This is your new

Cybersecurity
A Practical Guide to the Law of Cyber Risk

Edited by
Edward R. McNicholas & Vivek K. Mohan

The many recent sophisticated cyber threats—from hacktivists and empowered insiders to organized criminals and state-sponsored cyber attacks—means that the task of managing cyber risks, once the near-exclusive realm of IT professionals, is now also borne by attorneys, senior executives, and directors. PLI’s new Cybersecurity: A Practical Guide to the Law of Cyber Risk provides the practical steps that can be taken to help your clients understand and mitigate today’s cyber risk and to build the most resilient response capabilities possible.

Cybersecurity: A Practical Guide to the Law of Cyber Risk provides a comprehensive discussion of the complex quilt of federal and state statutes, Executive Orders, regulations, contractual norms, and ambiguous tort duties that can apply to this crucial new area of the law. For example, it describes in detail:

- The leading regulatory role the Federal Trade Commission has played, acting on its authority to regulate “unfair” or “deceptive” trade practices;
- The guidance issued by the SEC interpreting existing disclosure rules to require registrants to disclose cybersecurity risks under certain circumstances;
- The varying roles of other regulators in sector-specific regulation, such as healthcare, energy, and transportation; and
- The impact of preexisting statutes, such as the Computer Fraud and Abuse Act and the Electronic Communications Privacy Act, on current cybersecurity issues.

In addition, the authors of Cybersecurity: A Practical Guide to the Law of Cyber Risk have supplemented these more traditional sources of law with industry practices and the most important sources of soft law:

- An explanation of the National Institute of Standards and Technology (NIST) Cybersecurity Framework and information sharing environments from a former Department of Homeland Security official,
- The views of the U.S. Secret Service on partnering with federal law enforcement and effective information-sharing,
- The guidance of leading consultants about the appropriate steps to prepare for cybersecurity incidents,

(continued on reverse)
• The perspective of a leading insurance company on the evolving role of
insurance in protecting companies from the financial losses associated
with a successful cyber breach, and
• The views of one of the most sophisticated incident response organiza-
tions on the proper elements of effective incident response.

Throughout the book, Cybersecurity: A Practical Guide to the Law of
Cyber Risk includes practice tools developed during the hundreds of breaches
that the authors have weathered with their clients. These valuable practice aids
include checklists, an overview of the legal consequences of a breach, and a
tabletop exercise.

Table of Chapters

1. An Introduction to the Law of Cyber Risk
2. The General Legal Framework for Information Security
3. The Executive Framework for Cybersecurity: Executive Orders,
   the NIST Framework, and the SAFETY Act
4. Corporate-Government Engagement/Public-Private Partnerships
5. Cybersecurity in Regulated Sectors
6. Data Protection: Risk Management
7. Cyber Insurance
8. Incident Response

About the Editors

Edward R. McNicholas, co-leader of Sidley Austin LLP’s global Privacy,
Data Security, and Information Law practice group, has an extensive practice
representing technologically sophisticated clients facing complex cybersecuri-
ty, privacy and data analysis challenges and related constitutional issues. Com-
mended by The Legal 500 US for his “deep knowledge of privacy and infor-
mation security,” he spearheads Sidley’s cybercrime focus and has significant
experience with litigation and counseling matters involving privacy and data
protection, cybercrime, cloud computing, the Internet of Things, data science,
and national security.

Sidley’s Privacy, Data Security, and Information Law practice was named
2014 Privacy Practice Group of the Year by Law360, and Mr. McNicholas is
frequently recognized as a leader in his field. In addition to his inclusion in The
Legal 500 US, he has been named in a Computerworld survey of “Best Privacy
Advisers” as one of the “Top 25 Privacy Experts” in the country and has been
included in The International Who’s Who of Internet, e-Commerce & Data Pro-
tection Lawyers 2011. Chambers USA has included him in its rankings of the
country’s Leading Lawyers since 2008 and notes that he “impresses sources
with his outstanding knowledge and responsive service . . . handling complex
privacy matters in his trial and appellate practice.” Chambers Global has rec-
ognized the global reach of Mr. McNicholas’s data protection practice since
2011. Chambers also has commended him in its nationwide litigation rankings
for e-discovery.

