SIMS RECYCLING SOLUTIONS

Retired IT Assets?

White paper explains important data destruction and recycling tips.

Properly Recycling Retired Electronic Equipment Reduces Likelihood of Data Security Lapses

Digital data–much of it confidential and protected–is being gathered more rapidly and in greater volumes than ever before. Digital photos and videos, electronic medical records, email and text messages, Internet documents and searches, online commerce and banking, and posts to social media sites are some of the sources for this data. Technologies, such as cloud-based computing, file-sharing applications, and mobile devices, increase employee efficiency and customer convenience, and have made it easier to collect, store, access, and transfer this vast amount of information.

The 2.5 quintillion bytes of data created each day[1] represent tremendous opportunities for enterprises to perform analysis, gain insight, and make connections that allow doctors to detect and treat disease, police departments to better identify and prevent crime, and utilities to anticipate system demands. But equal to the opportunity this data represents is the risk of severe economic and legal penalties, fraud, and identity theft in the event the data is compromised. This means the need for digital data security–from the time the data is collected until the time it is destroyed–affects every organization and has never been more critical.

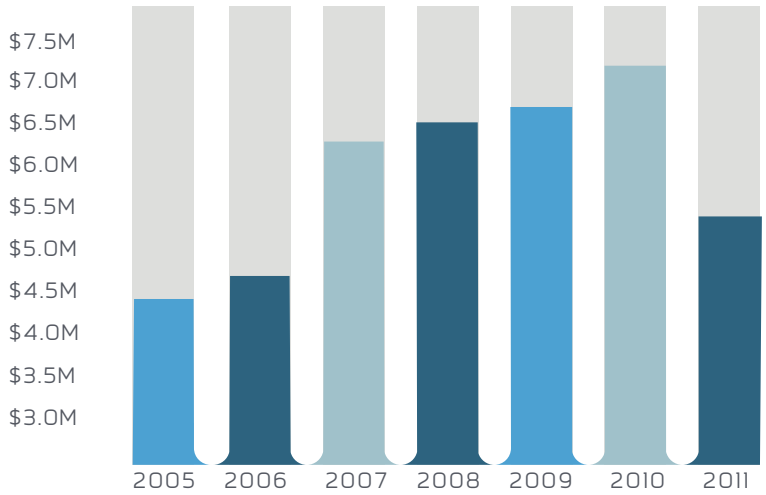
Why Data Security Matters

The Privacy Rights Clearinghouse reports that in the United States 26,474,373 records were compromised by the 671 data breaches made public in 2012.[2] The typical breach costs U.S.-based companies $194 per compromised record, resulting in an average total cost of $5.5 million per incident, according to research conducted by privacy think tank Ponemon Institute for their *2011 Cost of Data Breach Study: United States.*[3] Contributing to that hefty tab are legal defense fees, regulatory noncompliance penalties, data breach notification costs, revenue losses from increased customer turnover, and the expense of repairing a damaged reputation.

> The need for digital data security–from the time data is collected until the time it is destroyed–affects every organization and has never been more critical.

Stipulating how sensitive information must be handled and preventing the potentially devastating consequences of a data breach are central to the numerous privacy regulations in effect throughout the world. These measures compel organizations to protect personal identifiable information in all its forms, including electronic data, or be subject to substantial fines. In the United States, there are several privacy regulations intended to safeguard confidential information, including the Health Insurance Portability and Accountability Act (HIPAA), the Fair and Accurate Credit Transactions Act (FACTA), the Identity Theft and Assumption Deterrence Act (ITADA), and the Gramm-Leach-Bliley Act (GLBA). More than 46 states, as well as the District of Columbia, Guam, Puerto Rico, and the Virgin Islands, have passed legislation that requires owners of personal information databases to notify affected individuals in the event of a data security breach.[4]

Canada has two federal privacy laws, the public-sector Privacy Act and the private-sector Personal Information Protection and Electronic Documents Act (PIPEDA). Together these laws regulate how federal government agencies and departments as well as private enterprises collect, use, and disclose personal information.[5] Alberta, British Columbia, and Quebec have separate provincial personal information protection acts that are substantially similar to PIPEDA. Several provinces, including New Brunswick, Newfoundland and Labrador, and Ontario, have passed regulations that specifically address the collection, use, and disclosure of personal health information by health care providers and organizations. These laws have also been recognized as substantially similar to PIPEDA.[6]



Average total organizational cost of a data breach over the last 7 years:
$5.98M

Ponemon Institute LLC, "2011 Cost of Data Breach Study: United States" (March 5, 2012), p. 6, figure 2.

Where Data Lurks

The actions of hackers and negligent employees or contractors were responsible for exposing more than 8.2 million records in 315 data breach incidents made public in 2012, according to the Privacy Rights Clearinghouse.[7] With so much at stake, most data security efforts are justifiably directed toward protecting electronic equipment currently in use. These devices are subject to clearly defined security procedures that protect the equipment and the data they contain from intrusion, loss, and unauthorized access.

