# Information management

Best practices for maximizing the security of sensitive information

Advancement in Internet technology has been a double-edged sword. On the one hand, it has increased the efficiency of some processes and made everyone's life a lot easier. On the other, it has made people's sensitive information vulnerable and subject to theft by criminals.

By following a few basic steps, says Betty Steele, of counsel in Baker, Donelson, Bearman, Caldwell & Berkowitz, PC's Nashville office, businesses can greatly mitigate the risk of loss of sensitive information that is stored or transmitted electronically.

*Smart Business* asked Steele about the latest legislation governing information security and what companies can do to safeguard against the loss of sensitive information.

### What are the key drivers behind federal, state and international information security laws and regulations?

Worldwide laws and regulations are proliferating in response to consumer concerns about identity theft and privacy of personal financial, health and other sensitive information, investor concerns about corporate fraud and accounting irregularities, and government concerns about critical infrastructure and cyber attacks in light of terrorist attacks around the world.

These drivers are continually being reinforced as high-profile security breaches are being reported. For example, the TJX breach of data on more than46 million credit and debit cards used at TJX stores has spurred on legislation aimed at making retailers and other merchants liable to banks for the costs associated with card data breaches through such methods as consumer notification and card replacement.

### How does the constant introduction of new and faster technologies impact the ability to maintain sensitive information securely?

The constant introduction of new and faster technologies means organizations, in order to be competitive from a business perspective and have appropriate information security controls, must ensure that processes are in place for change control and integration of the administrative, physical and technical aspects of information security, privacy and corporate governance.

**Betty Steele**
Of counsel
Baker, Donelson, Bearman, Caldwell &
Berkowitz, PC

### Are there frameworks or best practices that can be used so that legal, technology and business requirements can be integrated into processes and aligned?

Many public companies are already using the COBIT (Control Objectives for Information and related Technology) framework for internal controls for financial reporting in order to comply with the Sarbanes-Oxley Act.

At the same time, those public companies as well as nonpublic companies can also effectively use ISO/IEC 17799 — now the ISO 2100 series and the de facto world information security management standard — in order to comply with multiple laws and regulations in one integrated framework. ISO/IEC 17799 easily maps to COBIT and, for any organization required to adopt the Payment Card Industry Data Security Standard (PCI DSS) — i.e., organizations accepting credit and debit card payments — this standard easily maps to ISO/IEC 17799. Effective use of these frameworks/standards may also have the beneficial effect of reducing compliance costs and maximizing the chances for secure systems.

### What action steps should organizations take at the beginning of the process?

A disproportionate number of information security breaches occur because of insiders intentionally and unintentionally violating organizations' acceptable use of IT assets. Many breaches occur because employees or contractors lose electronic media containing sensitive personal and/or organizational information, or because employees access sensitive information inappropriately. The following approach is recommended for organizations at the beginning of the information security management process:

1. Identify sensitive information, such as credit card numbers, medical records and employee files residing in both electronic and non-electronic media, and determine who has a need to use, disclose and request it.
2. Assign clearances to employees and vendors/service providers to access sensitive information based upon the concept of least privilege. Clear security roles and responsibilities with appropriate policies, training and accountability are key to the success of any information security management program.
3. Document current policies, practices and procedures, information flows, etc.
4. Provide a quick, basic risk analysis using a best practices information security management framework.
5. Identify gaps that can be filled inexpensively and quickly and provide the most protection.
6. Put administrative, technical and physical controls in place that address these gaps, many of which are caused by employees and vendors/service providers failing to comply with security requirements. These breaches include downloading unauthorized software, opening e-mail attachments from unknown senders, leaving laptops and PDAs in cars, and failing to encrypt sensitive information.
7. Consider using the highly prescriptive PCI DSS for all sensitive information, not just credit and debit card information.
8. Put together a realistic timeline and identify resources necessary to have an information security management program that reflects reasonable best practices. <<

**BETTY STEELE** is of counsel in Baker, Donelson, Bearman, Caldwell & Berkowitz, PC's Nashville office and is a member of the firm's Business Law Department. She is a Certified Information Systems Security Professional (CISSP) and concentrates her practice in technology, information privacy and security, corporate governance and international law. Reach her at (615) 726-5603.

**Insights Legal Affairs** is brought to you by Baker, Donelson, Bearman, Caldwell & Berkowitz, PC