As seen in *The Agency 100*

SEPTEMBER 11, 2020

LEGAL

CYBERSECURITY AND PRIVACY RISKS RISE WITH REMOTE WORKFORCE

With striking speed, the arrival and spread of the coronavirus pushed much of the U.S. workforce to a remote environment. The shift to a remote workforce is not expected to end any time soon. Many companies are extending their work from home policies, including Google, which announced that their employees will be allowed to work remotely until at least July 2021. Twitter and Facebook, meanwhile, have announced that their employees will be allowed to work from home indefinitely.

As an unwelcome consequence, many businesses are now exposed to a whole new array of data privacy and security vulnerabilities.

While some with existing work-at-home policies had likely already assessed and addressed the privacy risks that a remote workforce typically presents, many others, for whom an employee base "working from home" is new, are facing the resulting privacy and data security risks for the first time. Because these risks can be quite substantial, they require immediate attention.

The Risks

Cybercriminals are finding new (and many more) targets in employees who use personal laptops or home computers to work, and even those who use

ABOUT THE AUTHORS

Michael C. Lasky
is Founder and Chair of the Public Relations Law Practice Group of Davis & Gilbert LLP.

He may be reached at mlasky@dglaw.com or 212.468.4849

Richard Eisert
is Partner in the Digital Media, Technology & Privacy Practice Group, Davis & Gilbert LLP.

He may be reached at reisert@dglaw.com or 212.468.4863

company-issued devices and are now connecting from home every day. Phishing attempts — including by scam artists who use the coronavirus in emotional appeals (or scare tactics) to further their hacking, malware and ransomware attacks — are spiking as companies' security efforts are outpaced by the rate of work-related remote connectivity. As the recent cyberattack on Twitter demonstrates, even sophisticated companies are not immune to these tactics. The Federal Trade Commission has reported that, to date, it received over 3,900 reports of scams related to the coronavirus, amounting to an estimated $13.78 million in losses.

Privacy issues abound. Consider, for example, the risks of sensitive documents being visible when employees post selfies on social media while working from home — or even when using work-sanctioned video-conferencing. Couple these risks with concerns over how documents are being destroyed when away from the standard workplace shredder bins, and it is inevitable that sensitive or otherwise confidential information will be inadvertently disclosed.

Sudden increased reliance on remote technologies has also exposed latent data security risks. For example, Zoom's overnight popularity has made it synonymous with videoconferencing and yet its sudden boom led to highly publicized data security incidents. Hackers infiltrated private Zoom chat rooms, giving rise to the term "Zoombombing" and around 530,000 Zoom usernames and passwords were discovered being sold on the dark web. Zoom, in response, implemented a 90-day plan to address the security concerns, including adding a waiting room feature, implementing default passwords for chat rooms and allowing end-to-end encryption for all users.

Protecting against and remaining alert to any potential data breaches is only half of the battle. If any breaches do occur, they must be assessed, investigated and handled just as they otherwise would have been handled pre-pandemic and pursuant to all applicable data breach notification rules.

Mitigation Strategies

There are a number of steps firms and companies should consider to mitigate the exposure implicated by these, and similar, risks, including the following:

- **Clean Desk Policies:** Clean desk policies are equally important when working from home in an age when communication via video or other visual means is so prevalent.
- **Passwords:** Firms and companies should remind their employees to create strong passwords, and to change them regularly. To effectively implement this, regularly scheduled prompts should be sent to all employees.
- **Devices:** Firms and companies should help their employees effectively secure their devices, such as by working through a virtual private network (VPN), incorporating multi-factor authentication, using (and regularly updating) an antivirus program and limiting connectivity to other networks. Also, reminders should be given with respect to the installation of software programs on devices used for business purposes.

- **Emails:** Firms and companies should remind their employees to exercise caution when opening emails from external sources and to be wary of suspicious emails, such as requests for personal data (e.g., social security numbers, passwords or account information).
- **Authorized Systems:** Even though employees are working from home, they should still only use company-authorized systems and services. These may include the company's email systems (as opposed to personal email accounts) and document management systems. Firms and companies should continue conducting thorough due diligence data security reviews of any new vendors of remote technologies that are being used by their employees.
- **Policy Creation/Review:** Finally, firms and companies should review their security practices to ensure they have the proper security policies in place, including policies to prevent and address security breaches. Even if these policies already exist, they should be reviewed to ensure continued effectiveness in the current environment and IT support personnel should be trained and to maintain effective support to handle the increased pressures and new risks posed by a remote workforce.

It is important for businesses to address their cybersecurity and other risks they face with a remote workforce.

Firms and companies must stay vigilant and not become complacent as time goes on, as well as maintain regular communication with their workforce regarding safe data practices.