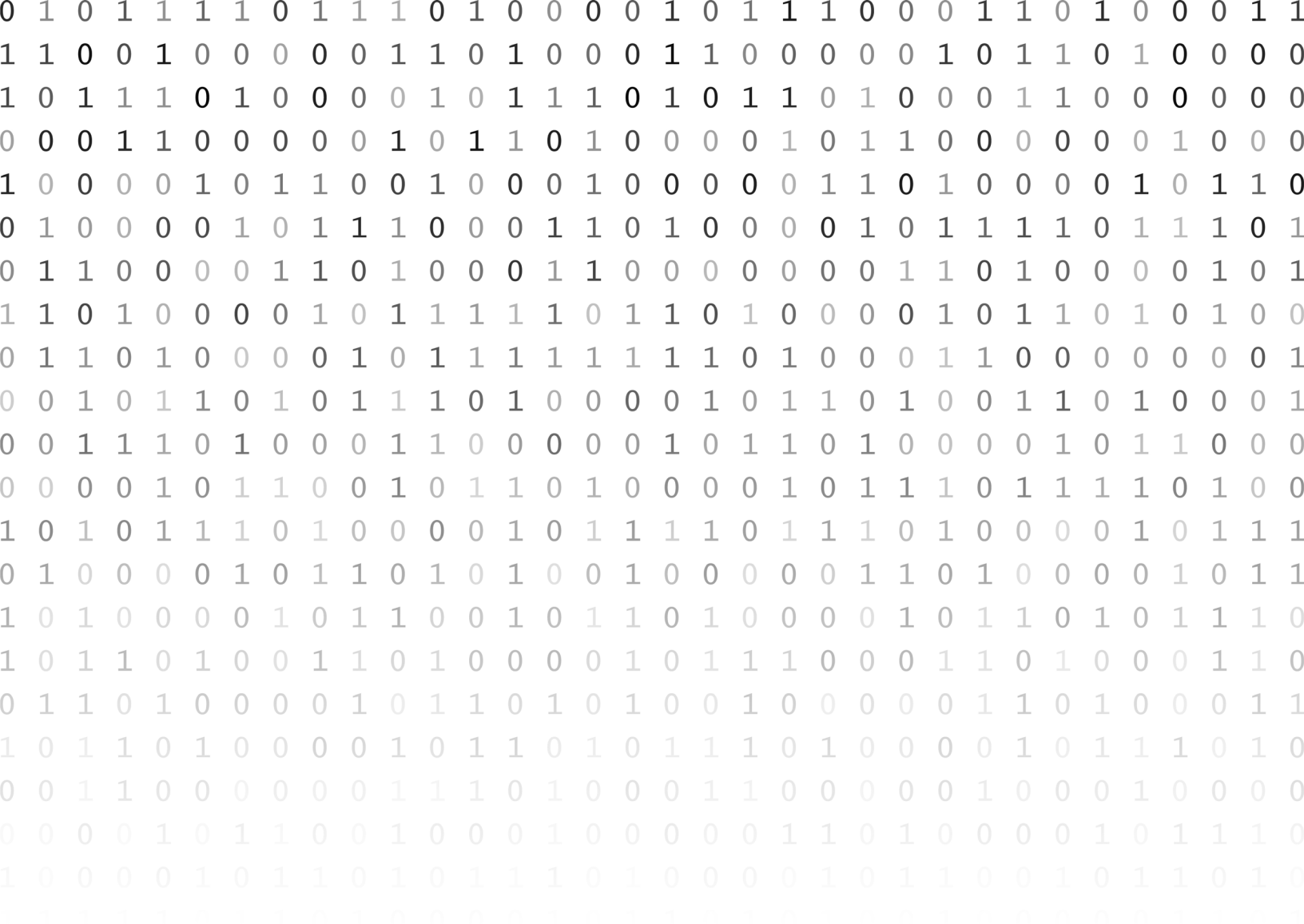

Understanding Data Destruction:

HOW TO PROPERLY PROTECT YOUR BUSINESS

LIQUIDTECHNOLOGY

This document is designed to provide a practical understanding of data erasure and disc sanitization, why it is essential for security, legal and business concerns and the methods and techniques accessible to the reader.

