wiley

PRESS RELEASE

Wiley Rein Team Co-Authors Cyber Risk Chapter in ABA's Practical Guide to Corporate Social Responsibility

September 12, 2019

Press Contact
Patricia O'Connell
T: 202.719.4532
poconnell@wiley.law

Washington, DC — A team of lawyers from Wiley Rein LLP's Privacy, Cyber & Data Governance, Telecom, Media & Technology, National Security, and White Collar Defense & Government Investigations practices authored a chapter on cyber risk management for a new book on corporate social responsibility, published by the American Bar Association (ABA). The chapter is "Cybersecurity Risk Management Is a Corporate Responsibility." It was co-authored by Wiley Rein partner Megan L. Brown and associates Michael L. Diakiwski, and Kathleen E. Scott, along with Matthew H. Solomson, Chief Legal Officer of Federal Government Solutions at Anthem, Inc.

This timely chapter is part of a comprehensive resource, *The Lawyer's Corporate Social Responsibility Deskbook: Practical Guidance for Corporate Counsel and Law Firms*, which will serve as a valuable tool for practitioners who want to learn more about board governance, community relations, stakeholder engagement, and much more.

The cybersecurity risk management chapter focuses on a range of cybersecurity risks that go beyond consumer data breaches – including threats from hacktivists, nation-states, and criminals – and that may impact companies, consumers, employees, competitors, and third parties. The authors point out:

Related Professionals

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Practice Areas

National Security
Privacy, Cyber & Data Governance
Telecom, Media & Technology
White Collar Defense & Government Investigations

There are no simple answers or compliance checklists. Responsible cybersecurity requires a mind-set that prioritizes risk management.

Cybersecurity is one of the most challenging issues facing organizations. Cybersecurity once was considered an offshoot of privacy. It is not. Cybersecurity goes beyond data control, integrity, and confidentiality. It involves the protection of networks and data from intrusions and disruptions.

The chapter describes existing U.S. and global obligations and emerging "soft law" on the expectations facing private organizations to manage cyber risk. It identifies best practices and sources of guidance in a shifting landscape. And it offers seven "key tasks" that corporate counsel and outside lawyers need to consider as they assess and help their organizations manage risk. These seven key tasks offer practical ideas and questions to focus decision makers and counselors on what they should be asking themselves about readiness and next steps, on issues from risk assessments to incident handling to vulnerability management to preserving privilege and working with the government.

Ms. Brown says, "we wrote this chapter to lay out the core considerations a responsible organization should have top of mind and provide practical resources. As government expectations are rising, companies must shed a compliance mindset and pivot to proactive risk management. This includes recognizing their place in the broader economic and national security landscape."

Ms. Brown, a leading cybersecurity lawyer, *served in the U.S. Department of Justice as Counsel to two U.S. Attorneys General. She* is Associate Director for Cybersecurity at the National Security Institute (NSI) at George Mason University Antonin Scalia Law School, and authored the NSI white paper, "Cyber Imperative: Preserve and Strengthen Public-Private Partnerships." She also co-authored the pivotal IoT Security Report published by the U.S. Chamber of Commerce. She serves on the U.S. Chamber's Cybersecurity Leadership Council and on the Board of the Women's High-Tech Coalition.

Mr. Gardner is a former Assistant U.S. Attorney for the Eastern District of Virginia; he worked in the Cybercrime Unit as a federal prosecutor in both the Eastern District of Virginia and the Southern District of California. He served as lead prosecutor on dozens of investigations involving computer crimes and cybersecurity issues, and has extensive experience in the Electronic Communications Privacy Act, the Computer Fraud and Abuse Act, and the Wiretap Act.

These Wiley Rein lawyers are all members of the firm's Privacy, Cyber & Data Governance Practice, which advises clients on cutting edge privacy, data security, and cybersecurity issues. The Practice provides a comprehensive range of compliance and strategic advice, from advice for Boards and senior management to managing government investigations into security incidents. Wiley Rein covers emerging technology and security trends at our blog, WileyConnect.com, where we host regular podcasts on technology law and policy, including cybersecurity.

For more details on the book, or to purchase a copy, please click here.