UT LAW CLE THE UNIVERSITY OF TEXAS SCHOOL OF LAW

PRESENTED AT

30th Annual Technology Law Conference

May 25-26, 2017
Austin, Texas

An Overview of Data Security Legal Requirements *for All Business Sectors*

Thomas J. Smedinghoff

An Overview of Data Security Legal Requirements *for All Business Sectors*

Thomas J. Smedinghoff[1]

TABLE OF CONTENTS

Page

[1] Thomas J. Smedinghoff is Of Counsel in the Privacy & Cybersecurity Practice Group at the law firm of Locke Lord LLP, in Chicago. He is a member of the ABA Cybersecurity Legal Task Force, and Chair of the Identity Management Legal Task Force and Co-Chair of the Cybersecurity Subcommittee of the ABA Section of Business Law, Cyberspace Committee. 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 a contributing author to the book: THE ABA CYBERSECURITY HANDBOOK - A RESOURCE FOR ATTORNEYS, LAW FIRMS & BUSINESS PROFESSIONALS (American Bar Association, 2013). He is also the author of the book titled INFORMATION SECURITY LAW: THE EMERGING STANDARD FOR CORPORATE COMPLIANCE, (2008). He can be reached at Tom.Smedinghoff@lockelord.com.

TABLE OF CONTENTS
(continued)

Page

An Overview of
Data Security Legal Requirements
for All Business Sectors

What are the data security legal obligations generally applicable to all U.S. businesses?

It is well known that certain sectors of the U.S. economy are subject to extensive regulations regarding data security. The most obvious examples are the financial sector,[2] the healthcare sector,[3] the federal government sector,[4] and the target of current regulatory efforts, the critical infrastructure sectors.[5] But what about companies in non-regulated sectors?

There is also no doubt that non-regulated businesses are subject to data security obligations. One need look no further than the last 10 years of FTC and state attorney general enforcement actions to see that numerous non-regulated companies have been targeted for failure to provide appropriate data security for their own corporate data. Examples include software vendors (Microsoft[6] and Guidance Software[7]), consumer electronics companies (Genica and Computer Geeks),[8] mobile app developers (Delta Airlines),[9] clothing retailers (Guess![10] and Life Is Good[11]), music retailers (Tower Records),[12] animal supply retailers (PetCo),[13] general merchandise retail stores (BJs Wholesale,[14] TJX companies,[15] and Sears[16]), shoe stores

---

[2] Subject to the Gramm-Leach-Bliley Act ("GLB"), Public Law 106-102, §§ 501 and 505(b), 15 U.S.C. §§ 6801, 6805, and implementing regulations at 12 C.F.R. Part 30, Appendix B (OCC), 12 C.F.R. Part 208, Appendix D (Federal Reserve System), 12 C.F.R. Part 364, Appendix B (FDIC), 12 C.F.R. Part 568 (Office of Thrift Supervision) and 16 C.F.R. Part 314 (FTC) (emphasis added).

[3] Subject to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), 42 U.S.C. 1320d-2 and 1320d-4, and HIPAA Security Regulations, 45 C.F.R. Part 164.

[4] Subject to the Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. Sections 3541-3549.

[5] See Presidential Executive Order, "Improving Critical Infrastructure Cybersecurity," February 12, 2013, at www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

[6] FTC V. Microsoft (Consent Decree, Aug. 7, 2002), *available at* www.ftc.gov/os/caselist/0123240/0123240.shtm

[7] In the Matter of Guidance Software (Agreement Containing Consent Order, FTC File No. 062 3057, November 16, 2006), available at www.ftc.gov/opa/2006/11/guidance.htm

[8] In the Matter of Genica Corporation, and Compgeeks.com, FTC File No. 082-3113 (Agreement Containing Consent Order, February 5, 2009), available at www.ftc.gov/os/caselist/0823113

[9] See, "California Attorney General Sues Delta Air Lines for Failing to Have a Mobile App Privacy Policy," at http://bit.ly/W11J4T

