Data Security Breaches:
Are Your Human Resources Policies Equipped to Avoid and/or Repair the Damage?

By Daniel Klein, Esq.

INTRODUCTION

Imagine discovering at the end of the day that your wallet is missing. Your driver's license, credit cards and other personal information are gone — stolen by someone who may use your information for any number of illicit purposes. Anyone who has experienced such a loss knows how burdensome it is to repair the damage — it can take days or weeks filled with paperwork and telephone calls to banks, credit agencies, credit card companies and others. Now imagine that you are the information technology manager at a large company, and you just discovered that the "wallets" of your entire workforce were stolen by someone — possibly even an employee — who broke into your computer system, gaining access to personnel records, private information and other data.

Such was the problem faced by executives at Pfizer, Inc. after it discovered that a former employee had hacked into the company's computer system and stolen the personal information — including names, social security numbers, addresses, credit card and financial information and other data — of more than 17,000 employees. Six months later, the company is still trying to sort out the mess and help employees recover their stolen identities.

©www.iStockphoto/Emrah Turudu

Given the increasing sophistication of cyber thieves and the prominence of identity theft schemes, preventing or limiting the scope of such data disasters has become a top priority for many employers. However, the risk does not come solely from high-tech hackers bent on stealing thousands of records at one time. A lost BlackBerry, a lax record retention policy, or even a lack of attention to what gets thrown out in the trash each can expose an employer to a data security breach. Because personnel information is often a target of cyber thieves, human resources professionals need to know the best ways to both protect information about their employees and to comply with the various state laws that now exist to combat the problem.

In October 2007, Massachusetts became the 39th state to implement a data security law, joining every state except for Alaska, Alabama, Iowa, Kentucky, Mississippi, Missouri, New Mexico, South Carolina, South Dakota, Virginia and West Virginia, to enact a statute concerning the security and disposal of the personal information of state residents. Although the Massachusetts law is not specifically targeted toward employers or

limited to personnel information, the statute clearly affects employers and the personnel files they maintain. While each state's data security law creates specific legal requirements for data and record retention and disposal programs, the Massachusetts law is particularly burdensome. Moreover, proposed regulations drafted by the Massachusetts Office of Consumer Affairs and Business Regulations would further impact information security practices, human resources policies and training obligations for employers. This article focuses on how the law and proposed regulations impact human resources policies for any employer handling the personal information of Massachusetts residents, as well as data security policies for employers as a whole.

THE MASSACHUSETTS DATA SECURITY LAW AND PROPOSED REGULATIONS

The Massachusetts law has two components that impact employers: Chapter 93H became effective on Oct. 31 and requires notification to the resident-victims and state authorities if "personal information," as defined by the statute, is improperly accessed or used; Chapter 93I became effective on Feb. 3 and mandates destruction of hard copy and electronic data containing personal information of Massachusetts residents. This law impacts any company that collects, maintains or owns personal information of Massachusetts residents without regard to the location of the company's place of business. Therefore, employers in neighboring states that employ Massachusetts residents or that have Massachusetts branches must comply with the law with respect to those employees, even if personnel records and other data are maintained elsewhere.

While the Massachusetts act is modeled after other state data security statutes, this law imposes more significant burdens than those in other jurisdictions. For example, Massachusetts requires companies and employers to notify victims whenever there is a breach of security for data maintained in either an electronic or hard copy format. Only four other states require notification of such "paper breaches." For example, a manager who takes home a box of personnel files to review over the weekend could be putting the company at risk if those files get lost or stolen. The law also defines "personal information" broadly. Most states define the term to include an individual's first and last name plus either social security number, driver's license number or financial account information along with the activating PIN; Massachusetts does not require the inclusion of a PIN before it deems a name plus financial account

information to constitute "personal information." Additionally, upon a breach, the law requires companies to notify the Massachusetts residents as well as two state authorities; whereas most states do not require authorities to be notified. The law sets stringent minimum requirements for the destruction of personal data as well, including the requirement that any document or other media containing personal information be destroyed so completely that reconstruction is impossible.

Employers may be even more concerned with proposed regulations drafted by the Massachusetts Office of Consumer Affairs and Business Regulations, which would dramatically impact information security practice, human resources policies and training obligations, essentially codifying certain best practices as law. The public comment period on the proposed regulations closed in late January 2008. If the regulations are enacted as written, companies will be required to, among other things:

- implement a comprehensive information security program, including internal policies and procedures on the handling of personal information;
- designate an employee in charge of security;
- conduct an internal and external risk assessment relating to the collection, storage and use of personal data held by the company;
- implement and monitor employee data security training;
- monitor employee compliance with policies and procedures;
- analyze and upgrade, if necessary, computer/information systems;
- develop a telecommuting policy pertaining to data access and storage;
- impose disciplinary measures for violations of program rules;
- prevent terminated employees from accessing records;
- take reasonable steps to verify that service providers treat data appropriately, including conducting security due diligence, and obtaining written certification that the service provider has a written security program;
- collect, use and retain personal information for the minimum necessary legitimate business purpose;
- inventory records containing personal information;
- regularly monitor and audit employee access to personal information to prevent unauthorized use and access;
- conduct a review of security issues at least annually or if there are material changes in business practices;
- document all actions relating to security breaches;
- implement specific computer system security requirements, including user authentication controls, access controls, encryption, monitoring, audit trails, firewalls, security agent, and antivirus software;
- educate and train on proper use of the computer security system;
- prepare written procedures restricting physical access to personal information; and
- implement mandatory review of the integrity of computer records when there is an unauthorized entry into a secure area.

