# Data Security: A Primer For The Midsize Company

*--By Joseph J. Lazzarotti, Jackson Lewis LLP*

**Law360, New York (October 20, 2009**) When a risk manager, company officer or general counsel thinks of data privacy and security programs for his or her company, employee personnel files, payroll and tax reporting information, client personal information for purchasing and marketing, and sensitive corporate information, among other things, immediately come to mind. However, when these same company officials are asked about such things, they commonly respond, "the IT Department handles it" or "we have a policy in our handbook" or "our client information is secure." There is no mention of employee personal information. Unfortunately, too often these are the wrong responses.

The growing number of data privacy and security laws requires an organization-wide effort to develop written policies and procedures that provide administrative, physical, and technological safeguards for sensitive and personal information. These laws do not require protections for confidential company information and trade secrets, but they also warrant protection. Leaving this task solely to your IT department will leave your IT employees overwhelmed and your company overexposed. In addition, you could lose a chance at a potential competitive advantage as individuals (clients, employees, dependents, and others) and business partners increasingly demand heightened security of their sensitive and personal information.

Some prime examples of the regulation directed at protecting personal information include:

- **Social Security numbers.** Written policy requirement and other protections for Social Security numbers in New York, Connecticut, New Jersey, and Michigan;
- **Comprehensive Data Security Program Requirements.** Regulations requiring comprehensive data privacy and security programs to protect personal information in states such as Massachusetts (effective Mar. 1, 2010), Maryland (in effect), Nevada (in effect); New Jersey (regulations proposed and expected to be finalized later this year), and Oregon (in effect);
- **Encryption Mandates.** Data encryption requirements Massachusetts (effective Mar. 1, 2010) and Nevada (Jan. 1, 2010);
- **Breach Notification Requirements.** Data breach notification requirements in 45 states (nearly all in effect);
- **Job Applicant Information.** Specific protections for personal information of job applicants in Utah (in effect);
- **"Red Flag" Regulations.** Federal "red flag" regulations for companies that are financial institutions or creditors;
- **HIPAA.** Privacy and security requirements under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) for company sponsored group health plans (including health flexible spending arrangements) and covered health care providers (including some on-site medical or occupational health clinics). Beginning February 17, 2010, many of these requirements also will apply directly to business associates of covered entities, which could include benefits brokers, consultants, third party administrators, electronic records storage companies and so on;

- **Federal Contractor Requirements.** Federal contractors generally are subject to the same federal laws, regulations, standards, and policies as the federal agency with which they have contracted. For example, contractors of the Department of Veterans' Affairs must comply with the policies and procedures outlines in VA Directive 6500, *Information Security Program* (http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=50&FType=2).
- **PCI Standards.** Certain companies processing credit card transactions and receiving payment for goods and services through credit cards may need to comply with the Payment Card Industry (PCI) Data Security Standards (https://www.pcisecuritystandards.org/).
- **International Standards.** Companies with subsidiaries or affiliates in other countries such as Canada, France, England or Germany may have difficulties exchanging personal information with their counterparts because of the expansive protections for personal data in those countries.

In general, these laws and regulations seek to protect certain categories of "personal information." These categories typically include an individual's first name (or first initial) and last name in combination with the individual's (i) social security number, (ii) driver's license number, (iii) state identification number, (iv) financial account, debit or credit card number, or (v) health information. Some states have more expansive definitions of personal information. For example, a recent Connecticut statute adds passport numbers, alien registration numbers and health insurance identification numbers. Virtually all businesses maintain this information in one form or another.

## So, What Do We Do?

Current data privacy and security laws generally do not contemplate an off-the-shelf policy. Businesses must assess the risks relating to their sensitive and personal information. They must question how that information is accessed, used, maintained, processed, disclosed, retained, and destroyed. At the same time, businesses must evaluate the safeguards currently in place. This process, referred to under many laws as "risk assessment," is critical to knowing what protections are needed and in many cases to learning about the information the company maintains. Done correctly, the risk assessment process will enable the business to craft comprehensive policies and procedures to address the risks identified.