[10] In the matter of Guess?, Inc. (Agreement containing Consent Order, FTC File No. 022 3260, June 18, 2003), *available at* www.ftc.gov/os/2003/06/guessagree.htm

[11] In the Matter of Life is good, Inc. (Agreement Containing Consent Order, FTC File No. 072 3046, January 17, 2008), available at www.ftc.gov/os/caselist/0723046

[12] In the Matter of MTS, Inc., d/b/a Tower records/Books/Video (Agreement containing Consent Order, FTC File No. 032-3209, Apr. 21, 2004), *available at* www.ftc.gov/os/caselist/0323209/040421agree0323209.pdf

[13] In the Matter of Petco Animal Supplies, Inc. (Agreement containing Consent Order, FTC File No. 042 3153, Nov. 7, 2004), *available at* www.ftc.gov/os/caselist/0323221/0323221.htm

[14] In the Matter of BJ's Wholesale Club, Inc. (Agreement containing Consent Order, FTC File No. 042 3160, June 16, 2005), *available at* www.ftc.gov/opa/2005/06/bjswholesale.htm

[15] In The Matter of The TJX Companies, Inc., FTC File No. 072-3055 (Agreement Containing Consent Order, March 27, 2008), available at www.ftc.gov/os/caselist/0723055

[16] In the Matter of Sears Holdings Management Corporation, FTC File No. 082 3099 (Agreement Containing Consent Order, September 9, 2009), available at http://www.ftc.gov/os/caselist/0823099/index.shtm

(DSW),[17] restaurant and entertainment establishments (Dave & Busters[18] and Briar Group[19]), social media sites (Twitter[20] and Facebook[21]), bookstores (Barnes & Noble),[22] property management firms (Maloney Properties, Inc.),[23] and hotels (Wyndham).[24]

The thesis of this paper is that all businesses, whether regulated or not, are generally subject to legal duties regarding the security of their corporate data. Those duties can be summarized as: (1) a duty to protect the security of their corporate data, and (2) a duty to disclose security breaches when they occur. The following sections will explain the source and scope of those duties. But first we begin with a general overview of the concept of data security itself.

A. WHAT IS DATA SECURITY?

Security is the protection of assets (such as buildings, equipment, cargo, inventory, and in some cases, people) from threats. Data security (or information security) has been generally described as "the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities,"[25] and as "the process by which an organization protects and secures systems, media, and facilities that process and maintain information vital to its operations."[26]

The terms data security, information security and cybersecurity are often used interchangeably, although some might argue that each has a somewhat different emphasis. But regardless of the label, the focus is on the protection of both (1) *information systems*[27] -- i.e., computer systems, networks, and

---

[17] In the Matter of DSW Inc., (Agreement containing Consent Order, FTC File No. 052 3096, Dec. 1, 2005), *available at* www.ftc.gov/opa/2005/12/dsw.htm

[18] In the Matter of Dave & Buster's, Inc., FTC File No. 082 3153 (Agreement Containing Consent Order, March 25, 2010), available at http://www.ftc.gov/os/caselist/0823153/index.shtm

[19] See "Massachusetts Attorney General Breaking New Ground in Data Security Enforcement?" at http://bit.ly/15rGiz4.

[20] In the Matter of Twitter, Inc., FTC File No. 092 3093 (Agreement Containing Consent Order, June 24, 2010; Decision and Order, March 11, 2011), available at http://www.ftc.gov/os/caselist/0923093a/index.shtm

[21] In the Matter of Facebook, Inc., File No 092 3184 (Agreement Containing Consent Order, November 29, 2011), available at http://ftc.gov/os/caselist/0923184/index.shtm

[22] http://www.steptoe.com/assets/attachments/514.pdf

[23] See, "Massachusetts Attorney General Announces $15,000 Settlement with Property Management Firm" at http://bit.ly/GU8iNU.

