# Data (In)Security: Is Your Company Protected?

## Introduction

The privacy and security of private information first became an area of concern in the 1960s and 1970s with military-based security data. However, the emergence of the Internet has resulted in widespread abuse and theft of personal information. Until the 1990s legislative regulation was limited to sector-specific regulation. However, with the rise in security breaches over the past ten years, the United States has implemented a number of federally-based security protection laws, with state-mandated regulations proliferating since 2008.

Even a moderate breach can cost a company millions of dollars in litigation, settlement fees, compliance costs, and fines imposed by state regulatory agencies. Customers, company shareholders, vendors, and other business partners may file class action lawsuits. Even more costly (and more difficult to quantify) is the loss of public goodwill toward the firm arising from a breach of data security.

## Consider this recent case history:

### TJX Data Breach

Framingham, Mass.-based TJX owns and operates over 2500 retail outlets, including T.J. Maxx, Marshalls, and Bob's Stores. In a 2007 filing with the Security and Exchange Commission, TJX disclosed that in 2005 an unknown intruder(s) illegally accessed one of the company's payment systems and stole the credit and debit card information of 94 million customers across the U.S. Canada, Puerto Rico, as well as the U.K. and Ireland over an 18-month period. This made the TJX breach the worst up until that time in terms of compromising consumer personal information. At the time of the filing, the company was attempting to contact all customers to notify them of the breach.

In June of 2009, TJX announced that it agreed to pay $9.75 million to settle investigations by forty-one states attorneys general who were examining the company's data security policies and practices. Under the agreement, TJC will pay 45.5 million in settlement fees, plus 41.75 million to cover the fees associated with the investigations. Additionally, the company agreed to

contribute $2.5 million toward the creation of a Data Security Fund that states will use to create number of security-related initiatives such as developing best practice models, new legislations, and establishing consumer information and outreach programs.

**Health Net**

In June 2010, the Connecticut Attorney General launched an investigation when Health Net, an insurance provider, lost a computer drive that contained unencrypted health information, such as claim forms affecting 1.5. million plan members (about one-third of whom, resided in Connecticut). The company reached a settlement agreement for violation of HIPPA regulations under the **Health Information Technology for Economic and Clinical Health Act** (HITECH Act). In the settlement, Health Net agreed to pay $250,000 to the state, offer two years of credit monitoring to affected plan members, purchase $1 million identify theft insurance, and reimburse plan members for security freezes. An additional $500,000 be paid by the company in the event the information is used for fraudulent purposes.

**Epsilon Interactive**

In what industry experts say may be the largest breach of personal security ever recorded, Epsilon Interactive, a Texas-based database services company for such firms as Capital One, Citigroup, Chase, Marriott, Target, Best Buy, and Walgreen announced that on March 30, 2011, customer information was retrieved by unauthorized access into the company's email system, thereby exposing customers to spam and possible phishing attacks..

Epsilon has claimed that the information stolen was limited to email addresses and customer names only. A rigorous review determined that no other customer data was exposed in the breach. A full investigation is currently underway.

According to privacyrights.org, there have been more than 500 million breaches from 2005-2010 (last reported in August 2010) in the United States involving records containing sensitive consumer information. Unfortunately, consumers are unable to take the necessary steps to protect their information from a data breach. It is up to *organizations to ensure that necessary precautions are in place to protect the privacy and security of personal data.*

## Here come the regulators

### Federal Legislation

The United States does not have a comprehensive data security law. Rather, there are several laws that address specific situations, such as with regard to healthcare information (**HIPPA**), **Gramm-Leach-Bililey (GLB)** for financial data, the **Fair Credit reporting Act** for credit information, and the information obtained from children (the **Children's Online Privacy Protection Act**). Another federal law that involves data protection and security is the **Electronic Communications Privacy Act** that has to do primarily with government surveillance but also includes provisions regarding access to privately stored information by unauthorized third parties. There is also the **Computer Fraud and Abuse Act** which prohibits access to computer-based information without prior authorization for the purpose of obtaining private information. The Computer Fraud and Abuse Act also prohibits someone from knowingly accessing private information with the intent to defraud.

New legislation is emerging on a daily basis. The recently enacted, "Red Flag Rule," part of the **Fair and Accurate Credit Transactions (FACT) Act of 2003** requires creditors and financial organizations to "provide for the identification detection and response to patterns, practices, or specific activities – known as 'red flags'—that could indicate identify theft." Every *known* violation will result in $2500. Fines. Exempted from the Red Flag rule are such professionals as doctors, dentists, lawyers, and accountants.

