BCLP. Client Intelligent

Insights

WHAT DOES THE CORONAVIRUS HAVE TO DO WITH CYBERSECURITY? THEY SHARE MORE THAN A FIRST LETTER

Mar 17, 2020

SUMMARY

With the explosive spread of coronavirus, the Coronavirus Disease ("COVID-19") is driving businesses, educational institutions, and governments to rapidly reassess everything from conference attendance to work-from-home policies to remote commercial transactions. At this juncture, technology has the potential to blunt the disruptive business effects of the virus. At the same time, increased reliance on technology accelerates the risks to entities who have not prepared for increased cyber-attacks in which threat actors may try to take advantage of the growing reliance on remote network, email, and transactional access.

You may have heard the saying that the Chinese word for "crisis" is composed of two distinct characters signifying "danger" and "opportunity." A more correct translation of "crisis," is "danger at a point of juncture." With the explosive spread of coronavirus, the Coronavirus Disease ("COVID-19") is driving businesses, educational institutions, and governments to rapidly reassess everything from conference attendance to work-from-home policies to remote commercial transactions. At this juncture, technology has the potential to blunt the disruptive business effects of the virus. At the same time, increased reliance on technology accelerates the risks to entities who have not prepared for increased cyber-attacks in which threat actors may try to take advantage of the growing reliance on remote network, email, and transactional access. In addition, hackers know that your company is distracted and, much like a pickpocket, may try to take advantage of the strain on your organization caused by COVID-19.

On March 3, 2020, in a letter from the European Central Bank ("ECB"), the ECB warned against "potential risks emanating from [COVID-19] effects...which may include...a potential increase of cyber-attacks... and cyber-security related fraud, aimed both to customers or to the institution..." In the U.K., scammers are sending phishing emails offering the recipient a list of people in their area

infected with COVID-19 or up-to-date information about the virus. When unsuspecting recipients click on the link, it takes them to malicious websites or requests for Bitcoin payments.

The U.S. Department of Homeland Security has issued a warning to remain vigilant for scams related to COVID-19, warning against unsolicited emails with malicious attachments or links, and recommending that everyone review its Risk Management for COVID-19 Guide.

In considering your continuity of operations plans to survive the COVID-19 outbreak, don't let cyber-security be a casualty of supporting remote workers. The following are a few risks to focus on in order to prevent greater disruption to your operations as result of the loss or disclosure of confidential information.

Business email compromises are one of the fastest-growing ways that companies lose control of confidential information. Phishing emails invite employees to enter their login credentials through a variety of pretexts, from fake DocuSign links to unsolicited invitations from a co-worker (whose account has already been compromised) to share information.

Wire transfer requests from the boss who is working remotely and needs the transfer to happen now in order to keep a business transaction on track.

Employees, used to working in the office behind a secure firewall, now provided with mobile devices (laptops and/or thumb drives containing their documents) who are unfamiliar with security protocols to protect those devices from theft or loss, and IT support having to scale up remote operational capabilities that may have bandwidth or equipment limitations.

Uncontrolled (or unrestrained) remote access without multi-factor authentication.

Unsecured remote data ports ("RDPs") through which threat actors may gain access and launch ransomware attacks.

Now is the time to take steps to minimize the threat of malicious actors who see the COVID-19 outbreak as an opportunity to exploit an already distracted and anxious world:

1. Review your cyber insurance policy for appropriate (and adequate) coverage should you be the victim of a ransomware attack, phishing or spoofing emails, or fraudulent wire transfers in addition to the loss or disclosure of personal information.

2. Review your incident response plan (or put one in place!) to ensure it is up-to-date and addresses security incidents involving remote working situations.

3. Ensure that members of the incident response team are prepared to activate in response to a data security incident, even if working remotely. Make sure every member of the response team has cell phone numbers and is reachable in the event of an emergency.

4. Ensure your contact information for your insurance carrier, cyber-security outside counsel, and IT vendors are up-to-date.

5. Prepare (or update) policies and procedures for remote access to your IT network, tele-working, and protection of confidential information, and ensure all your employees are aware of them.

6. Require multi-factor authentication, not only in accessing email and company networks, but in the authorization of wire transfers or transfers of secure information.

7. Permit access of networks and servers only via a VPN.

8. Ensure all devices (computers and memory devices) use full disk encryption.

9. Conduct refresher training for spoofing and phishing emails as well as security awareness when working in unsecure spaces (Starbucks, the library), not leaving devices in a car unattended, or not using the company computer for non-work related activities which may invite malware or viruses onto the computer.

10. Have a backup plan for your data that doesn't have the data backup stored to the same servers your data is on. Remote backup is necessary to minimize the all too common disaster of both your data and data backup being encrypted by ransomware in the same attack.

COVID-19 has the potential of transforming the way you work. At this critical juncture, don't lose sight of the danger that increased reliance on your IT infrastructure without appropriate training and safeguards may have on your employees, your customers, and your bottom line.

RELATED PRACTICE AREAS

- Data Privacy & Security
- Corporate
- Finance

MEET THE TEAM

Kate Brimsted

London

kate.brimsted@bclplaw.com
+44 (0) 20 3400 3207
