With a combination of risk assessment, technical solutions, and staff training, it is possible to keep data secure.

**INFORMATION IS** the new currency of commerce. Sensitive data, such as social security numbers, credit card information, financial records, health data, and intellectual property may be worth millions of dollars in the hands of hackers and data thieves. With the assistance of the Internet and new storage media, confidential information may be compromised on a larger scale and faster pace. In 2006 and 2007, for example, more than 300 major incidents of data breach were reported each year, and 2008 is on pace for a similar total. *Data Loss Archive and Database*, [www.attrition.org](http://www.attrition.org). Millions of pieces of personal data have been stolen in recent years, often from prominent companies and organizations. *Attorney General Announces Data Breach At New York Bank Possibly Affecting Hundreds Of Thousdands Of Ct. Consumers, Millions Nationwide*, [CT.gov](http://www.ct.gov/ag/cwp/view), May 21, 2008, [www.ct.gov/ag/cwp/view](http://www.ct.gov/ag/cwp/view). Even without actual identity theft, the magnitude of the problem of data security, and the potential cost of remedying data breaches, has become a major problem. If organizations and companies do not address data security issues, critical threats to information privacy may develop. Businesses and other organizations thus must take action to secure the sensitive data they control. This article provides a list of potential actions that businesses...
and other institutions may wish to consider in minimizing the risk of data security breaches and the consequences of breaches when they occur.

**LAWS CURRENTLY APPLICABLE TO DATA SECURITY BREACH**

There is no single federal law that governs all use and disclosure of sensitive information. Rather, specific statutes and regulations may restrict use and disclosure of information in certain contexts, and require entities that maintain this information to take reasonable steps to ensure the security and integrity of that data. Four major statutes in this area include: the Fair Credit Reporting Act ("FCRA"), 15 U.S.C. §1681 et seq., Title V of the Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. §6901 et seq., Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. §41 et seq., and Part C of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), 38 U.S.C. §1320d et seq. The FCRA primarily regulates the distribution of “consumer reports” by “consumer reporting agencies.” The GLBA imposes security obligations on “financial institutions.” The FTC Act holds liable companies that fail to implement necessary security protection, to the extent that such failures may be considered “unfair” or “deceptive” trade practices. HIPAA requires privacy and data security standards for health care information systems.

**State Laws**

On the state level, at least 38 states have passed some form of data breach notification law. See Scott Berinato, *CSO Disclosure Series: Data Breach Notification Laws, State By State*, CSOOonline.com, February 12, 2008, [www.csoonline.com](http://www.csoonline.com). In total, as many as 48 states have some kind of law “aimed at the prevention of unauthorized disclosures of personal and financial information.” *Security Breach Legislation, in 50 State Statutory Surveys* (2007). These laws, in general, require businesses to notify consumers when their personal information has been compromised. Some state laws also limit use of specific personal information, such as social security numbers.

**WHAT CAN BE DONE TO REDUCE THE RISK OF DATA SECURITY BREACH?**

Risk assessment and development of responsive measures can work in tandem to prevent or mitigate data security breaches. Rather than waiting for a breach to happen, companies can identify weak spots in their existing systems, and develop preventive measures. Most significantly, businesses should establish comprehensive data-detailed security policies, and create a security-conscious workforce, through training and periodic reminders. Companies may also invest in new data security technologies to stay ahead of ever-evolving security threats.

**Risk Assessment**

To develop an effective data security program, the first step is to identify all reasonably foreseeable internal and external threats to information assets in need of protection. Companies should examine each major area of data operations, including information storage, network security, regulatory compliance, and employee training. Appropriate questions may include:

- Is the information system ready to fend off a hacker’s attack?
- Is the company’s information storage policy understandable and comprehensive?
- Has the existing security policy been enforced? Is there any nonconformity in compliance that could create company liability for potential breach?
- Do the company’s employees have sufficient knowledge and awareness about data security attacks?

Expert assistance may help to identify all potential risks to an information system. Several companies specialize in cyber-crime response and computer
forensics. Internal data security assessments may also be conducted on a regular basis.

Risk Evaluation
Once potential threats are identified, companies should evaluate the magnitude of the risks presented, by assessing the likelihood that a threat will materialize, evaluating the potential damage that could result, and assessing the sufficiency of policies, procedures, and safeguards in place to guard against foreseeable threats. For example, if consumer information stored in company computers and mobile data systems such as laptops is not encrypted, the likelihood of a threat materializing may be significant, and potential damage may be great. As a result, the company may choose to implement a policy requiring data encryption, or some other procedures to safeguard such information.

Some smaller companies cannot afford the expense of sophisticated data security systems, even though their vulnerability to data security breach is as great as for their larger counterparts. One solution is to seek help from larger companies that share the smaller company’s data security interests. For example, merchants may request assistance from credit card companies to conduct security assessments and enhance security systems. Larger companies may have incentives to provide such assistance, when they must share consumer data with their smaller affiliates.

Implement Technical Solutions
Today’s technology has developed a variety of media to store data, ranging from backup tapes, to laptops, to flash drives. Companies must deploy varied security technologies to address diverse security problems. In general, technical security solutions include one or more of the following approaches.

