SWANSON, MARTIN & BELL, LLP

Data Protection and Information Privacy Newsletter

March 2020

Protecting Your Company When Employees Work From Home

With the outbreak of COVID-19, unprecedented numbers of employees are working from home. Whether you find your company scrambling to adjust to the new reality, or you developed extensive work from home policies years ago, now is a good time to review some of the basic principles that keep your company safe.

1. **Secure Your Devices –** The biggest risk remains theft of the devices that hold your company's secrets. Remind employees not to leave computers, cell phones or other devices in their cars or other places that might tempt opportunistic thieves.
2. **Do Not Use Public Wi-Fi –** In many regions, restaurants and coffee shops are already closed, but employees will look for ways to break the monotony of being at home. So please keep in mind that transmitting your corporate data and confidential information over public Wi-Fi places that information at risk.
3. **Beware of Phishing Scams –** Data protection professionals have already noticed an uptick of phishing attacks using coronavirus to get their targets to download malware or other malicious software.
4. **Update Anti-Virus Software –** Employers and employees should make sure their anti-virus is up to date for all systems, on both work devices and personal devices. Preferably, your corporation has reviewed and approved certain anti-virus software already installed on work devices.
5. **Use a VPN or Other Remote Desktop Application –** Employees should only access confidential or other work materials through a VPN or other pre-approved, secure channel.
6. **Review the Terms of Service for All Web Conference Tools –** Several popular web conference services claim a right to record and keep the recording of any teleconference. This may conflict with your company's data privacy needs and expose your confidential information. Together with counsel, you should carefully review the terms of service and privacy policy for all services employees use for work.
7. **Avoid Personal E-mail –** Personal e-mail and web storage should never be used for corporate work. Use of personal e-mail may open the employees to discovery in the event of litigation or when applicable, FOIA requests.
8. **Do Not Forget Data Regulations –** If your company is subject to HIPAA requirements, the Gramm-Leach Bliley Act, GDPR, or other data privacy laws, do not forget to confirm compliance with these regulations. Some telecommuting tools explicitly acknowledge they are not HIPAA compliant. Always work with counsel to assure you stay complaint with all applicable laws.

If you need to review your telecommuting policies or help establish procedures for your employees working from home, please do not hesitate to contact us at Swanson, Martin & Bell, LLP. We are here and ready to help.

If you have any questions regarding this alert please contact **Bill Patterson** or **John Arranz**, co-chairs of Swanson, Martin & Bell, LLP's Data Protection and Information Privacy Practice Group.

Prepared by Swanson, Martin & Bell, LLP attorneys Bill Patterson, Emily Fitzgerald and Madison Shepley.