Risk assessment. At a minimum, a risk assessment should include:

1. Establishing a key group to coordinate the project, including members of legal, human resources, IT/IS, finance, government relations, sales, public relations and others.
2. Selecting a project leader and obtain senior management approval early in the process.
3. Formulating a definition of protected information and locate that information. This includes, among other things:
    - Identifying all information systems, including all hardware, software and devices such as laptops, blackberries and so on, holding sensitive and personal information.
    - Examining alternative work/business arrangements (e.g., travel and working from home).
    - Determining which employees have access to sensitive and personal information and how the information flows through the organization.
    - Identifying contractors, vendors and other service providers who maintain sensitive and personal information.
    - Reviewing existing contracts requiring the company to safeguard sensitive and personal information.
4. Based on the information collected, identifying applicable laws, e.g., state data security regulations, Gramm-Leach-Bliley, HIPAA, federal "red flag" regulations, data destruction laws, Social Security number protection laws, and e-discovery rules. Any business may be subject to

one or more of these laws. To assist in identifying which laws apply, consider asking the following:

- *Does the company have a plan for responding to a data breach?* If your state has a breach notification statute, it is very likely that your business is subject to it. More companies are experiencing breaches of personal information in their possession, which in many cases require that they notify the affected individuals. The absence of a response plan increases the likelihood of an unnecessary delay and exposure to private lawsuit or state agency action.
- *Does the company maintain personal information?* It is hard to imagine a company that does not have some personal information in its possession. State and/or federal laws likely will apply to most businesses to some degree. For many, this will require that a written security program be adopted and implemented.
- *Does the company sponsor or provide services to a health plan?* If it does, HIPAA may apply. Some companies sponsor a health plan for employees and provide services to a health plan or health care provider. In that case, following the changes made under the American Recovery and Reinvestment Act of 2009, the company may become directly subject to many of the privacy and security requirements under HIPAA, with respect to the services it provides.
- *Does the company maintain medical information about employees in connection with leave determinations and disability accommodations?* If so, then the information must be segregated, consistent with FMLA and ADA regulations, and may also be subject to the recently enacted Genetic Information Nondiscrimination Act, which becomes effective November 21, 2009.
- *Is the company a "financial institution" or "creditor" that maintains "covered accounts"?* If so, then federal "red flag" regulations may apply. The compliance date for these regulations for those under Federal Trade Commission jurisdiction is November 1, 2009. A "creditor" is (i) any entity that regularly extends, renews, or continues credit; (ii) any entity that regularly arranges for the extension, renewal, or continuation of credit; or (iii) any assignee of an original creditor who is involved in the decision to extend, renew, or continue credit. A "covered account" is an account used mostly for personal, family, or household purposes, and that involves multiple payments or transactions. Covered accounts include credit card accounts, mortgage loans, automobile loans, margin accounts, cell phone accounts, utility accounts, checking accounts, and savings accounts. A covered account is also an account for which there is a foreseeable risk of identity theft – for example, small business or sole proprietorship accounts.
- *Does the company accept credit cards for payment?* If it does, it must adhere to the safeguards mandated by the Payment Card Industry Data Security Standard.

Developing Safeguards. At the conclusion of their risk assessment, businesses need to compare the information they have collected with the safeguards they employ in order to identify vulnerabilities. These vulnerabilities then must be addressed through additional administrative, physical and technical measures. Examples of these kinds of safeguards include:

1. Determining whether it is possible to collect, reformat and/or maintain information in a way that would cause it not to be subject to data protection laws, or whether the information may be discarded altogether.
2. Limiting access to sensitive and personal information through policy, physical barriers and/or user profiles, such as using locks on doors and file cabinets, not leaving sensitive and personal information unattended, and deploying password functions and screensavers.
3. Encrypting portable electronic devices, such as laptops and blackberries.

4. Entering into security agreements with vendors holding sensitive and personal information, or taking steps to ensure they have adequate safeguards in place.
5. Developing a protocol for responding to data breaches – identifying who will lead the response team, prepare template notices, line up legal counsel and other vendors.
6. Developing a disaster recovery plan.
7. Training staff upon hire and at least annually thereafter, or whenever an event suggests the need for retraining.
8. Developing a record retention policy; maintaining records no longer than is necessary; destroying information no longer needed.
9. Monitoring legal and technological developments.
10. Evaluating the effectiveness of existing data privacy and security programs and making changes as appropriate.

Sensitive and personal information have become an instrument of modern commerce. Efforts to protect it show no sign of slowing. Businesses of all sizes and in all industries need to take stock of this valuable asset and develop a comprehensive strategy for safeguarding it, taking into account size, complexity, capabilities and cost. Those which are thorough and thoughtful in addressing this challenge will have the best chance of succeeding in a more complex information age.

--By Joseph J. Lazzarotti, Jackson Lewis LLP

*Joseph Lazzarotti is a partner with Jackson Lewis in the firm's White Plains, N.Y., office.*