Alert

March 26, 2020

COZEN O'CONNOR

Cybersecurity Challenges for Companies in the Wake of the COVID-19 Crisis

Matthew J. Siegel

Member

msiegel@cozen.com
Phone: (215) 665-3703
Fax: (215) 701-2303

Related Practice Areas

- Coronavirus Task Force
- Technology, Privacy & Data Security

Now that much of the workforce has shifted to working remotely, the need for good cybersecurity hygiene has never been greater. Each new connection into the office is another potential avenue for a hacker to gain access and wreak havoc. Even those companies that have had remote access policies in place for years may not be ready for the sudden surge in at-home connections and may not have been able to provide employees with company-provided hardware and software with robust built-in security. This situation is not likely to wrap up in the short term. Even if your organization was caught flat-footed at the start of this crisis, take action now to prevent business interruption and reduce risk: How many employees are using their personal devices to access sensitive or confidential corporate information? Have all of those devices been updated and properly configured to protect against the latest online threats? Is IT able to successfully monitor and respond to what may be dozens or hundreds of individual requests for assistance by employees who are just learning the ropes of logging in from home? Below are some tips that all employers should keep in mind as their employees try to do from home what they would have otherwise done at the office.

Encourage employees not to conduct business (unless previously authorized to do so) from their personal email accounts. Yes, logging in to a work email account may be more cumbersome than simply logging in to a personal account, but if you have set up your workforce to use their corporate accounts from home, make sure they use it. Many free email accounts are easy to hack, don't have great antivirus and malware protection, don't offer two-factor authentication (or it hasn't been enabled), and offer no assurances of privacy.

Discourage employees from saving sensitive business-related information on the hard drive of their personal computers or portable media (unless provided by the company and, where possible, encrypted) or cloud-based storage sites that have not been pre-approved. To the extent possible, files should be saved directly into the corporate enterprise system through the firm network. As with free mail services, free cloud services may not offer robust security and privacy, or the settings may not be configured to provide the protection your business needs.

Employees who handle confidential materials, personally identifiable information, or personal health information, should use the same caution with paper copies at home as they would at the office. Documents should be stored in a secure location and, when no longer needed, shredded. Sensitive documents should not be disposed in the regular trash or recycling bins. If no shredder is available at home, they should bring the documents to the office when this crisis is over and dispose of them there.

Employees should use caution when sending confidential materials via email. Where possible, they should use only secure file transfer programs.

If your employees must use personal computers to conduct business, consider providing the tools and support to make those computers as safe as possible. Encourage and provide support to employees to update operating system patches, software, and settings. Desktop firewalls and antivirus software should be turned on. Home Wi-Fi routers can be updated and made more secure. Employees should, where possible, only connect through a VPN that your company should sponsor. As the work-from-home horizon continues to expand, contact your IT support to start making improvements for the long-run.

Ensure that your information security policies, incident response plans, and remote access policies are updated and, even more importantly, that employees have read and are familiar with them. If necessary, send them out again. If you don't have any written policies or if they haven't been

updated in a while, consider this an excellent opportunity to create or update them.

Remind employees about the risks of phishing attacks and be particularly wary of emails offering advice on the COVID-19 outbreak. Cybercriminals often try to exploit people in times of crisis, when they suspect our guard is down. Phishing attacks are on the rise, so use extra caution when receiving unsolicited emails offering such information as CDC or WHO alerts; sensational news articles; fake charities; local, city, state emergency declarations; or workplace policy and information emails. Where possible, businesses should establish a single email for official company-related updates about the response to the crisis. To stay safe from cyber threats:

- Always check the sender's email address.
- If the address looks like an internal company email, check for an "external sender" tag if applicable.
- Make sure that the greeting in the email is not generic — i.e., "Dear Valued Customer" or "Dear Sir/Madam"
- Hover over the hyperlink in the email to check the address of the website. Sometimes the links will not match the text.
- Poor grammar and layout are good indications of a possible phishing attempt.
- Do not open attachments included in emails until you confirm it is legitimate. A cybercriminal can use these attachments to install malware on your device.
- **Never** provide personal or financial information in an email or a phishing link contained in an email.

For any additional information or questions, contact Cozen O'Connor's Privacy & Data Security attorneys.