BERGER SINGERMAN
FLORIDA'S BUSINESS LAW FIRM

COVID-19: CYBER READINESS FOR REMOTE ACCESS WORKERS

March 26, 2020

By: Gavin C. Gaukroger

With employees abiding work-at-home directives and IT departments adding resources, buying equipment, and generally transitioning to full-scale remote operations, the propensity for exposure to cyber risks is heavily magnified. In the last week, clients, competitor law firms, and certainly many other businesses within and outside of Florida have been struck by cyber attacks, spoofed email accounts, and ransomware demands. These attacks create additional strains on already stretched IT departments, including the human resource elements associated with the relatively unknown long- and short-term effects of the coronavirus on what was previously business-as-usual. With many employees working at home and some using personal devices, employers should insist employees avoid public Wi-Fi hotspots or even their private Wi-Fi networks when accessing confidential information unless they are also connecting via the employer's virtual private network (VPN).

- If an e-mail has irregular typos or the fonts or colors look off, those are red flags suggesting more scrutiny is required. Also, scroll over any hyperlinks in the e-mail to see the URL to which they would direct you. If the URL is off by a letter or the syntax is inconsistent, that is another red flag to stop you in your tracks.

- If you receive an e-mail which appears to be from someone you know and it instructs you to pay money, reveal sensitive information, or otherwise is atypical, do not respond or open embedded links within the e-mail. Rather, send a new e-mail to your contact at the e-mail address you have on file for that person to confirm the request.

- Another trick of fraudsters is to create a false sense of urgency and secrecy. Unless you are aware of a specific deadline from a contractual obligation or other secondary sources, wire transfer instructions which include short deadlines or pressure you to act quickly should be another red flag.

If all efforts to prevent a cyberattack fail and your business falls prey to a fraudster or a hacker, there are things you can do right away to minimize the damage and get your business back on track. First, find out the source of the data breach and try to stop it. If your business is hit with a ransomware attack, you will likely know right away. Second, you should find out how to upright your business, budget for any losses, notify any customers who may be affected by the data breach, notify regulators if required, and check your insurance policy for coverages that may offset or cover the costs of these steps.

To that end, your business may be among the increasing number of businesses purchasing cyber insurance policies. According to a recent report from Marsh, which markets itself as a global leader in insurance brokering and risk management, "[a]s insurers have expanded coverage to include cyber business interruption, coverage has also become more attractive to manufacturers, which are increasingly aware of the operational risks cyber threats can present to them." See Cyber Insurance Purchasing Grows Again in 2019, March 2020. This follows the trend identified by Marsh in its 2019 report which described "property insurers, for example, are generally no longer willing to provide coverage for business interruption caused by network intrusions. Those losses are increasingly expected to be covered under cyber policies, which have expanded to respond to a wide variety of potential risks." See More Cyber Insurance Buyers as Awareness Grows, March 2019.

In addition to data breaches, ransomware attacks have become a one-two punch. Not only can confidential, sensitive information be compromised by a data breach, but ransomware attacks can also interrupt business and bring it to a halt. Having a comprehensive cyber insurance policy that accompanies general liability and property policies should be a part of that plan and will serve as another step towards fending off the potentially catastrophic effects of a cyber attack or a data breach.

Should you have any questions or concerns about your cyber insurance policy, making a claim, or your insurance carrier's obligations, please do not hesitate to contact Michael J. Higer of Berger Singerman's Insurance Team.

The COVID-19 pandemic is creating rapidly-changing issues for businesses, and government aid processes and measures designed to assist businesses may also change materially from when this post is issued. We therefore encourage you to monitor our website, review our future posts and generally remain alert for additional updates or modifications to laws and regulations.

Related Practices

Insurance

Intellectual Property

Related Practice Teams

Dispute Resolution

Related Team Member(s)

Gavin C. Gaukroger

Topics

COVID-19

Coronavirus