Lastly, to illustrate the breadth of data security legislation, even the **American Recovery & Reinvestment Act (ARRA) of 2009** (aka the Stimulus Act) required additional data breach notification policies for certain types of organizations that store sensitive customer information (e.g., financial and banking institutions).

On April 12, 2011, U.S. Senators John Kerry (D-MA) and John McCain (R-AZ) introduced the **Commercial Privacy Bill of Rights Act of 2011** (the "Act") "to establish a regulatory framework for the comprehensive protection for individuals under the aegis of the Federal Trade

Commission." The bill will be applied to all commercial businesses that "collect, use, transfer or store the covered information" of greater than 5000 people over a consecutive 12-month period.

Certain provisions of the bill would direct the FTC to guide regulatory proceedings within certain periods, but the bill also imposes mandates directly on companies themselves.

**State-based legislation**

State-based data privacy legislation has become quiet onerous over the past several years arising primarily from the breaches at TJX and Epsilon. California was the first state to pass legislation in 2008. However, the model for future legislation came from the state of Massachusetts where TJX is based. The Massachusetts Law titled, *"Standards for Protection of Personal Information of Residents of the Commonwealth"* (Chapter 93H) created a comprehensive set of data security requirements for business, including the development and continual oversight of a "comprehensive "written information security program" (WISP). The scope of the Massachusetts regulation is broader than any other existing federal or state law and requires public disclosure of a data security breaches and provides for the implementation of security freezes to prevent further intrusion. It also requires that WISP includes a process for how it will oversee all its vendors and partners who have access to the company's confidential data, including customer non-public information in providing services to the firm. Finally, all companies subject to the regulations are required to maintain various computer security protocols for storage and transmittal of personal data, along with installation of anti-virus software; employer-led training in how to properly use the computer security system.

**Regulations in other States[2]**

As of February 2011, 46 states as well as the District of Columbia have also passed breach notification legislation, and a large number of states also have laws that require the protection of their residents' private information.

On January 1, 2010, *Nevada's* new identify theft law, S.B. 227, went into effect. Among other requirements (such as mandating compliance with the PCI Data Security Standards for all credit card transactions), S.B. 227 specifically requires the 'encryption" of all personal data leaving the

"logical or physical control of the data collector," including electronic data on a "data storage device." As with the Massachusetts legislation, the Nevada law applies to business entities doing business with any residents of the state, whether or not the business is incorporated there.

*Nevada* and *Maryland* require that contracts between entities and third-party providers who disclose the personal information of state residents must include a stipulation requiring the party to whom the information is disclosed implement safety measures to protect the privacy of the person.

**California:** The California regulations stipulate that any business or license that owns or licenses personal data regarding a resident of California must:

> *implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.*

Personal Information to include when the information is not encrypted or redacted:

- Individual's first and last name or first initial and last name
- Social security number
- Driver's license number
- Credit or debit card account numbers in combination with security access code or password.
- Medical information

*Of particular note is that there is also a 5-hour window for notification of security breaches.* In effect, firms are required to publicly disclose that a security breach has occurred within 5 hours of the breach.

Protections for medical information are also in place in *Arkansas*, but that information is not covered to the same extent as the regulations in Massachusetts. *Illinois* requires safety measures for biometric data, a requirement also not covered by the regulations in Massachusetts.

**Oregon.** Oregon's Consumer Identify Theft Protection Act incorporates safety measures that are similar to those of the Massachusetts legislation, with some forbearance for small businesses (manufacturing firms with less than 200 employees) and other types of businesses with less than 50 employees. An important requirement is that firms implement an "information security program" (i.e., WISP) that contains administrative, technical, and physical safety measures (the same stipulation as in the Massachusetts regulations).

**Connecticut.** Without stipulating specific safety measures, Connecticut requires that any person or business that is in possession of confidential information of another person to:

> *Safeguard the data, computer files and documents containing the information from misuse by third parties, and [ ] destroy, erase, or make unreadable such data, computer files, and documents prior to disposal.*

"Personal information" includes social security number, driver's license or state ID numbers, a credit or debit card number, a passport number, alien registration number, or health insurance plan number.

Connecticut regulations also require that businesses and licensees notify appropriate government authorities and affected parties of the security breach as "soon as the incident is identified, but *no later than five (5) calendar days after the incident is identified."*

Similar regulations passed in other states, including *Arkansas, North Carolina, Rhode Island, Texas,* and *Utah.*

**The Cost of Data Security[3]**

Data security breaches can result in significant costs for a company and not only in terms of monetary loss. These costs include:

- The costs associated with disclosing the breach to government officials and the public at large. This can average $30. To $150. per notice (times 40 million notices and you begin to get a sense of the fiscal impact).

