

Publications

Remote Work Increases Data Security Risks

Related Attorneys

John L. Landolfi

Marcel C. Duhamel

Jackie Ford

Christopher L. Ingram

Eric W. Richardson

Related Services

Data Strategy, Privacy and Security

CLIENT ALERT | 4.13.2020

Your employees are sheltering in place and working remotely. They now communicate with each other, business partners and customers via email, Zoom, and text messages. Maybe you have a robust VPN (virtual private network (VPN) environment, but are your employees always taking the time to log in through that VPN to work with your data? Do you know where they are saving documents they edit and create at home? Are they creating electronically stored information (ESI) that you may someday need to locate, preserve, and perhaps produce in litigation? Are they putting customers' privacy at risk?

Email use, bring your own device (BYOD) programs, and telecommuting have always raised privacy and security concerns, but with tens of millions of Americans suddenly working from home those issues have taken on new urgency. Even where employers have technological and policy safeguards in place, those measures are only as good as the on-the-ground practices of the employees using them. All too often, IT and legal departments develop and implement policies that employees circumvent and undermine, often unaware of the risks they create by doing so.

If you have not already done so, now is the time to reiterate and retrain your workforce on proper and secure online practices. It may also be the perfect time to provide online training for employees on paid furloughs who are not otherwise fully occupied with day-to-day business needs.

Vorys has been working with many clients recently on tips for navigating data privacy and security issues in these challenging times, including:

Email hygiene

- How to spot and avoid phishing and social engineering attacks
- How to spot and avoid scams

- How to minimize the risk of disclosure of private information
- How to communicate effectively without creating unnecessary liability
- When, and how, to use chat, instant messaging, and alternatives to email

Telecommunications safety

- How to minimize privacy risks when using tools like Zoom, Skype, and other videoconferencing solutions

Information governance

- How, and why, to control the location of data and confidential information
- How to maximize the benefits of instant messaging tools while mitigating the risks
- How to use, and not to use, personal devices, hard drives, thumb drives, and personal email accounts

Vorys offers training to law departments, sales teams, customer service teams, and your workforce generally on the above topics. To discuss any of these issues or schedule a remote training session, contact Marcel C. Duhamel, Eric W. Richardson, or any of Vorys' other privacy and security lawyers.

--

Vorys COVID-19 Task Force

Vorys attorneys and professionals are counseling our clients in the myriad issues related to the coronavirus (COVID-19) outbreak. We have also established a comprehensive COVID-19 Task Force, which includes attorneys with deep experience in the niche disciplines that we have been and expect to continue receiving questions regarding coronavirus. Learn more and see the latest updates from the task force at [vorys.com/coronavirus](https://www.vorys.com/coronavirus).