Executive Summary

In an effort to compete within the scope of their industry, and to ensure top-tier speed, reliability and security, corporations upgrade their computer network systems on a regular basis. In many cases, the older computer equipment is moved to another area of the business where they are restructured to perform functions of lesser security importance.

When a company no longer has a need for their antiquated equipment, it may be donated to charity, offered to employees or sold or auctioned off on the secondary market as a reliable source of working capital. Another option is for the hard discs to be rendered completely inoperable through physical destruction. In each of these scenarios, it is extremely important that complete data erasure, disc sanitization or physical destruction be successfully conducted to prevent sensitive information from being viewed or collected by persons unauthorized.

Because IT hardware obsolescence is a natural force in today's technology-driven industry, the secondary computer market has become a reliable resource of revenue for corporations that regularly upgrade their systems. If the data is not completely destroyed before the equipment begins its secondary purpose, the organization can be exposed to a variety of negative effects, such as:

- Privacy/identity litigation
- Violations of federal regulations
- Infringement of intellectual property
- Disclosure of sensitive business strategies
- Breach of software licensing agreements
- Environmental damage
- Negative publicity

For these reasons, it is critical that every IT director and CIO institute a formal process that ensures all sensitive data contained on storage media is thoroughly erased and/or destroyed prior to disposal or reuse of the equipment.

Why is Data Destruction so important?

According to a 2005 IDC study, only 37 percent of commercial entities have a formal PC end-of-life and recycling policy already in place. This means that those companies that do not have a similar policy in effect are placing the privacy of their employees, partners and customers at severe risk.

In many cases, the destruction of the sensitive information is left in the hands of low level IT employees, who don't have the tools or the budget necessary to perform a task of such critical proportion. All too often, in an effort to keep operational expenses low, companies rely on data deletion and disc formatting as means of destroying sensitive data. Tech-savvy thieves understand this and therefore use the secondary PC market as a means of collecting sensitive information that can be used to their benefit. What results is a flurry of negative reactions to the organization that thought their vital information was destroyed. Litigation issues, financial risks and many other problems resulting from recovered data can quickly bring a fortuitous company to the brink of devastation.

What Types of Businesses Should Exercise Secure Data Destruction?

Every business that values their and their customer's privacy and security should have a data destruction policy in place. Every key decision-maker of enterprise or organization must provide secure data destruction in order to ensure that all sensitive business data is effectively eliminated from any and all storage media before its disposal for whatever reasons; recycling or remarketing a computer, returning a PC that was leased, or for companies that are upgrading their IT assets.

How can Complete Data Destruction be Attained?

Complete data destruction can be performed in-house by personnel within the organization's IT department or the task can be outsourced to a reputable IT asset management company. While many companies may feel compelled to save money by allowing their own employees to handle the data destruction, this often fails to meet the "checks and balances" demand of business. In many situations, drives are lost, stolen or misplaced. To ensure that delicate information does not get in the wrong hands, there needs to be a policy in place that guarantees accountability and accuracy.

Methods of Data Erasure/ Destruction

DEGAUSSING

Degaussing is a technique used in data destruction that incorporates powerful magnetic fields to effectively erase and eliminate all of the data recorded on a magnetic storage device such as a hard drive. Once a hard drive has been degaussed, it is completely inoperable.

The advantage of using the degaussing method of data destruction is that the process is relatively quick and effective. In addition, if performing the job in-house, purchasing the degaussing machine is likely to be a one-time investment.