- Credit monitoring services for affected parties—usually a public relations gesture to restore company good will.
- ID theft insurance coverage
- Litigation expenses include the cost of retaining an attorney and settlement fees.
- Costs associated with assessment of damage and reparation of compromised security systems.
- Maintaining compliance with state regulations
- Fines for security violations (e.g., HIPAA, GLBA, FRCA)
- Loss of company reputation and trust can have a significant impact on future earnings.

**Data Security for Small and Mid-Size Firms**

Considering the recent spate of regulation, it is no longer sufficient for company executives to pass on the task of data security to ensure that the privacy of sensitive is maintained. The recent wave of state-based regulations necessitates that organizations of all sizes implement a companywide effort to ensure that the privacy of sensitive data is maintained.

Specific samples of regulation directed an enhancing the confidentiality of personal information include:[4]

- **Social Security numbers. The written** policy requirement regarding the privacy of Social Security numbers is in effect in *New York, Connecticut, New Jersey, and Michigan*.
- **Comprehensive Data Security Program Requirements.** Regulations require the creation of either comprehensive plans or WISPs that contain information regarding the administrative, physical, technical and safety measures implemented by a company with regard to data security and integrity in each of the 46 states. WISPs in *Massachusetts, Maryland, Nevada, New Jersey, and Oregon.*

- **Encryption Mandates.** Data encryption requirements in *Massachusetts and Nevada*.

- **Breach Notification requirements.** Data breach notification requirements in all 46 states.

- **Job Applicant Information**. Specific protections are in effect in *Utah* with regard to personal information on job applications.

- **Red Flag Regulations.** Federal "Red Flag" regulations for businesses that are financial institutions or creditors. As of this writing, lawyers, doctors, dentists, and accountants are exempted from this regulation.

- **HIPPA Regulations.** Privacy protection under the Health Insurance Portability and Accountability Act of 1996 (HIPPA) for company-based health plans and covered health care providers, including on-site medical services. As of February 2010, many of the requirements also apply to insurance brokers, third party plan administrators, and electronic storage firms, etc.

- **Federal Contractor Requirements**. Federal contractors are subject to the same federal laws, regulations, and standards as the agencies which they serve.

- **PCI Standards.** Some companies that process credit card payments or receive payment for products and services by credit or debit card may need to comply with the Payment Card Industry (PCI) Data Security Standards (https://www.pcisecuritystandards.org/).

- **International Standards.** Those companies with branches or associates in the European Union (EU) may have difficulty in exchanging personal information with their counterparts due to the stringent regulations in these countries. As one example, in July 2009, the UK's Financial Services Authority (FSA) fined three HSBC Holding companies a total of £3 million ($4.9 million) for not adequately protecting customers' confidential information. This was the highest fine ever imposed by the FSA for a data security breach.

Overall, these protections seek to protect the "personal information of various stakeholders: employees, customers, business partners. Personal information typically includes: 1) first and last

name, 2) social security number; 3) driver's license number or state issued ID; 4) credit and/or debit card number, and 5) medical information. As noted, some states (e.g., Connecticut) have expanded this definition to include passport numbers and alien registration numbers.

For a listing of what constitutes "personal information" in all states that have implemented regulation, visit:
http://www.aicpa.org/INTERESTAREAS/INFORMATIONTECHNOLOGY/RESOURCES/PRIVACY/FEDERALSTATEANDOTHERPROFESSIONALREGULATIONS/Pages/default.aspx

**Managing the regulatory challenge: Prevention is the best strategy**

Considering the wave of regulations and their specificity with regard to each state small and medium size firms must assess their risks regarding established safety measures in storing and transmitting personal information. They must examine how personal information is stored, retrieved, disclosed, and destroyed. The process, known as "risk assessment," is critical to understanding the types of personal information the company compiles and what protections need to be implemented. When performed correctly, the risk assessment process enables a business to develop a comprehensive policy and procedure plan that will sufficiently address all the risks identified.

**Call to Action**

-----Associates can offer your company the help your firm needs. With the assistance of data security industry experts, a thorough risk assessment can be developed that will ensure your business complies with required mandates and is able to ride the regulatory storm successfully in terms of both continued financial viability and reputational integrity.

***References***


1. www.wlf.org/publishing/publication_detail.asp?id=2172

2. http://www.workplaceprivacyreport.com/2010/03/articles/data-security/wisps-beyond-ma

3. http://www.zurichna.com/internet/zna/SiteCollectionDocuments/en/media/whitepapers/DOCo
l d2DataSecurity082609.pdf

4. www.law360.com/.../**data-security**-a-**primer**-for-the-**midsize-company**