On occasion, computers and other electronic devices marked for recycling fall outside those established security protocols even though they may still contain easily accessible data that can leave an organization vulnerable to a data breach incident. This data exists not just in computer and server hard drives that have been declared obsolete or redundant, but across a wide array of devices, including copiers, printers, scanners, and fax machines. Two office workhorses–copiers and printers–often have hard drives that store readily obtainable data and can be the unexpected source of a data breach. A lesson Affinity Health Plan, a New York-based not-for-profit managed care plan, learned in April 2010 after having to notify more than 400,000 current and former customers and employees that their personal information might have been breached because of the unerased data found on the hard drive of a previously leased copier.[8]

This data exists not just in computer and server hard drives that have been declared obsolete or redundant, but across a wide array of devices, including copiers, printers, scanners, and fax machines.

Copier and printer hard drives are two places where data lurks. Here are a few more.

Computer and server hard drives

For corporate data security experts, protecting the data on these devices is the foundation of their data security policies and procedures. Most people are aware of the significant data security risk posed by failing to eliminate information from computer and server hard drives and understand the need to destroy the data on these devices.

Solid-state drive-equipped devices

Devices equipped with solid-state drives offer improved durability, energy-efficiency, and speed over those equipped with conventional hard drives. More recently, desktop and laptop computer manufacturers have taken advantage of the benefits of solid-state drives to make their devices faster, lighter, and more reliable.

Solid-state drives look like traditional magnetic hard drives, but the data they contain cannot be destroyed by the same methods used for standard hard drives. Solid-state drives require special processing to ensure all data has been removed. For instance, an absence of magnetic components makes solid-state drives impervious to degaussing. Also, currently available hard drive wiping techniques may give the appearance of complete data erasure during verification, but recoverable data may remain due to the unique recording, storage, and organizational characteristics of this technology.

Cell phones, smartphones, and tablets

The consumerization of business IT continues to gain momentum, but the growing number of employees who are allowed to use their own mobile devices, such as smartphones or tablets, to connect to corporate

networks, email accounts, or file-sharing applications can put confidential data at risk. Whether company- or employee-owned, mobile devices have computing power and data storage capacity that rival some desktop and laptop machines and their size and popularity make them vulnerable to loss and theft, substantially increasing the data security risk posed by mobile technology. Unlike computers and servers whose contents are subject to strict security protocols, retired, broken, or employee-owned mobile devices sometimes fall outside the scope of these policies, setting up the possibility of a data breach.

Also keep in mind that many smartphones and tablets are equipped with solid-state technology, making them subject to the same data erasure challenges as other devices using this technology to record, store, and access data.

How to Get Rid of Data, Completely

As the information organizations collect and store increases in quantity and value, the importance of safeguarding that data needs to inform every decision they make about the disposal of their electronic equipment. To preserve the trust of those whose privacy they have promised to protect and to ensure compliance with state and federal regulations, it is essential for these organizations to work with electronics recyclers that take data security as seriously as they do. This checklist will help companies assess whether recyclers have the infrastructure in place to satisfy their data security needs.

Certification

Responsible and secure reuse and recycling hinge on two principles: knowing who will handle old electronics and knowing how they will be handled. Recyclers that have achieved R2, e-Stewards, and National Association for Information Destruction, or NAID, certifications are committed to conforming to recycling industry best practices that regulate environmental and worker health and safety management systems. Certified recyclers are also dedicated to following the latest standards that regulate information destruction and the secure handling, warehousing, and transportation of electronics. Choosing a certified recycler can also minimize the irregularities in environmental protection, worker safety, and security procedures that can result in potential liability concerns for companies sending equipment to be recycled.

Observation

Certification delivers assurances that retired equipment will be processed in a manner that protects employees and the environment from harm, but it should not be the only measure by which a possible recycling partner is evaluated. Contracting with a third-party service provider, such as an electronics recycler, does not relieve a business of its obligation to protect data, so conduct a site visit to observe firsthand the physical security measures in place and confirm that employees

have been background checked and drug screened. Also, determine how hazardous wastes are managed, watch equipment teardown procedures, and examine the equipment used to shred and separate e-waste. Confirm that a recycler's shredders will reduce electronic equipment, such as hard drives, sufficiently to ensure that neither the device nor the data can be reconstructed.

Electronics contain many different types of metal and plastic, as well as hazards such as batteries and mercury bulbs. This means most recyclers depend on downstream vendors to completely process electronic waste. For a company concerned about data security, who a recycler does business with is just as important as how they do business, so request the names and locations of a recycler's downstream partners and find out if the recycler conducts regular, on-site audits to ensure these vendors handle materials according to the same environmental, safety, and security standards as the primary recycler.

