DATA SECURITY

May 2015

IREM® Legislative White Paper

IREM Institute of Real Estate Management

IREM® Headquarters
430 North Michigan Avenue
Chicago, IL 60611-4090
www.irem.org

Phone (800) 837-0706
(312) 329-6000
Fax (800) 338-4736
E-mail custserv@irem.org

As technology has evolved and become vital for businesses, a growing number of public and private entities that keep and maintain personal information, such as personal financial account information, have become victims of security breaches. These breaches have exposed fundamental security flaws in the way that companies handle consumers' personal information. Individual privacy has been compromised and these breaches have put consumers at an elevated risk of becoming victims of identity theft.

The number of Congressional proposals to counteract identity theft multiplied in the spring of 2005 after ChoicePoint Inc, a commercial data broker, announced that February it may have improperly sold the personal information of almost 163,000 individuals. ChoicePoint was consequently investigated by the Federal Trade Commission. In January, 2006, the company agreed to pay $15 million to settle charges it violated consumer privacy rights, but did not admit any wrongdoing.

Then, the substantial security breach at the U.S. Department of Veterans Affairs (VA) on May 3, 2006—widely publicized by the media—triggered more legislators on Capitol Hill to introduce data security legislation. The laptop and external disk drive, containing information on 26.5 million veterans and 1.2 million active duty personnel, of a VA employee were stolen from the employee's residence. The Secretary of the VA was not informed of the breach until May 16 and the public was not informed until May 23. The VA breach prompted Congress to narrow their focus as to when the public should be notified if sensitive data is lost or stolen.

Several House and Senate committees engaged in creating data security legislation since the major security breach in 2006. . The Senate Judiciary Committee, Senate Commerce Committee, House Energy and Commerce Committee, and House Financial Services Committee each held mark-ups and passed legislation. The House and Senate worked to find compromise between varying proposals.

Legislative proposals primarily addressed jurisdictional authority, procedures to be followed by businesses when clients' sensitive personal information is stolen, or when businesses should notify their clients.

In December, 2009 the "Data Accountability and Trust Act" passed the U.S. House and would require any organization that experiences a breach of electronic data containing personal information to notify all U.S. individuals whose information is breached. The law requires that the Federal Trade Commission to also be notified. In addition, organizations would be required to designate an information security officer and establish a data security policy. The policy would have to address the collection of personal information and include a process for identifying and correcting system vulnerabilities and disposing electronic data. The bill died and was re-introduced as H.R. 1707 in the 112th Congress on May 4, 2011. The bill was then referred to the Subcommittee on Commerce, Manufacturing, and Trade.

In the spring of 2010, IREM became aware of a change in how credit reporting agencies interact with property managers and other businesses and professionals. Credit reporting agencies may begin to enforce on-site visual inspections by a third party of the business premises of each subscriber or headquarters location of the subscriber (property management company in this

case). The third party would need to verify the business is legitimate, that they have permissible purpose to order the reports and they are storing the reports securely and destroying any unnecessary reports. Best practices include having a lockable filing cabinet, a shredder, and a password protected computer (depending on how the company receives their reports).

This new guideline came out of a civil suit filed against ChoicePoint by the United States Attorney General on behalf of the Federal Trade Commission. The court's decision detailed that organizations requesting credit checks for business purposes are required to have on-site visual inspections conducted by an independent third party at the client's expense. The court made this decision in connection with the Fair Credit Reporting Act (FCRA). It is important to note that this new rule is not in the FCRA, but instead an interpretation by the court in response to the lawsuit. Although the on-site inspections are not required by the FCRA, it is probable that most credit reporting organizations will require them in order to be in compliance.

Since the ChoicePoint Inc. security breach, there have been a handful of other breaches of great magnitude. In March of 2008, Heartland Payment Systems experienced a breach that exposed 134 million credit cards. A federal grand jury indicted Albert Gonzalez and two unnamed Russian accomplices in 2009 who were responsible for the data breach. Similarly, in March of 2011, Epsilon inadvertently exposed the names and e-mails of millions of customers stored in more than 108 retail stores as well as numerous large and influential financial firms like CitiGroup Inc. and the non-profit educational organization, College Board. Shortly after in April of 2011, another vast security breach occurred. Sony's PlayStation Network experienced a major breach where 77 million PlayStation Network accounts hacked. The company allegedly lost millions of dollars while the website was down for a month.

The frequency and magnitude of data breaches has increased dramatically in recent years. According to a study by the Ponemon Institute, 43% of companies experienced a data breach in 2014. Among those, a breach at JP Morgan Chase compromised the account information of 76 million households. Another breach at eBay compromised the account information of all 145 million users.

