 535-1069 fax

RICHMOND
901 East Byrd Street
Suite 950
Richmond, VA 23219
(804) 644-1300
(804) 644-1354 fax

TAMPA
1 Tampa City Center
201 North Franklin Street
Suite 3550
Tampa, FL 33602
(813) 488-2920