Protection

Locate a recycler that not only provides data destruction methods that comply with National Institute of Standards and Technology Special Publication 800-88 Guidelines, but also performs verification of that destruction to be certain all confidential information has been removed from a device. Verification is especially important if a company intends to reuse or resell its IT assets. Realize the data destruction process is only as good as the technicians performing it, so check that a recycler has documented policies that cover employee training on the use and calibration of data destruction equipment and software.

Every organization has different data security requirements so understand which data destruction methods will best meet those needs. Reselling IT assets? Data erasure through overwriting–a process that replaces sensitive data with nonsensitive, random data–allows hard drives to be resold or reused. This process not only overwrites data on the file allocation table, but on all addressable locations. For maximum security, a minimum of three overwriting passes need to be performed. No plans to repurpose hard drives? A degausser's powerful electromagnetic field will destroy data and render a drive useless. These hard drives can then be shredded and the resulting material separated and recycled. Regardless of the method of data destruction, request certificates of destruction to demonstrate that all equipment and data were handled responsibly.

Additional security comes from choosing a recycler that owns its facilities and offers an unbroken chain of custody from collection to transportation to destruction of old electronics. The farther equipment containing confidential data moves downstream, the harder it becomes to protect that data. For this reason, establish from the beginning who will have access to equipment and how it will be handled from the time it is picked up until it is processed. A recycler that is able to provide a complete range of recycling services internally eliminates reliance on subcontractors to process an organization's retired electronics, which improves accountability and streamlines reporting.

As soon as retired electronic equipment leaves a company's premises, any intact data residing on that equipment becomes vulnerable to exposure and can subject that company to a potential data breach incident. This is because companies remain responsible for the security of collected data even after the donation, retirement, or sale of the equipment containing that data. For those organizations with exceptional data security and regulatory compliance needs, locate a recycler that can provide on-site data destruction services. In these situations, a recycler will send technicians equipped with a portable degausser and hard drive crusher to a customer's location, where a company representative can witness hard drives being removed, degaussed, and crushed. The destroyed hard drives are then typically transported in locked containers to a facility for shredding. Need to ensure maximum protection of a company's data and reputation? Inquire about the availability of mobile shredding equipment.

The conscientious collection and analysis of data will continue to yield new insights that will very likely lead to greater efficiency, innovation, and productivity in every industry. But the liability, privacy, and security issues associated with managing the data collected from customers, employees, patients, and students have raised valid concerns. An organization's ability to thrive in this climate will depend on its ability to effectively protect that data. With an awareness of the special risks presented by some data-bearing devices and an understanding of the best methods for diminishing those risks, a company can develop a comprehensive data security policy that will not only protect data throughout its life cycle, but also provide peace of mind to all those who have entrusted their information to a company.

The liability, privacy, and security issues associated with managing data have raised valid concerns. An organization's ability to thrive in this climate will depend on its ability to effectively protect that data.

For more information contact us at:
800.270.8220 or
info.datasecurity@simsmm.com

ENDNOTES

1. "What is big data – Bringing big data to the enterprise," International Business Machines Corp., accessed January 8, 2013, http://www-01.ibm.com/software/data/bigdata/.
2. "Chronology of Data Breaches," Privacy Rights Clearinghouse, accessed January 8, 2013, http://www.privacyrights.org/data-breach/new.
   These parameters applied to the search conducted: all types of breaches selected to display, all organization types selected to display, year 2012 selected to display.
3. Ponemon Institute LLC, "2011 Cost of Data Breach Study: United States," p. 2, March 5, 2012, http://www.ponemon.org/library/tag/cost%20of%20data%20breach.
4. "Chronology of Data Breaches: FAQ," Privacy Rights Clearinghouse, accessed January 8, 2013, https://www.privacyrights.org/data-breach-FAQ.
5. "Fact Sheet: Privacy Legislation in Canada," Office of the Privacy Commissioner of Canada, accessed January 18, 2013, https://www.priv.gc.ca/resource/fs-fi/02_05_d_15_e.asp.
6. "Fact Sheet: Privacy Legislation in Canada," Office of the Privacy Commissioner of Canada, accessed January 18, 2013, https://www.priv.gc.ca/resource/fs-fi/02_05_d_15_e.asp and "Legal information related to PIPEDA," Office of the Privacy Commissioner of Canada, accessed January 18, 2013, https://www.priv.gc.ca/leg_c/legislation/ss_index_e.asp.
7. "Chronology of Data Breaches," Privacy Rights Clearinghouse, accessed January 8, 2013, https://www.privacyrights.org/data-breach/new.
   These parameters applied to the search conducted: hacking or malware and insider types of breaches selected to display, all organization types selected to display, year 2012 selected to display.
8. Privacy Rights Clearinghouse, accessed January 8, 2013, https://www.privacyrights.org/data-breach-asc?title=Affinity+Health+Plan.

Contact us:

1600 Harvester Road • West Chicago, IL 60185

800.270.8220 • info.datasecurity@simsmm.com • www.simsrecycling.com

SIMS RECYCLING SOLUTIONS