Encryption
Encryption is the most commonly used method to keep confidential information secure. Through encryption, bits of data are mathematically jumbled, with a password-key. The encryption process makes data unreadable until decrypted. Encryption can be very cost-effective in data protection. Protecting customer records through encryption may be substantially less expensive than paying for cleanup after a data breach. In testimony on identity theft at a Senate hearing after the Department of Veteran Affairs lost personal data on 26.5 million veterans, Gartner, a research company, noted that encryption can cost as little as $6 per customer account, while cleanup costs can range upwards of $90 per customer account. Gregg Keizer, Security Cleanup Costs Much More Than Encryption: Gartner, TechWeb.com, June 6, 2006, www.techweb.com.

Despite the benefits of encryption, and many highly publicized losses of unencrypted data, many organizations lag in use of encryption. In the Ponemon Institute’s 2008 Annual Study, only 21 percent of the 975 companies polled reported that they had enterprise-wide encryption plans, although the figures are increasing. Ponemon Institute, LLC, 2008 Annual Study: U.S. Enterprise Encryption Trends 2 (2008), www.pgp.com/downloads/research.

New technologies have helped to simplify the process, and reduce the cost of encryption. For example, companies have increasingly adopted a platform approach to encryption. Id. at 3. A “platform approach” uses a single console “to deploy and manage multiple encryption applications.” Id. at 20. Companies see this approach as increasing efficiency and cutting costs. Id. at 3. In addition, hardware encryption appliances may replace older software-based designs, and may eventually replace them altogether. Neil Roiter, Hardware-Based Encryption Gains Most Innovation Of ’07, SearchSecurity.com, Jan. 3, 2008, www.searchsecurity.techtarget.com.

The new hardware designs may decrypt data in close to real time, and users may not notice any delays in data access. System performance can be further enhanced by limiting encryption to sensi-
tive data only. Often, only a small portion of information needs protection, such as social security numbers, credit card information, or health information. Encrypting the most sensitive fields and leaving everything else unencrypted may boost the performance of a database. Data partition is a commonly used method in this regard. Instead of encrypting one big database that contains detailed information about all customers, companies may place sensitive data into discrete databases developed and tailored to meet the specific data security needs of clients (inside and outside the firm), and safeguard the discrete databases according to their varying security levels.

**Lock Down Endpoints**

Another option to prevent sensitive data from security breach focuses on controlling the exit point of information flow, such as the flash drive, CD-ROM burner, or handheld device. Restriction of access to data endpoints prevents malfeasant employees and data thieves from easily downloading sensitive data onto flash drives or other portable data devices. Sophisticated management software can restrict use of such personal storage devices. Such software can determine the flow of information based on a user’s identity or the type of personal data device connecting to the network. The software will refuse to transfer data if the external storage devices are unrecognized or the user lacks required data access privileges. More sophisticated software allows further fine-tuning of access; such software can limit both the type of content users can view and the time of day they can see it.

End-point lockdown, however, cannot provide protection once data has been legally downloaded from points of control. For people who might need to carry protected data from one location to another, one solution uses encrypted flash drives. Data downloaded into a flash memory is encrypted and can only be read by plugging into another endpoint in the network. Thus, the data retains at least one layer of protection even if the portable memory device is lost.

**Information Content Management**

Another approach to secure sensitive data involves restriction of access rights and other security protections within individual documents. This system, often called an enterprise rights management (“ERM”) system, allows distribution of protected content within a network and to business partners. The system protects document content by requiring the document creator to encrypt the document and apply rules to determine who may gain access to the file. The document creator can also specify whether the document can be printed, copied, or forwarded to others. This access control is embedded within the document, and stays with it wherever it goes. In this way, the document can be freely distributed outside the system with reduced concern for security breach, because only authorized users can read and revise the document. ERM also records the chain of custody, providing an audit trail of persons who have accessed a document, when access occurred and what was done to copy or otherwise distribute the document. Information content management, such as ERM, thus offers increased storage security.

ERM must nevertheless overcome certain hurdles before it can be embraced by the business world. For example, an interoperability problem exists across ERM products from multiple vendors. Some systems simply are not compatible. As a result, ERM systems do not always work with all applications, or with each other. More importantly, ERM requires creation of data security policies, and role and classification guidelines. This process is both technical and time-consuming. It requires the data system manager, responsible for creating such document classifications, to understand the various types of information an organization stores, and to negotiate a consensus on the level of accessibility for each type of data. High costs have

Creating Security Policies

In tandem with implementing data security technologies, a company may reduce risk by creating clear data security policies and enforcing them effectively. An enforceable security policy should be short, simple, and clearly worded. Many companies create laundry lists of compliance items, and impose them all on their employees. This approach seldom works because employees can only comply with a limited number of standards. A short policy can be created to identify the company’s highest level data-protection goals, such as protection of the most important data, or minimization of liability for security breach. Compliance items along the lines of best practices need not be included in this list; they may be separately stated. Security policies also must be easy to enforce. Consultation with personnel who will take responsibility for enforcing the policies can help formulate more easily enforceable data security procedures.