The disadvantages of degaussing include the inability to fully guarantee all of the data has been reliably destroyed, risks of equipment in close proximity being affected by the magnetic field and the method is only effective on magnetic media. Additionally, while degaussing does effectively erase older drive technologies; modern storage media is constructed with reinforced shielding, thus requiring a much stronger magnetic field to perform the same function.

PHYSICAL DESTRUCTION OF THE HARD DRIVE

The primary method of physical hard drive destruction is disc shredding. In this process, the hard drive is fed into a machine that shreds it into hundreds of smaller pieces. The advantage of physical destruction is that it offers the opportunity to destroy multiple forms of recordable media like hard drives, floppy discs, CDs and DVDs in large volumes. Once a hard drive has been physically destroyed, it has been rendered completely inoperable, thus preventing any recovery of data through conventional means.

The primary disadvantage of physical destruction is that it prevents the opportunity for the revenue gains available through secondary market resale. Physical destruction of recordable media also presents certain environmental risks and poses potential violations of EPA regulations. Lastly, if the destruction is not performed correctly, sensitive data can still be recovered from the individual fragments.

SOFTWARE DATA DESTRUCTION/ERASURE

Software data destruction is one of the most effective means of eliminating sensitive data from the disc, while maintaining the functionality of the disc for re-use or resale. This is a process in which each drive sector of the disc is overwritten with meaningless data.

The advantage of using software data destruction is that it protects your investment, allowing you to use the equipment in another area of your business or as potential working capital through resale. Software effectively eliminates all traces of data on the disc and it can be utilized over a network to target certain drives. This technique also enables the user the opportunity to create auditable reports of the destroyed data, thus ensuring compliance with federal standards and meeting the demands of external and internal auditors. Reports typically include the name of the technician who performed the data destruction, the drive's serial number, the extent of the data erasure, the name of the procedure used and any errors that were encountered during the erasure process.

The disadvantages of using software often lie in the individual or individuals assigned and the technologies used to carry out the task. When performed in-house, it is not uncommon for ineffective software to be used. Not all data erasing software affords the same results, as some freeware versions only erase to a certain point, unable to access hidden or locked directories on the disc. If this occurs, sensitive data may still reside on the disc. Additionally, software data destruction is not an option if the disc is overwrite protected or physically damaged.

Ineffective Means of Dealing with Data Destruction

In an effort to cut the costs often associated with data destruction, many companies and organizations may choose alternatives to outsourcing their security needs. In many cases, they do so unaware of the potential risks associated with the ineffectiveness of the following procedures.

RE-FORMATTING

Re-formatting a hard drive does not deliver reliable data destruction. When a hard drive is re-formatted, all of the data still resides on the disc. The process simply makes changes the File Allocation Table (FAT) of the drive, erasing only the address tables that point to the data, not the actual files themselves. After a hard drive has been re-formatted, it is very easy for someone to access the older files using readily available software.

Ineffective Means of Dealing with Data Destruction (continued)

STORAGE

When a data destruction decision cannot be reached, it is not uncommon for the equipment to be stored in a locked room. This is considered by many managers as an effective means of preventing the discs from falling into the wrong hands, and in fact, storage is one of the most commonly used methods of data security in business today. Unfortunately, it is entirely too easy for anyone in the company to access the storage room and obtain critical information about their fellow employees or the company they work for. If a company does not have on-site storage capabilities, off-site storage is often utilized which results in added expenditures for antiquated equipment.

Considerations

Data destruction is a vital component to an organization's overall security efforts. Therefore, it is essential that every company have a data destruction policy in effect. Whether the choice is made to perform the data erasure in-house or through a reputable IT asset management company, there are specific guidelines and criteria which should be met to ensure an effective enterprise-class data erasure strategy so your security objectives remain intact.

