RCCB Royer Cooper Cohen Braunfeld

CYBERSECURITY RISKS AND TRANSITIONING TO REMOTE WORK

PUBLICATION, *RCCB CORPORATE & BUSINESS ALERT* - CHASE J. WRIGHT, APRIL 6, 2020

CYBERSECURITY RISKS AND TRANSITIONING TO REMOTE WORK

Our thoughts are with our clients, friends and their families. We are here and available to help. Together we will get through this difficult time and gather strength from each other.

April 6, 2020

Among the countless implications of the Coronavirus (COVID-19) pandemic, one of the most urgent for businesses is the rush to implement “telecommuting” or “work-from-home” (WFH) capabilities for employees, with little preparation for the security risks associated with remote access to company servers and databases. Additionally, with “shelter-in-place” orders becoming a norm, lax company policies, procedures, and standards are adding to confusion as employers are struggling to adapt to WFH models. As businesses are transitioning from in-person to WFH remote platforms, employees are inundated with emails and online meeting requests, which can include phishing attacks and the introduction of malicious software (i.e., malware) to a company’s network.

This article tackles some of the perils associated with remote work and offers tested solutions to keep your business running and secure. While the below guidance is general in nature, RCCB is here to help guide your business through these challenging times.

A phishing attack is the fraudulent use of electronic communications, such as emails and text messages, to dupe and deceive users into providing sensitive information like passwords and usernames to a seemingly reputable source. By disclosing the information, the users can provide cybercriminals with a direct gateway to private servers, databases, and other proprietary systems containing confidential information about your business, employees, suppliers and customers. A phishing attack can also result in the introduction of malware to a company database which can compromise an entire company network. In the wake of the current crisis, there has been a surge of email phishing attacks designed to resemble correspondence from the CDC and World Health Organization and organizations should advise their personnel to be on the lookout for such official-looking correspondence.

MORE.

Recent cyberattacks have grown not only in numbers but also in sophistication. For instance, business email compromise attacks (BECs) have been widely reported, whereby cybercriminals target specific employees in an company (like a CEO or President) and send spoof emails to customers or others in the organization, oftentimes requesting financial or other proprietary information. Training staff to make in-person or telephone verifications to known contacts before following through on such requests, particularly when the requests are unanticipated, can help your organization limit the risk of a costly BEC.

When working on-site from a secure office and network, a company's online security measures often include virtual private networks (VPNs), firewalls, secure monitoring, and anti-virus and anti-malware software. However, with employees transitioning to home offices, businesses' systems become only as secure as its employee's personal Internet connections and whatever security training those employees may or may not have.

Below are some factors to consider when implementing a secure remote system in any environment, particularly during the current COVID-19 pandemic.

Implement Effective Company Policies and Procedures

In implementing an effective telecommuting work policy, businesses should include specific guidance pertaining to employees' use of the company systems, many of which are related to HR. For instance, employers may restrict certain non-essential employees' ability to access or download certain company records as a means to limit what information could be compromised in the event of a security breach. If possible, you may want to instruct employees to refrain from connecting to public networks (i.e., via public Wi-Fi), as these networks substantially increase the risk of a fraudulent compromise. Additionally, have your employees confirm that they are not relying on the default, out-of-the-box network settings (such as network and administrator names, and open guest networks), on their home Wi-Fi routers.

Employers will also want to consider the following:

- Mechanisms to manage conduct and monitor employee performance metrics;
- Lists of approved and prohibited equipment and technology that may be utilized (e.g., desktop, laptop, cell phone, fax equipment, printers, USB drives, etc.); and
- Confidentiality requirements to ensure that company equipment and records are not purposefully or inadvertently shared.

Require a VPN to access the Company Network

Employers should consider utilizing a VPN as a means for all employees to remotely access the company network. A VPN is a secure, encrypted, end-to-end “tunnel” that ensures that the users accessing business data and company network are authorized to do so. All traffic through a VPN (i.e., from the employee to employer) is encrypted. Therefore, regardless of the network or Wi-Fi that the user is connected to, the communications being transmitted should be secure from interception. If your business utilizes a third party vendor for managing IT and technology infrastructure, they will likely be able to assist you in setting up a VPN and training your employees on proper usage. If you have not done so, consider having your IT vendor confirm that the software and systems your business is using have been updated with the latest security patches as they are updated by your applicable software vendors.

Utilize Two-Factor Authentication

Two-factor authentication (2FA) is an added layer of security that ensures that those individuals trying to access a certain network are who they say they are. Utilizing a standard user name and password combination to access a network provides one type of authentication. An example of a 2FA process is the sending of a code via text messages, phone call, or email to the authorized individual’s account after the user enters their username and password, but before the user is granted access to the network. Only by entering that second type of authentication is the user granted access. 2FA helps protect against the downfalls of unsecure passwords and other common user errors as having a valid user name and password is not enough to gain access.

Review Customer Contracts

Businesses should also review their current and future customer agreements to ensure that the company is permitted to work remotely, as some agreements prohibit accessing confidential and sensitive information by remote means. If such activity is prohibited, the business should work to secure an amendment, even if only on a temporary basis in order to provide continuity of services during the current crises.

Educate Employees

When it comes to cybersecurity, employees are on the front line of a company's virtual defenses. For this reason, one of the best investments for businesses is to educate their staff on current issues and threats, the available tools to combat and mitigate risk, and the overarching importance of remaining alert and diligent when utilizing company software, hardware and systems. Education of staff should include (i) knowledge-based programming to ensure that employees are substantively familiar with common scams such as phishing, BECs, and ransomware; and (ii) hands-on training to ensure that employees are practicing secure tactics, such as periodically updating passwords, installing all company-authorized updates of software, knowing where to report suspicious activity, and being prepared to act in the event that a breach occurs. To the extent you decide to roll out new WFH software or have personnel install security updates, be sure to set clear expectations and provide detailed instructions to limit the risk of anyone installing unauthorized files.

Secure Adequate Cybersecurity Insurance

Lastly, your company should ensure that it is adequately covered by a cybersecurity insurance policy. A cybersecurity policy ensures that the business is covered for costs associated with a data breach, phishing attack, virus, or other cyberattack. If your business currently has a cybersecurity policy, you should ensure that working remotely is covered under the policy terms.

PROFESSIONALS

Chase J. Wright

CAPABILITIES

Corporate & Business