One important data security policy that every company should strive to follow is removal of obsolete records. Many companies keep enormous stores of sensitive data that provide marginal business benefit, but create risk. For example, retailers often keep databases of highly sensitive credit card data, even when not necessary. Best security practices should require a clear policy spelling out how such data should be stored and how frequently it should be deleted. Regularly conducted “privacy audits” also can help companies monitor enforcement of security policies and mitigate risks presented by unnecessary data retention.

CREATING A SECURITY-CONSCIOUS WORKFORCE • Although malicious attacks by outside hackers have drawn the most attention from the media, security breaches often can result from inappropriate conduct by insiders with authorized access. For example, in June 2008, an AT&T employee inadvertently lost an unencrypted laptop when it was stolen from the employee’s car; leaving the names, social security numbers, salary and bonus information of an undisclosed number of management staff at risk. Dan Kaplan, AT&T Management Staff Data On Stolen Laptop, June 4, 2008, www.scmagazine.com.

As the title of a Wall Street Journal special report rightfully pointed out, the biggest threats to information security may come from “The Dangers Within.” Michael Totty, The Dangers Within, Wall St. J., Feb. 13, 2006, at R1. A recent study by the Ponemon Institute revealed that many employees are unaware of, do not follow, or otherwise fail to comply with security policies. Ponemon Institute, LLC, Data Security Policies Are Not Enforced: US Survey of IT Practitioners 7 (2007), www.redcannon.com.

A workforce untrained in data security protection, and unscreened for compliance, may foster data security breaches. An unwary employee, for example, could inadvertently disclose sensitive data in public media, such as blogs. Employees may also become victims of “social engineering” designed to deceive them into disclosing data. An employee may also encounter “spyware,” software embedded in email messages that enable the email sender to gain access to the recipients’ computer and network. Another hacking technique similar to spyware is “evil twinning,” a malicious wireless network located close to a legitimate wireless network for the purpose of capturing private electronic communications. Even viruses can expose sensitive data to breach. Markian Hawryluk and Betsy Q. Cliff, Hospital Donor Files Compromised, www.BendBulletin.com, March 6, 2008.

There are many ways for hackers to trick an unsuspecting employee into giving away data, especially when the employee is ignorant about the danger. Thus, one of the most important aspects
of data security is creation of a well-educated and alert workforce.

Training

Companies can use training programs to remind employees that information related to consumers (such as social security numbers, financial information, and health information) can be misused. Employees should be trained to recognize spyware, viruses, and other hacking techniques, and to report such encounters to system administrators.

Confidentiality Agreements

To deter intentional security breach from malicious insiders, employers may toughen employment confidentiality agreements, adding terms that emphasize information security and an employee’s responsibility to follow company policies. If the company is publicly traded, it may take advantage of Section 406 of the Sarbanes-Oxley Act by voluntarily adopting a tougher code of ethics. Such new codes of ethics may require employees to keep data secure, and to report any security breach to the company ethics officer.

WHAT TO DO AFTER A BREACH OCCURS

• If a data security breach occurs, companies must consider their duty to notify persons affected by the breach. California and many other states require disclosures to persons whose personal information may have been compromised.

  Companies should establish notification protocols to be used in the event of a breach. The incident response plan should designate an executive in charge of responding to such an event. The plan should ensure that appropriate persons within the affected organization are promptly notified and prompt actions taken. Such actions may include maintaining the integrity of the computer system for forensic examination, conducting investigations to determine the scale of damage, taking actions to deter further attack, and informing law enforcement authorities about the incident. Development of an incident response team and an incident response plan before a breach occurs may help avoid missteps.

  When disclosures issue, moreover, companies should strive to provide clear and informative notification to persons affected by a breach. A national survey on data security breach notifications by the Ponemon Institute showed that more than half the victims of breach rated notification timeliness, quality, and clarity as fair or poor, and that 55 percent received notification a month or more after the breach. Ponemon Institute, LLC, Consumers’ Report Card on Data Breach Notification 3 (2008), www.idexpertscorp.com/breach/ponemon-study. Fifty-eight percent of surveyed customers stated that they lost confidence in the company after notification, and 31 percent terminated their relationship with the organization that lost the data. Id. at 7-8. Some eight percent filed formal complaints. Id. at 8. In addition to clear and prompt notification, a telephone hotline and offers of free credit report monitoring may be well-received by consumers. According to the Ponemon Survey, less than one third of companies provided such services as credit monitoring in response to a data breach. Id. at 6. Of consumers provided with such services, less than half used the service, but almost all consumers who used the services rated them highly. Id. at 6-7. Part of planning for management of a data security breach should include preparation for communications about the breach and the company’s response.

CONCLUSION • Companies should fully understand the data security risks they face and adopt appropriate policies and technologies in response. Such measures, however, may fail unless employees who manage sensitive data understand the company’s data protection policies and implement them. Development of data security measures can be relatively inexpensive solutions compared to the cost of a major data security breach.