Published on *The National Law Review* https://natlawreview.com

Cybersecurity and Privacy: 10 Best Practices When Working From Home

Article By:

Danielle Vanderzanden

Rebecca J. Bennett

As the news reports show, the sudden shift to employees working from home poses new cybersecurity risks for businesses and the employees who work remotely. Below are 10 important measures that can help mitigate these substantial risks.

1. Encrypt Data and Tightly Control Access to Encrypted Data.

Encrypting data at rest and in transit continues to be essential to information security. Instruct employees to store work on the employer's system (rather than on company-owned or personal devices). When working with third-party vendors, review contract terms to provide ample protection for your data.

2. Deploy Secure Devices to Remote Employees.

Most employee-owned personal computers lack important malware and encryptions protections, and hackers already are capitalizing on the vulnerabilities of personal computers. Such vulnerabilities increase the risks to data on these personal computers and data accessed from those computers (including data that resides on company servers accessed remotely). For entities covered by the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), and other regulatory schemes, this is essential. Given these vulnerabilities, employers can consider requiring employees to keep all work data on company-owned devices and avoid cloud-sharing applications that have not been vetted for privacy and security. Limiting the diversity of storage repositories helps limit the number of potential avenues of attack.

3. Enhance VPN Security, Password Strength, and Telephone/Video Conference Protections

Require multi-factor authentication to access the employer's virtual private network (VPN) (especially if employees are using their own devices to obtain such access). The fact that employees cannot interact in-person increases the need for multi-factor authentication and strong passwords. Reiterate

the importance of using strong passwords and protecting the security of those passwords. Weak or stolen passwords remain a primary cause of compromise to information security.

Advise employees who discuss confidential matters by telephone or videoconference of the risks that intruders may attempt to hear and see such conversations. Sending conference coordinates (such as a meeting identification number) and passwords separately minimizes such intrusions. Turning on participant identification features and using technology that allows a moderator to remove unexpected participants will help ensure that only authorized individuals participate.

4. Beware of Insecure Wi-Fi

Advise employees to avoid accessing the internet on shared or public Wi-Fi services. If employees do not have access to multiple networks within their homes, advise them to use a personal hotspot or other dedicated wireless networks separate from the Wi-Fi to which others have access.

5. Refresh Phishing Warnings and Employee Trainings

Employees will expect to see additional email traffic during this unique period. Accordingly, hackers are deploying new phishing scams and employees are falling prey to them. To help protect against nefarious actors, remind employees to refrain from clicking on links in any unanticipated email messages; follow company procedures when responding to requests for funds; refrain from buying gift cards from anyone claiming to be a company employee; avoid opening unexpected documents, links or other downloads; and beware of impersonation attempts. The uptick in phishing is widespread, and hackers are posing as banks offering COVID-19 assistance, entities providing COVID-19 avoidance and health advice, and a myriad of other businesses.

6. Limit Access to Games and Websites on Devices Used to Access Employer Systems

Many websites and online games provide vulnerability vectors; therefore, preventing employees from accessing non-work-related sites on devices used to perform work will limit these risks.

7. Keep Track of Devices and Secure Physical Work Spaces

During periods of remote work, tracking physical assets used to access employer systems is critical. In addition, employers may want to remind employees to apply physical measures to secure any devices that contain company data. Such steps may include locking home and home-office doors, placing devices in a safe, keeping devices with them while traveling, and locking screens before stepping away from their computers. Many information security incidents occur when a device is stolen or misplaced, and protecting the physical security of devices that may store information or perform computing functions is essential.

8. Prevent External Device Attachment

Thumb drives and other external devices provide avenues for data exfiltration and vectors for information security compromise. Employers may want to remind employees to limit the use of these devices and to keep them safe if they use them.

9. Formalize Work-From-Home Arrangements and Train Employees

Employers may find it useful to establish written protocols for remote work arrangements that address information security, privacy, and other work restrictions. In addition, employers can ensure that these policies require immediate disclosure of any potential information security compromise. Such written policies must protect the employer's ability to remove employer data from personal devices.

10. Prepare an Incident Response Plan

Extensive remote work arrangements, as have been necessitated by COVID-19, pose a myriad of heightened security risks to professional and personal information. Prepare to address those risks.

National Law Review, Volume X, Number 108