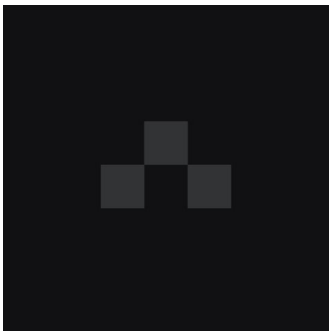
PUBLICATIONS

Internal Investigations and Data Security in a Bring-Your-Own-Device Company

March 18, 2015

As cell phones have become smartphones, employees have gained 24/7 access to a tremendous amount of company information. And as the Bring-Your-Own-Device ("BYOD") trend has spread, so has the risk that companies will lose control of that information. In a BYOD company, employees own the mobile devices that they use for work. Company information is therefore being transmitted to and from, and stored on, devices that the company does not own. Further, because many employees choose to avoid the "two-pocket" problem by having only one smartphone or laptop, they engage in both business and personal activities on the same device. Left unaddressed, these two facts — employee ownership and dual use — could severely hamper companies' ability to protect their data and conduct internal investigations. In this article, SRZ partner Holly H. Weiss and former SRZ attorney Michael L. Yaeger discuss how companies should draft their information security policies with special attention to the ways that BYOD practices create security risks and affect investigations.

Related People



Holly Weiss

Retired Partner

New York

Practices

CYBERSECURITY AND DATA PRIVACY

EMPLOYMENT AND EMPLOYEE BENEFITS

LITIGATION

Attachments

Download Article