IREM Position

IREM has identified two main concerns with data security and consumer notification legislation. First, those bills that contain specific provisions and mechanisms that trigger notifying the consumer of a security breach, and IREM is concerned with assuring the reasonableness of the trigger mechanism and notification process. Second, the costs of compliance with state and/or federal laws would be of major concern to property managers, thus pointing to the reasonableness thresholds above referenced. IREM encourages Congress to approve legislation which is not onerous on property owners and managers or their clients. Small businesses should not be liable for the negligent acts of third parties unless contributory negligence exists.

IREM strongly encourages its members to use best practices protect the confidential personal information of their clients.

Federal Proposals

Data security is an increasingly important matter in this day in age where virtually all business is or can be conducted using the Internet. Over the past seven years, Congress has received pressure to legislate data security. With seemingly never-ending occurrences of data security breaches in major corporations, universities, and government agencies, privacy is an utmost important rule in today's climate. Federal lawmakers have worked to create legal protections that would protect citizens against such security malfunctions.

In February, 2012, the White House released a a Consumer Privacy Bill of Rightsin which is intended as the blueprints for future legislation in Congress. The rights "give consumers clear guidance on what they should expect from those who handle their personal data." The document encouraged privacy advocates, consumer protection enforcement agencies, and other groups and individuals to implement the principles.

In February of 2015, the Obama Administration reintroduced a discussion draft of the Consumer Privacy Bill of Rights. The intended purpose of the document is to:

> "Establish baseline protection for individual privacy in the commercial arena and to foster timely, flexible implementations of these protections through enforceable codes of conduct by diverse stakeholders.

The Consumer Privacy Bill of Rights, like the Data Security and Breach Notification Act, seeks to address the patchwork of state laws regarding data security. The provisions in the proposal (along with the Data Security and Breach Notification Act) would preempt any statute, regulation, or rule of state or local laws.

The Draft defines personal data as any data that are under the control of a covered entity, and can be linked to by the covered entity to a specific individual, or linked to a device used by an individual.

The draft is meant to start a discussion with Congress about the issue of data security, and is considered a companion to the Data Security and Breach Notification Act of 2015.

Legislative proposals around the nation

As of January 2015, forty-seven states, the District of Columbia, Puerto Rico, and the Virgin Islands have state statutes requiring entities to notify individuals and groups in the case of a security breach involving information. To see the entire list of statutes, please see this link.

See the attached chart "Data Security Legislation in the 114th Congress" below

Data Security Legislation in the 114th Congress

Bill Number and Title	Cosponsor(s)	Status of Bill in 114th Congress	Applies To	Summary of Legislation	Mandated Security Programs:
H.R.1121 - "Cyber Privacy Fortification Act of 2015"	Rep. John Conyers Rep. Henry Johnson, Jr.	Pending. Referred to Subcommittee on Crime, Terrorism, Homeland Security, And Investigations	Federal Agencies	Amends the federal criminal code to provide criminal penalties for intentional failures to provide required notices of a security breach involving sensitive personally identifiable information. Defines "sensitive personally identifiable information" to mean specified electronic or digital information.	Requires federal agencies as part of their rulemaking process to prepare and make available to the public privacy impact assessments that describe the impact of certain proposed and final agency rules on the privacy of individuals. Directs federal agencies to periodically review promulgated rules that have a significant privacy impact on individuals or a privacy impact on a substantial number of individuals. Requires agencies to consider whether each such rule can be amended or rescinded in a manner that minimizes any such impact while remaining in accordance with applicable statutes.
S. 177 – "Data Security and Breach Notification Act of 2015" and H.R. 1770	Sen. Bill Nelson, Sen. Richard Blumenthal, Rep. Peter Welch, Rep. Michael Burgess, Rep. Fred Upton	Pending. Referred to the Committee on Commerce, Science, and Transportation	Sole proprietorship, corporation, trust, estate, cooperative, association, or other commercial entity, and any charitable, educational, or nonprofit organization	Requires covered entities to establish and implement policies and procedures regarding information security practices for the treatment and protection of personal information	Must notify individual, Secret Service, or FBI of breach
H.R. 1560 – "Protecting Cyber Networks Act"	Reps. Adam Schiff, Lynn Westmoreland, James Himes, Peter King, Frank LoBiondo, Terri Sewell, Mike Quigley, Patrick Murphy	Passed House April 22nd. Pending in Senate.	Federal Agencies	To improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, to amend the Homeland Security Act of 2002 to enhance multi-directional sharing of information related to cybersecurity risks and strengthen privacy and civil liberties protections, and for other purposes.	The Director of National Intelligence shall develop procedures to share cyber threat indicators in the possession of the federal government with relevant non-federal entities