ENSURING DATA SECURITY DURING IT ASSET DISPOSITION

WHITE PAPER EXPLAINS IMPORTANT DATA DESTRUCTION AND IT ASSET DISPOSITION TIPS

SIMS LIFECYCLE SERVICES

Responsible Disposition Reduces the 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[1] created each day 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

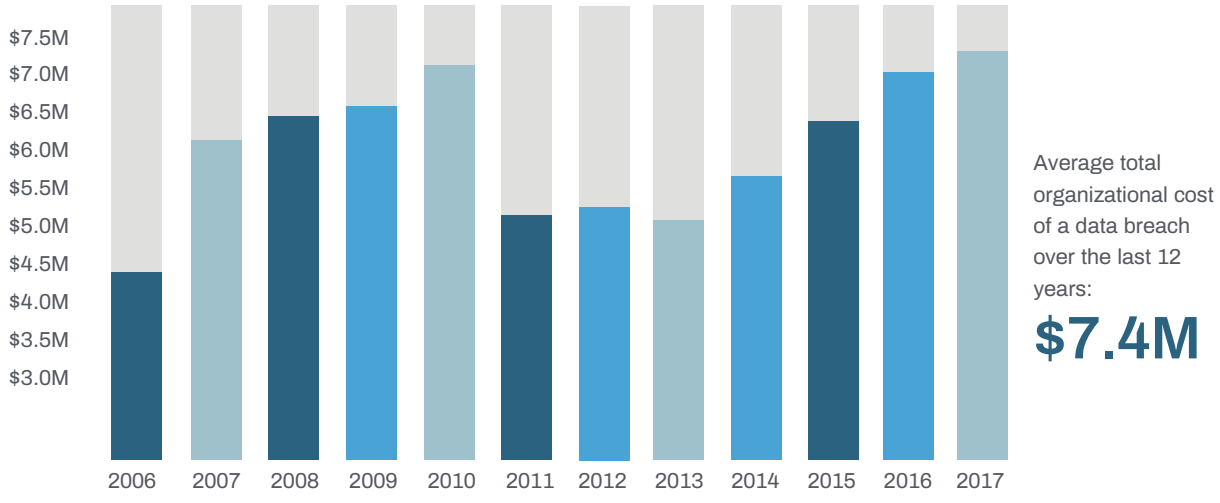
Risk Based Security reported that 4.2 billion records were compromised by 4,149 data breaches in 2016.[2] The average breach costs companies $3.62 million (€2.69 million), according to global research conducted by privacy think tank Ponemon Institute for their *2017 Cost of Data Breach Study: Global Overview*.[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. There are many certifications around the world dedicated to security including,

- The **Transported Asset Protection Association (TAPA)** which was created to prevent cargo theft.
- The **ISO/IEC 27001** - A standard which provides requirements for an information security management system (ISMS), which is a system in place to manage sensitive company information so it remains secure.
- The **National Association for Information Destruction (NAID)** certification which
- describes itself as the standards setting body for the information destruction industry.

These global standards that exist are just the minimum requirements expected from IT asset disposition vendors. Other security measures vary depending on the client and their unique needs.



Ponemon Institute LLC, "2017 Cost of Data Breach Study: United States" (July 2017), p. 9, figure 2.

Where Data Lurks

The actions of hackers and negligent employees or contractors were responsible for more than 918 data breach incidents globally in the first half of 2017.[4] With so much at stake, most data security efforts are justifiably focused on 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 disposal 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.

In fact several Universities have had incidents where printers were hacked. Since printers today are networked devices with hard drives, anything scanned or printed is stored on the device until it is overwritten. A survey by the Ponemon Institute stated that 62 percent of IT security practitioners did not feel confident they could protect their printer-related data. More often than not these printers are not encrypted and can be an easy target for hackers not only when in use, but also upon disposal. The same survey also showed that only 38 percent of respondents felt confident that the data on their printers was wiped before disposal or refurbishment, a figure that will hopefully increase over time.[5]

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 risks 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 similar to traditional magnetic hard drives but are often smaller, more durable and store data on flash memory chips which have no moving parts. 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. It is important to validate that any data destruction methods being implemented are truly removing all data from the solid-state drive on the flash translation layer and all sectors.

> 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.

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. Their size and popularity however make them more 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 IT asset disposition vendors that take data security as seriously as they do. This checklist will help companies assess whether vendors have the infrastructure in place to satisfy their data security needs.

Certification

Responsible and secure IT asset disposition hinges on two principles: knowing who will handle old electronics and knowing how they will be handled. IT asset disposition vendors that have achieved Responsible Recycling (R2) or related certifications are committed to conforming to the IT disposal industry best practices that regulate environmental and worker health and safety management systems. Certified vendors are also dedicated to following the latest standards that regulate information destruction and the secure handling, warehousing and transportation of electronics. Choosing a certified IT asset disposition vendor 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 disposed.

Observation

Certifications deliver 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 partner is evaluated. Contracting with a third-party service provider, such as an IT asset disposition vendor, 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 assets are tracked and managed, and watch equipment teardown procedures. If offered, utilize on-site shredding to reduce electronic equipment, such as hard drives, sufficiently ensuring that neither the device nor the data can be reconstructed.

Most organizations who manage end-of-life IT equipment depend on downstream vendors to completely process electronic waste. For a company concerned about data security, request the names and locations of the IT disposal vendor's downstream partners and find out if the vendor conducts regular, on-site audits to ensure these downstream partners handle materials according to the same environmental, safety and security standards as the primary vendor.

Protection

Locate an IT vendor that not only provides data destruction methods, 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 for documented policies that cover employee training on the use and calibration of data destruction equipment and software.

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.

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 vendor that owns its facilities and offers an unbroken chain of custody from collection to transportation to destruction of old electronics. The farther your equipment data moves downstream, the harder it becomes to protect the data stored. 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 vendor 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. Every organization has different data security requirements so understand which data destruction methods will best meet those needs.

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.

> 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 organizations with exceptional data security and regulatory compliance needs, locate a vendor that can provide on-site data destruction services. In these situations, a vendor will send technicians equipped with data destruction equipment to a customer's location. Once on-site, a company representative can witness hard drives being removed, data destroyed and, if requested, the hard drives can be physically destroyed. These destroyed hard drives should then be transported in locked containers to a facility for further processing. Need to ensure maximum protection of a company's data and reputation? Inquire about the availability of mobile shredding equipment.

Data eradication or hard drive degaussing?

In closing, 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 unique risks presented by data-bearing devices and an understanding of the best methods for diminishing those risks, a company can develop a comprehensive data security policy. This policy 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.

ENDNOTES

1. "What is big data – Bringing big data to the enterprise," International Business Machines Corp., accessed January 8, 2016, http://www-01.ibm.com/software/data/bigdata/what-is-big-data.html
2. "2016 Year End Data Breach QuickView Report," accessed July 12, 2017, https://pages.riskbasedsecurity.com/2016-ye-breach-quickview
3. Ponemon Institute LLC, "2017 Cost of Data Breach Study: Global Overview," accessed July 12, 2017, https://www.ibm.com/security/data-breach/
4. "The Reality of Data Breaches," accessed February 16, 2018, http://breachlevelindex.com/assets/Breach-Level-Index-Infographic-H1-2017-Gemalto-1500.jpg
5. "Printer security: Is your company's data really safe?", accessed July 18, 2017, http://www.computerworld.com/article/3074902/security/printer-security-is-your-companys-data-really-safe.html.

Contact Us:
info.national@simsmm.com
www.simslifecycle.com