THE PRACTICAL IMPACT ON EMPLOYERS

What does this mean for employers? From a practical perspective, any employer who employs Massachusetts residents will likely prefer to apply the state's rigorous requirements to its entire workforce rather than maintain one information security program for Massachusetts residents and another for non-Massachusetts residents. For employers with data security programs already in place, the Massachusetts law effectively codifies certain best practices into law. Employers that have not yet implemented data security policies will need to implement a compliant process in short order. The Massachusetts requirements provide a good, albeit comprehensive, template for any employer's data security program. The Federal Trade Commission also has published a guide to data security for employers, located at **www.ftc.gov/bcp/edu/pubs/business/privacy/bus69.pdf**, which breaks down the process into five basic steps:

Given the increasing sophistication of cyber thieves and the prominence of identity theft schemes, preventing or limiting the scope of such data disasters has become a top priority for many employers.

1. **Know what you have.** Is your personnel information kept in a single, central location or more than one site? What does the information consist of? Is there more than one copy of information?

2. **Scale down your data** to only what your organization needs to function, and what it must retain for legal purposes.

3. **Lock it.** Employ stringent data security protection practices, both electronic and practical. For example, encryption of personal information can be a safe harbor to the need to provide notice of a data security breach under all state notice laws including Massachusetts. Limit the physical access to personnel information to those with a "need to know"; keep files locked and passwords secret.

4. **Pitch it.** Employ proper data destruction practices. Do not get caught merely dumping old files in the trash.

5. **Plan ahead for a breach.** Does your organization have a plan to comply with the law in the case of a data security breach? What steps will it take to notify individuals and authorities and work to repair the damage from the breach itself?

EMPLOYER NOTICE UPON A DATA SECURITY BREACH

Even the best data security policies can sometimes fail, and employers need to be prepared to communicate with employees who will understandably be angry, worried and confused about the theft of their personal information. Under Massachusetts law, as part of the required notice of a data security breach, victims must be informed of their right to obtain a police report about the incident and their right to institute a security freeze on their credit and other information. In addition to providing a basic notice of employees' rights, employers in any state should use the notification as a means to reassure employees that the employer is taking all possible steps to rectify the problem. Some suggestions for the notice include:

- providing basic information about what happened and the nature of the information taken;
- describing the steps the employer and/or authorities are taking to rectify the problem, stop the release of information and reestablish the security of employees' personal data; and
- listing the ways that both the employer will help the employees (such as through the hiring of a free credit restoration service) and the employees can help themselves (such as information for obtaining free credit reports).

COMPARISON TO THE DATA SECURITY LAWS OF OTHER NEW ENGLAND STATES

Employers located in neighboring states should be familiar with the Massachusetts data security law because of the likelihood that they will employ a Massachusetts resident. Of course, employers also must comply with the data security laws of other states of which they employ residents, some of which have their own unique attributes:

- **Connecticut** — Conn. Gen. Stat. 36a-701(b): While a majority of states require unauthorized acquisition of personal information in order to trigger a data security breach, Connecticut only requires

unauthorized access. For example, under Connecticut law, a hacker who breaks into a computer system merely to view employees' records online engages in a data security breach.

- **Vermont** — Vt. Stat. tit. 9 § 2430 et. seq.: Like Connecticut and Massachusetts, Vermont requires only unauthorized access of data to constitute a security breach.
- **Rhode Island** — R.I. Gen. Laws § 11-49.2-1 et. seq.: Similar to most state laws, Rhode Island requires notice to victims for breaches involving unauthorized acquisition of personal information.
- **Maine** — Me. Rev. Stat. tit. 10 §§ 1347 et. seq.: Like Massachusetts, Maine requires notice to a state authority in addition to notification to victims.
- **New Hampshire** — N.H. Rev. Stat. §§ 359-C:19 et. seq.: Like Massachusetts, New Hampshire also requires notice to a state authority in addition to notification to victims.

CONCLUSION

Data security breaches cost employers more than time and money. They can damage employee relations and generate negative publicity. A poor response to a breach only exacerbates the problem; especially if it surfaces that the employer did not have an effective data security program in place. As tedious as the Massachusetts law may be for employers, it provides a valuable guideline for employers having to comply with the requirements of every state in which they do business or have employees. Employers should further consider establishing a policy and procedure that requires its managers and employees to promptly report data security breaches. Employees should receive training on this requirement and the reporting procedure, and employers should establish a company protocol or action plan for responding promptly upon receiving a report of a data security breach. Multi-state employers should consult with counsel to develop a comprehensive data security plan that complies with all applicable legal requirements. ■

Daniel Klein, Esq., is a partner with Seyfarth Shaw LLP. He may be reached at dklein@seyfarth.com.