SHERMAN&HOWARD

shermanhoward.com

DATA SECURITY & PRIVACY ADVISORY

Best Security and Privacy Practices for Remote Work Environments

As a result of COVID-19 and mandatory stay-at-home or shelter-in-place orders, many employers have recently moved to 100 percent remote work environments. This transition creates unique challenges to protecting a company against a security breach or loss of client or company data. As a result, additional security measures are recommended to enhance your company's data security.

This advisory outlines the following important areas for businesses to consider in devising policies, procedures, and employee training programs:

- How to access your company's network remotely
- Dual or multifactor authentication
- Protecting and securing personal computers and devices
- How secure are file share apps and cloud services
- Best practices for secure communications
- Protecting against cybersecurity breaches
- Clarifying or reiterating policies and employee expectations of privacy matters

Jessica Arett
Associate
Denver, CO
303.299.8170
Email

Emily Keimig
Member
Denver, CO
303.299.8240
Email

Melissa Reagan
Member
Denver, CO
303.299.8310
Email

Katie Varholak
Member
Denver, CO
303.299.8428
Email

HOW TO ACCESS YOUR COMPANY'S NETWORK REMOTELY

Remote access must be implemented in a secure manner:

- Virtual Desktop Infrastructure (VDI) Access. The most secure manner for employees to access a company's network is through a VDI system. VDI uses a highly secure virtual desktop infrastructure with a gateway using remote desktop technology to shield applications and sensitive data.

- Virtual Private Network (VPN) Access. If a VDI system is not available, the next best secure manner for employees to access a company's network is through a VPN on a company-issued computer. VPNs use secure channels that protect a company's systems and network, which a personal or unmanaged system may not have.

- Remote Access

  - Personal Computers or Laptops. If a company's employees can only work remotely on personal devices, companies should consider other ways to allow remote access without a direct VDI or VPN connection from personal computers. This could include licensing a third-party remote access solution to provide connectivity through a web browser without the need for VPN software. This permits an employee to access the company's network or devices through a secure environment. Companies should consider limiting employees' abilities to file transfer and print through this remote environment.

  - Mobile Devices. If a company allows employees to access company data on their mobile devices, the company should implement controls to protect the device and its data. At a minimum, a company's IT administrator should be able to remotely lock and erase the device or business information stored on the device.

DUAL OR MULTIFACTOR AUTHENTICATION

Dual or multifactor authentication requires more than one mode of authentication for the employee to access the system. Implementation of dual or multifactor authentication is one of the strongest security methods to prevent the compromise of the company's network or online accounts. The following are examples of different types of authentication that, when combined, constitute dual or multifactor authentication:

- Something the employee knows (username and password)

- Something the employee has (one-time passcode)

- Something the employee is (fingerprint or eye scan)

An employee's access to the company's network, including VPNs, or online accounts should be protected with a dual or multifactor authentication to mitigate the risk of unauthorized access to the company's systems or applications.

PROTECTING AND SECURING PERSONAL COMPUTERS AND DEVICES

The following is a list of best practices for employees to protect and secure personal computers and devices when working in a remote work environment:

- Install antivirus software and ensure it receives and installs regular, automatic updates.

- Practice good password management, including a secure password on home systems. For even stronger protections, set up multiple home Wi-Fi networks — one Wi-Fi network for work only and one network for personal uses such as kids' devices.

- Keep confidential and proprietary data inside the company's network. Avoid conducting work over public Wi-Fi networks or when working in public spaces. If an employee must use a public Wi-Fi network, he or she should connect using the company's VPN or a secure personal VPN application.

SECURING CLOUD SERVICES AND FILE SHARE APPS

Companies that use cloud services such as email or file sharing should ensure that data is protected from additional threats that are introduced through a remote work environment:

- Companies may consider providing their own secure file share platform for employees and the company's clients, vendors, and third parties to share and exchange files and data.

- Companies should consider limiting access to cloud services and file sharing apps from an employee's personal device to preclude employees from downloading company or client data and causing potential data loss on personal devices.

- If companies or their clients or vendors use sources such as DropBox or GoogleDrive to send files, train employees to confirm the source is legitimate before clicking on any links.

- Companies should work with their cloud providers to validate that the appropriate access controls are in place to protect a company's business, confidential, and proprietary data.

BEST PRACTICES FOR SECURE COMMUNICATIONS

- Emails with Individuals Outside the Company. Companies should consider deploying a secure email solution for sharing confidential, proprietary, and protected information. This solution should include end-to-end encryption. A secure email solution guards data and increases compliance with federal and state privacy laws and regulations.

- Employees Using Email Outside of VPN/Personal Devices. Companies should ensure that employees who are using email outside of the VPN are still secure by utilizing network passwords and email filtering solutions (e.g., filtering spam). Email filtering of inbound email protects against spam, malware, phishing, and targeted attachments. Companies should have an email security platform in place that works no matter where email is being checked. Companies should discourage employees from pulling data from email and saving it to personal devices.

PROTECTING AGAINST CYBERSECURITY/DATA BREACHES

- Be Aware of New Schemes. Hackers will try to take advantage of COVID-19 and the significant increase in remote work environments to find new ways to attack a company's networks and data. Hackers will use news and other information about COVID-19 and new processes in remote work environments (e.g., depositing checks electronically) to make emails, phishing, and other social engineering seem more believable to employees. This, in turn, could lead to a loss of a company's data or financial fraud.

- Educate Employees. Companies should continue to educate and train employees to be aware of these types of cyber-attacks and suspicious communications. Employees should be able to recognize fraudulent emails and phone calls that will help companies protect against cyber-attacks such as phishing and spoofing. Employees should also know the appropriate person/department to contact if they suspect they have received this type of communication.

CLARIFYING OR REITERATING POLICIES AND EMPLOYEE EXPECTATION OF PRIVACY MATTERS

- Review and Redistribute Your Policies. It is important that you review policies to ensure they address the new workplace reality, especially if employees are required or expected to use personal devices.

- Consider Additional or More Stringent Protections for Sensitive Information and Data. Be mindful that certain information, including trade secrets, health-related information, and other confidential or proprietary data may need to be protected separately and more stringently than other data when there are employees accessing networks remotely.

- Make Communications Easy. Providing one contact point where employees may seek help and answers to IT-related matters will provide an opportunity for the company to remind employees of the applicable policies and help them navigate the best way to do business remotely.

These security measures will remain relevant after the stay-at-home orders are lifted because employees will be better prepared for handling remote work in an array of environments, including travel and other remote locations such as hotels, airports, and coffee shops.

Click HERE to receive S&H Advisories and invitations to events.