When developing an in-house data erasure directive, the following criteria should be met:

INDUSTRY REGULATIONS

There are many industry-specific regulations that need to be taken into consideration when developing a data erasure policy. Some of the more common regulations include:

- FACTA (Fair and Accurate Credit Transactions Act) – Requires the destruction of all papers containing personal consumer information.
- GLB (Gramm-Leach Bliley) – Federal law requiring banking and financial institutions to describe how they protect consumer confidentiality and security.
- SOX (The Sarbanes-Oxley Act) – Mandate that holds top executives personally accountable for the accuracy and timeliness of their company's financial data destruction.
- CAL SB1386 (The California Information Practice Act) – This law requires companies to notify California residents if their personal information has been accessed illegally.

Considerations (continued)

- HIPPA (Health Insurance Portability and Accountability Act) – Requires certain security and confidentiality measures to ensure the protection of health information.
- PCI DSS (PCI Data Security Standard) – Set of standards produced by the PCI Security Standards Council for enhancing payment account data security through security management, network architecture, software design, policies, procedures and other critical protective measures.

INTERNAL POLICIES

Guidelines and policies should be written to enable the effective enforcement of the company's data destruction procedure. Said policies should reflect the requirements associated with the industry and federal regulations.

D.O.D. & NIST COMPLIANCE

The U.S. Department of Defense Standard otherwise known as D.O.D. 5220.22M, is the guideline that describes the methods and standards by which classified data needs to be secured by government employees and their contractors. The National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure.

The most current documentation addressing secure data destruction is the NIST special publication 800-88.

AUDITABLE SOLUTIONS

To ensure that your employees carry out the process to the specifics detailed in your written policies, every aspect of the data destruction should be completely auditable.

Enterprise-Class Software Considerations

As stated earlier, not all software data erasure solutions are created equal. To satisfy security requirements and maximize confidentiality, enterprise-class data erasure software should offer the following capabilities:

- The software should be compatible with, or offer the capability to run independently of, the operating system loaded on the drive.
- The software should be able to overwrite the entire hard drive independent of any limitations the BIOS or firmware may have in effect.

- The software should offer the capability to run independent of the hard drive being sanitized, regardless of ATA, SCSI or IDE classifications.
- The software should be able to detect, access and overwrite locked and/or hidden sectors as well as spare hard drives in RAID configurations.

Quality software data erasure solutions will provide auditable reports upon successful completion of disc sanitation and offer the capability to ensure the integrity of the reports through digital signatures.

Choosing an IT Asset Management Company

For many companies, a reputable IT asset management company offers a cost-effective and reliable solution for secure data destruction. But, before you choose a company to handle the onsite or offsite destruction of your sensitive data, there are certain attributes you should look for. When evaluating an IT asset management company, be sure to ask the following questions:

- Does the company have an errors and omissions insurance policy (minimum of USD 1 million) in the case they fail to perform the data destruction properly?
- Are their services compliant with D.O.D. 5220.22M and NIST?
- Can they provide references?
- Do they offer onsite or offsite options for data destruction and support?
- Can they provide auditable reports of the data destruction, including serial numbers?
- Do they use proven software and data erasure techniques?
- Do they provide cost-effective alternatives to data destruction or offer combined solutions?
- Do they offer chain of custody documentation?
- Does the company have essential industry certifications?

Some certifications to look for include:

E-STEWARDS CERTIFICATION

Being certified as an e-Steward is one of the most telling ways to determine whether or not an e-waste recycler adheres to responsible recycling standards. In order to become e-Stewards Certified, a recycler must meet the following criteria:

- Pass annual 3rd party audits
- Demonstrates the downstream disposition of all hazardous waste throughout their supply chain
- Operate a management system to achieve compliance with all laws
- Does not export e-waste to developing countries or use prison labor

R2 CERTIFICATION

R2 certification is the EPA's way of ensuring that a recycler is fully adherent with the agency's eco-responsible measures of disposing of e-waste. Officially called "Responsible Recycling practices for Use in Accredited Certifications Programs," the R2 Standard was initiated in 2008.

Most recently, the program was updated in 2013 to include greater transparency requirements and additional best practices.