[24] FTC v. Wyndham Worldwide Corporation, 2015 U.S. App. LEXIS 14839; 2015-2 Trade Cas. (CCH) P79,269 (3rd Cir. Aug. 24, 2015); FTC v. Wyndham Worldwide Corp., 2014 U.S. Dist. LEXIS 47622 (D. N.J., April 7, 2014). Complaint and other information at http://www.ftc.gov/opa/2012/06/wyndham.shtm).

[25] ISO/IEC 27002:2005, *Information Technology – Security Techniques – Code of Practice for Information Security Management* (June. 2005), at p. viii (hereinafter "ISO 27002").

[26] FFIEC, *IT Examinations Handbook – Information Security* (July 2006) at p. 1; available at http://ithandbook.ffiec.gov/it-booklets.aspx.

[27] The Homeland Security Act of 2002 defines the term "information system" to mean "any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information, and includes – (A) computers and computer networks; (B) ancillary equipment; (C) software, firmware, and related procedures; (D) services, including support services; and (E) related resources." Homeland Security Act of 2002, Pub. L. 107-296, at Section 1001(b), amending 44 U.S.C. § 3532(b)(4).

software, and (2) the *data, messages, and information* that are typically recorded on, processed by, communicated via, stored in, shared by, transmitted, or received from such information systems.[28]

Measures designed to protect the security of information systems and data are generally grouped into three categories, which are typically referred to as follows:

- **Physical security measures:** These are security measures which are designed to protect the tangible items that comprise the physical computer systems and networks that process, communicates, and store the data, including servers, devices used to access the system, storage devices, and the like. Examples include fences, walls, and other barriers; locks, safes, and vaults; armed guards; sensors and alarm bells.
- **Technical security measures:** These are security measures which involve the use of safeguards incorporated into computer hardware, software, and related devices. They are designed to ensure system availability, control access to systems and information, authenticate persons seeking access, protect the integrity of information communicated via and stored on the system, and ensure confidentiality where appropriate. Examples include: firewalls, intrusion detection software, access control software, antivirus software, passwords, PIN numbers, smart cards, biometric tokens, and encryption processes.
- **Administrative security measures:** Sometimes referred to as "procedural" or "organizational" security measures, these are security measures which consist of management procedures and constraints, operational procedures, accountability procedures, policies, and supplemental administrative controls to prevent unauthorized access and to provide an acceptable level of protection for computing resources and data. Administrative security procedures frequently include personnel management, employee use policies, training, and discipline.

Within each of these three categories, security measures are further classified as preventative, detective, or reactive. *Preventative* security measures are designed to prevent the occurrence of events that compromise security. An example of a preventative security measure is a lock on a door (to prevent access to a room containing computer equipment), or a firewall (to prevent unauthorized online access to a computer system). *Detective* security measures are designed to identify security breaches after they have occurred. An example of a detective security measure is a smoke alarm (which is designed to detect a fire), or intrusion detection software (which is designed to detect and track unauthorized online access to a computer system). *Reactive* security measures are designed to respond to a security breach, and typically include efforts to stop or contain the breach, identify the party or parties involved, and allow recovery of information that is lost or damaged. An example of reactive security is calling the police after an alarm detects that a burglary is in process, or shutting down a computer system after intrusion detection software determines that an unauthorized user has obtained access to the system.

The objectives to be achieved through the use of security measures can be defined in terms of either the positive results to be achieved or the negative consequences to be avoided. The positive results to be achieved are typically described as (1) ensuring the *availability* of systems and information, (2) controlling *access* to systems and information, and (3) ensuring the *confidentiality, integrity, authenticity*

[28] The *data, messages, and information* to be protected potentially includes a wide variety of data, such as personally identifiable information about employees, customers, prospects, and other individuals; corporate financial information, information regarding corporate business transactions, trade secrets and other confidential information, information relating to corporate communications, including e-mail, and a variety of other types of corporate data. It can also take a variety of forms, including data, messages, documents, voice recordings, images, video, software, and other content in both electronic and paper form.

Title search: An Overview of Data Security Legal Requirements for All Business Sectors

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