UT LAW CLE | THE UNIVERSITY OF TEXAS SCHOOL OF LAW

PRESENTED AT

30th Annual Technology Law Conference

May 25-26, 2017
Austin, Texas

Addressing Director Responsibilities for Data Security

Thomas J. Smedinghoff

Addressing Director Responsibilities for Data Security

Thomas J. Smedinghoff[1]

Protecting the security of corporate data and information systems was once just a technical issue to be addressed by the IT department. Today, however, it has become a Board-level responsibility.

Digital information, systems, and communications are now critical to all businesses. Virtually all of a company's daily transactions and key records are created, used, communicated, and stored in electronic form using networked computer technology. Likewise, virtually all information that a company relies on to conduct its business, manage its finances, run its production machinery, and control its operational systems, is created and stored in digital form.

This corporate dependence on electronic records, digital processing, and a networked computer infrastructure introduces vulnerabilities that can lead to significant harm to the business and its stakeholders. As a consequence, it creates a major source of risk for most businesses – a risk for which corporate boards have oversight responsibility.

That risk is illustrated by the many recent cybersecurity incidents constantly in the news. In 2014, for example, the New York Times noted that:

> "In the last two years, breaches have hit the White House, the State Department, the top federal intelligence agency, the largest American bank, the top hospital operator, energy companies, retailers, and even the Postal Service. In nearly every case, by the time the victims noticed that hackers were inside their systems, their most sensitive government secrets, trade secrets and customer data had already left the building. …
>
> But the value [of stolen credit cards during this period] … which trade freely in underground criminal markets, is eclipsed by the value of the intellectual property that has been siphoned out of the United States corporations, universities and research groups by hackers in China – so much so that security experts now say there are only two types of companies left in the United States: those that have been hacked and those that do not yet know they have been hacked. …
>
> 'Most large organizations have come to the painful recognition that they are already in some state of break-in today.'"[2]

---

[1] Thomas J. Smedinghoff is Of Counsel in the Chicago office Locke Lord LLP, and a member of the firm's Privacy & Cybersecurity Practice Group. He is Chair of the ABA Identity Management Legal Task Force, Co-Chair of the Cybersecurity Subcommittee of the ABA Section of Business Law, Cyberspace Committee, and a member of the ABA Cybersecurity Legal Task Force. He is also a member of the U.S. Delegation to the United Nations Commission on International Trade Law ("UNCITRAL"), where he participated in the negotiation of the United Nations *Convention on the Use of Electronic Communications in International Contracts*. Mr. Smedinghoff is the co-editor of A GUIDE TO CYBERSECURITY DUE DILIGENCE IN M&A TRANSACTIONS (to be published by the ABA in June 2017), and author of the book titled INFORMATION SECURITY LAW: THE EMERGING STANDARD FOR CORPORATE COMPLIANCE, (2008). He can be reached at Tom.Smedinghoff@lockelord.com..

The subsequent high product profile security breaches experienced by Sony, Yahoo, the Democratic National Committee, and many others, only serves to further emphasize the pervasiveness and significance of these cyber risks.

As a consequence, implementing appropriate "data security" or "cybersecurity" measures has become a legal obligation for most businesses.[3] Moreover, applicable law generally recognizes that overall responsibility for compliance lies directly with the Board of Directors and senior management.

The obligations of all companies to protect the security of their own data are defined by a rapidly expanding patchwork of state, federal, and international laws, regulations, and government enforcement actions, as well as common law fiduciary duties and other implied obligations to provide "reasonable care."[4] At its essence, it's all about protecting the corporate stakeholders, be they shareholders, vendors, customers, or other third parties.

Moreover, such laws increasingly recognize that overall responsibility for fulfilling that obligation falls directly on the Board of Directors and senior management. Beginning in 2001, the role of the Board of Directors in the development and implementation of the information security program of financial institutions was explicitly recognized in financial sector regulations. In particular, the GLB regulations required that "the Board of Directors or an appropriate committee of the board" must:

- "Approve the institution's written information security program;" and
- "Oversee the development, implementation, and maintenance of the institution's information security program, including assigning specific responsibility for its implementation and reviewing reports from management."[5]

Thereafter, similar requirements have appeared in other data security laws, regulations, standards, and best practice documents. These include the recently approved regulations issued by the New York Department of Financial Services, which require that security "policies must be approved by a Senior Officer or the company's board of directors (or an appropriate committee thereof) or equivalent governing body,[6]" and the 2013 ISO 27001 information security management standard.[7]

---

[2] Nicole Perlroth, *Hacked vs. Hackers: Game On*, THE NEW YORK TIMES, December 3, 2014, pp. F-1 and F-7. This recap by *The New York Times* immediately preceded the disclosure of the North Korean attack on Sony Corporation in December 2014 and China's massive breach of the U.S. Government's Office of Personnel Management in 2015.

[3] See, e.g., Thomas J. Smedinghoff, "An Overview of Data Security Legal Requirements for All Business Sectors," (October, 2015), at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2671323

[4] Id.

[5] 12 CFR Part 364, Appendix B, III.A.

[6] New York Department of Financial Services Regs: 23 NYCRR 500.03 (effective March 1, 2017).

[7] ISO/IEC 27001:2013, *Information technology -- Security techniques -- Information security management systems – Requirements*.

Title search: Addressing Director Responsibilities for Data Security

First appeared as part of the conference materials for the
30th Annual Technology Law Conference session
"Cyber Security Governance—Addressing Emerging Expectations"