NAID CERTIFICATION

The NAID AAA Certification Program is a voluntary program for NAID (National Association for Information Destruction) member companies that provide information destruction services. Developed by information security professionals, the program is recognized by private and governmental organizations around the world. Through rigorous, unannounced audits, NAID certified companies have demonstrated that they ensure the security of confidential material throughout all stages of the destruction process, this

includes such areas as operational security, employee hiring and screening, the destruction process, responsible disposal, and insurance.

NAID AAA Certification helps companies meet laws and regulations that protect customer information, including:

- The FACTA Final Disposal Rule which requires the destruction of all consumer information before it is discarded.
- The FACTA Red Flags Rule which requires audits of data-related vendors with access to personal information of customers.
- Technical, administrative and physical safeguard requirements under the HIPAA Security Rule.
- Payment Card Industry (PCI) security standards.

ISO 14001 CERTIFICATION

The ISO is the International Organization for Standardization that's responsible for setting international standards for businesses, government and society. The ISO 14000 family of standards addresses several aspects of environmental management. More specifically, a company that has met the guidelines as outlined in ISO 14001, has been found to:

- Meet current environmental regulations
- Provide customers, the community and regulatory agencies with an assurance on environmental issues
- Support its own environmental policies, plans and actions
- Provide its employees with assurances that they are working for an environmentally-responsible organization
- Receive annual external audits to ensure all guidelines are being met

OHSAS 18001 CERTIFICATION

OHSAS 18001 is an internationally-applied standard for occupational health and safety management systems. It is a set of standards that were designed by The Occupational Health and Safety Advisory Services (OHSAS) Project Group in 1999 to help control and improve health and safety performance in the workplace.

In order to be certified, a company must meet certain workplace safety requirements, such as air quality, noise levels, regular machine inspections, and more. What this means to consumers is that OHSAS 18001 certified companies, provide their workers with the safest workplace environment possible, thereby reducing injuries and illnesses as well as mechanical downtime. This translates into greater efficiency and productivity which helps keep costs down.

Summary

In summary, an effective data erasure/destruction strategy is your first line of defense against identity theft, breach of confidentiality agreements and stolen information. Each data disposal or sanitation method has its advantages and disadvantages, and a decision should never be made on price alone. As the CIO or IT director, it is essential for you to choose a data destruction strategy, either in-house or outsourced, that ensures your company's security, maximizes ROI and minimizes business risk. It is imperative that you know under all circumstances that the proper policies and procedures are in place in order to be protected from the risks and liabilities associated with mishandled proprietary data.

When the security of your business, customers, employees or partners is made vulnerable, you are placing your entire business at significant risk. Sensitive data must be completely destroyed or erased in order to protect those who have a stake in your business. The only way to ensure this is accomplished is to have verifiable proof of the data erasure or destruction through an auditable means.

LIQUID TECHNOLOGY

LIQUID TECHNOLOGY, INC.
BROOKLYN ARMY TERMINAL
140 58TH STREET
SUITE 8C, BOX 33
BROOKLYN, NY 11220

MAIN TELEPHONE **800-797-LIQUID (797-5478)**
FAX **(212) 214-0424**
EMAIL **BUYER@LIQUIDTECHNOLOGY.NET**

LIQUIDTECHNOLOGY.NET

REGIONAL OFFICES:

LOS ANGELES, CA **(949) 753-5124**
SAN FRANCISCO, CA **(650) 249-6368**
NORWALK, CT **(203) 242-8760**
FORT LAUDERDALE, FL **(954) 376-5794**
CHICAGO, IL **(312) 382-8208**
CAMBRIDGE, MA **(617) 737-6100**
DALLAS, TX **(214) 256-4298**
MCLEAN, VA **(703) 533-3100**

CERTIFICATIONS:

e-Stewards CERTIFIED
R2 2013 Responsible™ Recycling
ISO 14001
AAA CERTIFIED
OHSAS 18001