SECURING THE FUTURE

In this Issue

Secure Information Destruction; A Legal Imperative

Regulatory and legal compliance are aspects of information security that are increasingly important, but are still often overlooked, particularly by smaller organizations. As a business decision-maker, you are probably aware of the negative consequences of information security breaches including: loss due to customer attrition, damaged reputation and costly fines and restitution.

Do you realize, however, that information security extends beyond sound business practices – it's also your legal responsibility to eliminate the very conditions that may lead to potential breaches.

In the U.S. and internationally, governments and regulators are now mandating that organizations of all sizes take responsibility for the security of their sensitive data. Today's newsletter explores what local laws require, and what steps your company should take to ensure your clients, partners and employees are legally compliant.

Information as a Double-Edged Sword

Your company's organizational growth and survival depend on an abundance of quality information. After all, we live in what is known as the "information age."

SECURING THE FUTURE

Your company produces and consumes vast amounts of data from clients, partners, employees and other stakeholders. Managing payroll, analyzing cash flow, keeping track of suppliers, researching client profiles, data-mining for trends and collecting competitive intelligence are just a few of the data points you manage every day.

While this information and associated tasks are critical to your success, the same pools of data can leave your company vulnerable. If this information is accessed by internal employees or individuals outside of the company with malicious intentions, this sensitive data represents a goldmine to them…and a huge risk to your company.

"Unfortunately, individuals not bound by ethical constraints are capable of using easily available information for illegitimate purposes," says Vince De Palma, President and CEO at Shred-it. "Information theft, including identity theft, is a substantial and growing business these days. Criminals operating in both the U.S. and abroad extract handsome profits by exploiting organizations' security vulnerabilities."

Armed with a few key pieces of information such as name, birth date, social security number and address, identity thieves can reconstruct and steal the information of your clients, employees, owners, partners and even your entire company. This stolen information is typically used for criminal gain through false loan applications, credit card fraud, bank account "skimming," false medical insurance claims and more.

Information security laws and regulations have been put in place for organizations for this very reason.

Not Knowing the Law Does Not Exempt You From the Law

Given the wealth of confidential information available, U.S. law-makers have taken strides to protect consumers by safeguarding confidential information. This legal framework includes:

- **The Health Insurance Portability and Accountability Act of 1996 (HIPAA)** includes several sections that specifically address patient privacy and medical record security. While HIPAA legislation took several important steps to protect patient privacy, lawmakers wanted to widen the scope of legal protection so the Health Information Technology for Economic and Clinical Health (HITECH) Act was passed in 2009.
    - **Part of the HITECH Act** states that healthcare providers will be given financial incentives for use of electronic health records (EHR). The HITECH Act also provides financial aid for training in order to

support health information technology infrastructure. Physicians who elect not to use EHR by 2015 will be subject to penalty, starting with 1% Medicare fee reductions. After 2015, the penalty will progress and reach 5% fee reduction by 2019. The main objective of this Act is to minimize data security breaches and contain patient information to physicians and other authorized personnel.

- **The Fair and Accurate Credit Transactions Act (FACTA) of 2003** mandates that U.S. financial institutions and creditors comply with the Identity Theft Red Flag provisions by November 1, 2008. The "Red Flag" is a pattern, practice or specific activity that indicates the possible existence of identity theft. This rule is applicable to all banks and savings institutions regardless of whether they hold a transaction or transition account belonging to a customer, whether directly or indirectly. This rule seeks to ensure that all financial institutions and creditors are alert for signs or indications of potential misuse of an individual's data and to respond appropriately.

- **The Sarbanes–Oxley Act of 2002**, commonly referred to as SOX, is a federal law that sets accounting and privacy standards for all U.S. public companies. The bill was created as a reaction to a number of highly public accounting scandals including Worldcom, Tyco International and Enron. Its complex legislation provides provisions for the protection and secure destruction of confidential information and financial records.

- **The Gramm-Leach-Bliley Act (GLB)**, also known as the Financial Services Modernization Act of 1999, was designed to protect the privacy of consumer information held by financial organizations. It tackles three core areas of financial responsibility including: a) privacy policy - the financial institution must disclose the kind of information it collects and how it uses it, b) right to opt-out - the financial institution must explain how customers can prevent the sale of their data to third parties, and c) safeguards - financial institutions are required to develop policies that prevent unauthorized access to confidential information.

Organizations covered by these rules must have policies in place to comply with the new standards to avoid costly fines, regulatory enforcement actions and to avoid the risk of security breaches. The price for noncompliance with these regulations can be very costly to an organization from both a monetary and reputation perspective.

Secure Information Destruction and Legal Compliance

As you can see, U.S. law requires businesses to be aware of potential security risks and to be proactive in addressing compliance situations. Many organizations are still caught off guard by the news that they should be adopting best practices to ensure the safety of confidential information in their custody, and that they are required by law to do so.

SECURING THE FUTURE

According to Shred-it's 2011 Information Security Tracker, research conducted by Ipsos Reid indicated that 36% of U.S. small to mid-sized businesses have no policies for document storage or disposal.[1]

"Part of our job as an information security company is to consult organizations on what best practices and security strategies they should be implementing to become compliant," says Mr. Vince De Palma. "Typically, there are several key strategy components we recommend to each client. One of them is that they should always opt for document destruction methods that meet or exceed all national compliance standards. Another recommendation is to have an organization-wide policy in place that stipulates how company employees should go about the disposal of their paper waste."

It is important to remember that legal compliance is a minimum requirement. An organization's efforts to protect itself, its clients, employees and other stakeholders should not limit itself to only these mandated standards. The ultimate goal is to create a total security culture, with zero tolerance of security breaches and the existence of the very conditions that make them possible.

Information Security Recommendations From Shred-it

Given the importance of compliance, and the changing nature of the legislation and the sometimes onerous rules, what should your company being doing today to protect itself?

- Understand security legislation as it pertains to your specific industry and work toward full compliance with all privacy regulations.
- List all information security risks specific to your organization, targeting both paper-based and electronic information sources. Consider every stage of the information cycle; from data generation and storage, to the transfer of data from location to location, and the document destruction process.
- Train your employees in best practices and develop a clearly documented and well-understood process for secure document management and destruction.
- Outsource document destruction to professional providers who ensure the total security of the document destruction process. Look for a professional provider that offers:
    - On site information destruction services.
    - Locked security consoles that feature a beveled slot and security plate to ensure documents cannot be removed once placed in the console.

SECURING THE FUTURE

- Powerful shredding machines that can quickly destroy large volumes of paper, using cross-cut shredding technology.
- Various shred size "levels," allowing your organization to choose a shred size that suits your needs.
- Ability to witness the document destruction process as it's occurring.
- Proof of destruction confirming that your confidential information has been securely destroyed.

[1] Shred-it Security Tracker 2011

About Shred-it

Shred-it is a world-leading information security company providing document destruction services that ensure the security and integrity of our customers' private information. The company operates 140 branches in 16 countries worldwide, servicing over 150,000 global, national and local businesses, including the world's top intelligence and security agencies, more than 500 police forces, 1,500 hospitals, 8,500 bank branches and 1,200 universities and colleges. To learn more, please visit http://www.shredit.com/Home.aspx