Information Security: A Legal, Business, and Technical Handbook

Kimberly Keifer, Stephen Wu, Ben Wilson, and Randy Sabett
ABA Publishing, 2003
$59.95 (paper), 82 pp.
ISBN 1-59031-300-3

Reviewed by Nancy Tribbensee

Information Security: A Legal, Business, and Technical Handbook, published by the Information Security Committee of the American Bar Association Section of Science and Technology Law, is an excellent summary of legal, policy, and practice issues that will inform ongoing discussions of data protection and security, both for information technology professionals and other policy makers. The book has only 82 pages but outlines essential issues in a very accessible and readable format. It is very clearly written and uses nontechnical language throughout. It does not require an in-depth understanding of computer technology yet addresses sophisticated policy and legal issues at a level appropriate to any high-level institutional security policy review. It will assist policy makers, administrators, contract officers, and lawyers in managing risks, promoting regulatory compliance, and minimizing legal liability and financial costs associated with information security.

Accurate and complete information is essential to the operation of public and private institutions. Colleges, universities, and businesses need to protect the confidentiality and integrity of information they create and acquire. The importance of information security cannot be overstated. Information technology professionals are often aware of the need for security, as well as the vulnerability of systems and networks to threats, either from negligence or malice. Because they are familiar and comfortable with technology, technology professionals might be asked to take a leadership role in developing information security policy for their institutions. Although they are important stakeholders and essential resources, they cannot shoulder the responsibility for institutional information security alone. Other administrators and representatives of the campus or business also must participate—to recognize the benefits and limits of the technology; to gain an awareness of relevant federal and state laws and regulations; and to understand other circumstances that create compliance obligations to protect and regulate data security.

This second group of individuals often can provide a broad understanding of institutional history and culture and of the value of information and data to the essential mission of the campus or business—a perspective essential to developing effective security practices. Because some of these individuals might be uncomfortable with the technology, however, or might not feel competent discussing operational details of computer systems, networks, and data storage, they might not participate in important institutional dialogues about protecting the information that the institution receives and generates and on which it relies to achieve its goals.

This book will serve as a useful resource for technology professionals by relating security issues to statutory and regulatory compliance, liability, and risk management. It includes information on best practices and provides many excellent additional resources. The book also will be valuable to administrators and others with nontechnical backgrounds because it demonstrates that the analysis of compliance, liability, risk management, and practice issues is managed for information security in exactly the same way as it is for more familiar, nontechnical topics. The book provides nontechnical methods to assess, manage, and shift risks while protecting valuable university resources. Because it is equally accessible to multiple audiences, the book can reinforce the need for all members of the community to take active responsibility for some piece of the security puzzle.

This book includes eight chapters. The first two introduce the concept of information security and outline potential risks from intentional acts, inadvertent acts, and natural events. The third chapter outlines statutory and regulatory requirements, including the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act, the Sarbanes-Oxley Act, the Government Information Security Reform Act, and the Federal Information Security Management Act. This chapter also covers other sources of security obligations, such as operating rules and attorney-client privilege. Chapter 4 discusses sources of criminal, contract, negligence, and statutory liability.

Chapters 5–8 address best practices, responses to security incidents, and the need for risk management. These chapters also discuss the challenges that institutions face as they work toward these goals. The book includes very useful examples of standards, guidelines, and best practices in the areas of enterprise security, software development, systems and product security, disclosure of system vulnerabilities, electronic signatures, physical access controls, personnel control, and network and computer security.

One of the biggest obstacles to effective information security is the reluctance of many stakeholders to join the conversation and accept responsibility. Often this can be traced to feeling at once overwhelmed and intimidated by technical and voluminous detail. At times, the sentiment appears to be that because technology is evolving so quickly, it's easier to avoid the discussion than to try to keep up. This very helpful handbook supports a more productive alternative. It presents essential issues in a brief and nontechnical format that will support multidisciplinary efforts to promote information security. *e*

Nancy Tribbensee (trib@asu.edu) is Deputy General Counsel at Arizona State University.