Mr. McNicholas frequently assists corporations with preparation for and re-
sponses to sophisticated cybersecurity incidents; and advises global companies
on cross-border data transfer, cloud computing issues, and complex policy issues
involving the Internet and information law. For example, his practice includes representing major retailers experiencing congressional, litigation, and investigative challenges after cybersecurity attacks including in Moyer v. Michaels Stores, Inc., 2014 WL 3511500 (N.D. Ill. 2014) and Frank v. The Neiman Marcus Group, No. 1:14-cv-233 (E.D.N.Y. 2014). He also advises on cutting-edge Internet governance issues as part of Sidley’s counsel to working groups for the Internet Corporation for Assigned Names and Numbers (ICANN) during the transition of the Internet Assigned Names Authority (IANA) function.

Vivek K. Mohan is an associate in Sidley Austin LLP’s Privacy, Data Security and Information Law practice group in the Washington, D.C. office. His practice focuses on technology related regulatory response and litigation, including privacy, cybersecurity, and information law issues. He counsels major technology, healthcare, industrial, and telecommunications companies on privacy and security program management, cyber incident response, surveillance and information sharing, and attendant global public policy considerations.

Mr. Mohan works with major technology and data-driven clients to respond to governmental inquiries relating to product development, “Big Data,” as well as to address national security and surveillance related issues. He represents clients in matters before government agencies including the FTC, SEC, FCC, state Attorneys General, Department of Homeland Security, and Department of Justice, as well as in private litigation.

Mr. Mohan has substantial experience with privacy and security issues confronting multinational corporations, including cloud computing, cross-border data flows, data localization, and data transfer agreements. He also has a particular focus on the emerging field of cybersecurity governance, regulation, and oversight, and serves as a key member on several high-profile internal investigations relating to cybersecurity incidents. He works with clients from the point an attack or breach is suspected through the process of incident response, including preparation for congressional testimony, response to government investigations, and associated litigation. He often serves as a technical liaison with forensic experts and internal information security personnel.

Mr. Mohan is a part of the Sidley team that advises working groups of the Internet Corporation for Assigned Names and Numbers (ICANN) on governance and accountability issues relating to the “stewardship transition” of the Internet Assigned Names Authority (IANA).
The rise of sophisticated cyber threats means that the task of managing cyber... Goodreads helps you keep track of books you want to read. Start by marking cybersecurity: A Practical Guide to the Law of Cyber Risk as Want to Read: Want to Read saving… Want to Read. While it requires commitment, developing a practical guide to cybersecurity for your firm need not be complicated or even all that expensive. In this report, we will outline some tools, services, and tips that even the smallest practice can use to prevent or mitigate an attack. But first, let us start with what has happened to most law firms: you have been breached. The breach itself is no longer the biggest risk companies face: it is the backlash from clients and customers if they find out that you had no plan to recover when the cyber event happens. In this section, we help you to craft a basic IRP to keep yourself and the firm’s reputation protected. Incident vs Breach. Cybersecurity: A Practical Guide to the Law of Cyber Risk provides a comprehensive discussion of the complex quilt of federal and state statutes, Executive Orders, regulations, contractual norms, and ambiguous tort duties that can apply to this crucial new area of the law. The guidance issued by the SEC interpreting existing disclosure rules to require registrants to disclose cybersecurity risks under certain circumstances; The varying roles of other regulators in sector-specific regulation, such as healthcare, energy, and transportation; and. In terms of mitigating cyber risk, the first step every organization should take is to implement the ISMS standard ISO/IEC 27001 and then commission an independent ISMS certification audit to ensure compliance with the requirements of ISO/IEC 27001. An ISMS certification will help organizations demonstrate their cyber-risk approach has considered local and international laws and regulations. ISO/IEC 27014, which offers support on the governance of information security, recommends such an approach. The two-part ISO/IEC 27035 presents principles of incident management and a complete guide to planning and preparing for incident response. 7. Don’t forget supplier relationships in your security strategy. IRM’s Cyber risk practical guidance. Our Cyber and Information Management Special Interest Group (SIG) conducted extensive research into the dynamic issue of cyber threats to business, governments and global enterprises. They have produced a practical guide for risk professionals and senior executives to help demystify the issue of cyber risk. Members of the group commented that “the true extent of the risk has yet to be assessed” and alone managed. The threat is very real. Risk professionals need to wake up and smell the coffee before it is too late.” Cyber risk: Nightmare or o