DAVIS GILBERT

Cybersecurity and Privacy Risks Rise with Remote Workforce

The Bottom Line

- It is important for businesses to address their cybersecurity and other risks they face with a remote workforce since remote work is likely here to stay in one form or another.
- Employers must stay vigilant and not become complacent as time goes on, as well as maintain regular communication with their workforce regarding safe data practices.

With striking speed, the coronavirus pushed much of the U.S. workforce to a remote environment. Even as businesses and cities reopen, this remote work trend is likely to continue for the foreseeable future.

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

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. Resulting data breaches, however, 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 employers 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**: Employers 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**: Employers 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**: Employers 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). Such 'phishing' scams are often how vulnerabilities first enter a corporate network.
- **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.
- **Policy Review**: Finally, employers should review their security practices to ensure continued effectiveness and train and maintain effective IT support to handle the increased pressures posed by a remote workforce.

Related People

Richard S. Eisert
Partner/Co-Chair Advertising + Marketing
212 468 4863
reisert@dglaw.com

Gary Kibel
Partner
212 468 4918
gkibel@dglaw.com

Oriyan Gitig
Counsel
212 468 4880
ogitig@dglaw.com