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*)

Practising Law Institute
1177 Avenue of the Americas
New York, NY 10036
#133898

- 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 organizations 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

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 cybersecurity, privacy and data analysis challenges and related constitutional issues. Commended by *The Legal 500 US* for his "deep knowledge of privacy and information 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 Protection 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 recognized 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 responses 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).

Cyber-attacks are an ever present and increasing risk, and there our global cyber team benefits from extensive experience across all lines of insurance business affected by cyber risk.Â We are a global law firm with 59 offices, associations and co-operations in jurisdictions that our clients need us most, including in the Americas, Asia Pacific, Europe and the Middle East. Where we are. Asia Pacific. A Practical Approach. Citi GPS: Global Perspectives & Solutions May 2019. Citi is one of the worldâ€™s largest financial institutions, operating in all major established and emerging markets.Â The risk of cyber attacks is most likely growing versus subsiding and having an intelligence-led approach will be critical to getting ahead of new threats. As an FBI agent recently said at a conference â€œThe goal is to avoid a massive loss either in a business line at a corporate or in a personal account because someone clicked on a dancing kitty.â€ Product details. Publisher : Practising Law Institute; 1st edition (September 7, 2015). Language : English. Loose Leaf : 562 pages.Â Dimensions : 7.67 x 1.54 x 9.84 inches. Best Sellers Rank: #5,039,127 in Books (See Top 100 in Books). #685 in Computer & Internet Law. #990 in Science & Technology Law (Books). #32,344 in Law (Books). Start reading Cybersecurity: A Practical Guide to the Law of Cyber Risk on your Kindle in under a minute. Don't have a Kindle? Get your Kindle here, or download a FREE Kindle Reading App. line banking, cyber health check, cyber incident response management, cybersecurity risk. management, cybersecurity schemes and services. Keywords: Cybersecurity, threats, risk, cyberwar, ISA, cyberspace, mobile securityÂ As indicated by this law the administration just utilize this mutual data to: Discover the motivation behind cybersecurity. Distinguish the reason for digital security risk or security helplessness.Â supportive to littler social orders. It sets up standards of the guide similarly as how comput-. erized hazard information should be shared, which HIMSS considers is to a great degree a. central steps to hint at enhancement advanced information to the private territory, including. Cyber risk is now a major threat to clientsâ€™ businesses, which face new exposures like damages, business interruption and regulatory consequences.Â Increasing interconnectivity, globalization and "commercialization" of cyber crime are driving greater frequency and severity of cyber incidents, including data breaches. Data privacy and protection is one of the key cyber risks and related legislation will toughen globally. More notifications of, and significant fines for, data breaches can be expected in future. Legislation has already become much tougher in the US, Hong Kong, Singapore and Australia, while the European Union is looking to agree pan-European data protection rules. Tougher guidelines on a country-by-country basis ca