SECURING THE FUTURE

In this Issue

Don't throw your reputation in the garbage bin.

Ponder the consequences of security breaches, which may result in identity theft and fraud, unhappy clients or employees, negative media attention and expensive lawsuits. Add to that, your company's intellectual property and commercial secrets leaked to your competitors, and you can see that the damage of compromised security to an organization's reputation and brand can be significant and potentially devastating.

Reputation: Your Most Valuable and Fragile Business Asset

In today's economy, when the pressures to cut costs are apparent, it is important not to lose sight of your organization's long-term goals and most valuable business assets. Reputation is one of those assets – powerful, yet intangible and fragile it serves as a magnet, attracting resources and attention.

In a survey at the World Economic Forum, more than one hundred of the world's top executives regarded a company's reputation as the second most important measure of success, closely behind quality of products and services.[1] If your products and services are already meeting your customer's needs, reputation is the engine that will continue to drive growth, increase profits and help you beat the competition.
Reputation is not only defined by your company's services and products; "Leading companies understand that serving their clients also means protecting them, particularly from any harm caused through these companies' own actions," says Vince De Palma, President and CEO at Shred-it. "In this digital age, one of the most

important individual rights is the right to privacy, which is closely related to the security of our personal information. New and existing laws and regulations recognize and protect these rights, and so should all businesses and organizations, large or small. Furthermore, this protection should extend beyond your clients to your business partners, employees and all stakeholders."

The protection of this sensitive information is critical to an organization's ability to conduct business with various stakeholder groups. If your clients or partners have concerns about the security of their financial or personal information while it's in your trust, they may take their business elsewhere; and they are almost certain to do it if the security of their personal information has been compromised while in your custody. At the same time, an untainted reputation for information security will give your customers, employees and partners the level of comfort they need to count on you as a trusted partner.

According to research performed by Ponemon Institute[2], the cost of a data breach is also something to consider when taking into account the company's reputation and brand. 2011 research showed that one compromised record costs a company an average of $214.00 and $7.2million per data breach event. One may question, what's a company to do with this information? The answer is simple; calculate your potential cost of a data breach. This can be done internally or by using a reputable vendor who can perform a free data security assessment.

How to Save Your Company's Reputation

An organization's reputation is not adequately protected if its stakeholders are exposed to any of the risks below:

- Inadequate protection from unauthorized access by *outsiders* of your electronic or paper-based information, such as employee records, customer data, email lists, etc.
- Inadequate protection from unauthorized access by company *employees* of electronic or paper documents.
- Paper waste leaving the office in a way that allows reconstruction of confidential documents.

While the risks associated with electronic information receive a large portion of media and corporate attention, a large number of security breaches can still be traced to paper documents, particularly when they are recycled without prior shredding, or simply thrown into unsecured garbage bins.

Small and medium-sized organizations are especially vulnerable to such risks particularly those that are in early stages of organizational development and/or relying on a more informal style of conducting business as they

may not have formal information security policies and procedures in place yet. According to Shred-it's 2011 Information Security Tracker conducted by Ipsos Reid Research 36% of small to mid-sized businesses have no policies for document storage or disposal.

If a breach does happen, smaller organizations are less likely to have adequate legal and other necessary resources to deal with the regulatory and financial consequences of such a breach. Companies of any size should realize that taking risks with the security of their customer and business information could lead to potential repercussions such as: litigation costs, fines, negative media attention and reputation damage. A secure document destruction process allows organizations to not only invest in their security and reputation, but also in long-term productivity.

Information Security: Good Business Practice and Legal Imperative

Sensitive paper documents, such as employee records, customer data and financial information must be securely stored and destroyed when no longer needed. This is not only a good business practice that saves cost and protects reputation, but also a legal and regulatory imperative. According to Shred-it's research, 57 percent of U.S. companies use document destruction services as a direct result of government regulation.[3]

Two regulations that all U.S. organizations should be aware of and comply with include:

- The Health Information Technology for Economic and Clinical Health (HITECH) Act was signed in February of 2009 as part of the stimulus package. The Act creates a federal requirement for the breach of protected health information and provides incentives for physicians to put into practice "meaningful use" of an Electronic Health Record system.
- As of June 1 2010 the Federal Trade Commission (FTC) implemented the "Red Flags Rule." A "Red Flag" is a pattern, practice or specific activity that indicates the possible existence of identity theft. The Rule requires U.S. financial institutions and creditors with covered accounts (creditors include organizations such as finance companies, automobile dealers, mortgage brokers, utility companies and telecommunications companies) to have a standardized program that detects, prevents and mitigates identity theft. Organizations covered by the rule 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.

Lack of compliance in both of these regulations could cost an organization thousands of dollars or more.

"The reputation of any organization is threatened when confidential documents become accessible to unintended recipients," says Mr. De Palma. "Companies are responsible to their employees, their clients and

their business partners to adopt secure business practices that ensure all these various constituencies are not only well-served, but also well-protected."

Shred-it's Tips for Reputation Protection and Security Breach Prevention

- **Shred all:** A simple and effective way to improve your information security is through the adoption of "shred all" policies and procedures. Forward-looking organizations increasingly recognize the importance of destroying all paper documents that are no longer required.
- **Shred before recycling:** Shred all confidential documents before recycling – don't let them sit unattended in recycling bins or be intercepted in transit once they leave your office.
- **Limit insider access:** Help prevent insider information theft by limiting internal access to confidential information.
- **Create a culture of security:** Train all employees in information security best practices to reduce human error; conduct regular security audits of your office to assess its security performance.

For more information on proper document destruction for a specific industry, please visit Shred-it's online resource center.

---

[1] "Corporate Brand Reputation Outranks Financial Performance as Most Important Measure of Success." WEF 2004.

[2] Ponemon Institute " Cost of data breach climbs higher" March 8, 2011 http://www.ponemon.org/blog/post/cost-of-a-data-breach-climbs-higher

[3] Shred-it's 2009 customer research

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.