Top 5 Data Privacy Considerations when Managing a Workforce Working at Home

Amundsen Davis Data Privacy & Security Alert
April 16, 2020

For most businesses the mass transition to working from home during COVID-19 shelter in place orders is a new venture. However, with this (temporary) transition from operating out of the same building, what should remain is adherence to good cyber hygiene protocols. For securing your company's online or at-home business practices, consider the following:

1. **Secure Your Home Network:** Now that employees are all operating off of different networks, businesses are more vulnerable than ever to hackers and cyber attacks. Make sure internet-connected devices are up to date with the latest operating systems and security software. This is especially critical for those working from personal devices. Also, encourage employees to secure their wireless router by changing any preset passcodes or updating current passwords.
2. **Beware of Phishing Scams:** Just because you aren't down the hall or in the next cubicle from coworkers, doesn't mean that your communication should be limited to email. In fact, scams perpetrated via business email compromise continue to run rampant. Make sure employees are being vigilant and flagging suspicious requests—such as wiring money or sharing passwords over email and an unfamiliar webpage prompt. Even better, before making any electronic deposits or exchanging private information, encourage teams to *pick up the phone* to ask and verify requests or to take other and additional steps to authenticate and legitimize.
3. **Protect Your Virtual Meetings:** Online business platforms have been making headlines since hackers have learned how to infiltrate video meetings. To avoid unwanted guests, take advantage of your video platform's privacy and security settings. If you are able, require a meeting password or allow the host to lock the meeting once all participants have joined. Additionally, be cognizant of what team members are sharing in the chat feature and turn off settings that may allow these conversations to be saved.
4. **Opt-In to Security Authentication:** When your workforce was mainly (or totally) under one roof, you may have declined certain "optional" security offerings by your business-to-business partners. For example, banks and

PROFESSIONALS

Molly A. Arranz
Partner

RELATED SERVICES

Cybersecurity & Data Privacy

communication providers offer multifactor authentication and other technology backstops, but you may need to "opt in" to these protections. Perhaps these optional offerings weren't, previously, as critical, but it may be appropriate to reconsider those security protections given the current work from home challenge to access management protocols.

5. **General Security of Confidential Information:** Privacy and security isn't limited to technology. Best practices at the main office also included physical security of the workspace, erasing sensitive material from whiteboards, logging-off and shredding confidential and private materials. Remind your employees that privacy protections are not just restricted to online. When working from home, it is still important to be mindful of the workspace and any paper materials generated.