blancco

Protecting Your Enterprise with an Effective Data Erasure Strategy:

Steps to Ensure the Removal of Sensitive Information
When IT Asset Ownership Changes

Blancco White Paper

Improper Data Erasure Can Pose Serious Business Risks

A corporation would never consider operating without property and casualty insurance. The financial, legal, and public relations-related risks are simply too great. But every day, businesses operate without effective data leak prevention strategies.

What's the risk? Consider this scenario reported in a major tech-industry publication:

"An Idaho Power Company found itself in an uncomfortable situation as it attempted to track down several unscrubbed disk drives that had been sold on eBay. The drives contained confidential employee information, correspondence with customers and memos that discussed proprietary company information. The company said it hired an outside contractor to recycle about 230 SCSI drives. The contractor had sold 84 of those drives to 12 different parties using the online auction website."

Unfortunately, these kinds of situations are becoming commonplace. As rapidly-evolving technological innovation has caused the acceleration of IT hardware obsolescence, the secondary market for PC, server, and storage is becoming a haven for information thieves who seek to retrieve and exploit business and personal data from improperly erased hard drives.

Conventional attempts to erase business data on the millions of computer hard drives discarded by companies each year often fail, leaving data to be resuscitated by unscrupulous individuals. And, many third-party vendors who claim to wipe hard drives before disposing of them don't do a thorough job of completely removing the data.

Despite this, a 2005 IDC study suggests that **only 37% of commercial entities have a formal PC recycling and end-of-life asset policy in place.** In addition, for enterprises with operational data centers, managing these processes for IT equipment such as servers and storage arrays is even more demanding.

> *A poorly designed data disposal process can expose an organization to a variety of legal, financial, and public relations risks.*

The report also indicated that similar percentages apply to data destruction.

Beyond the inconvenience and embarrassment of proprietary data getting into the wrong hands, there are many more serious repercussions of failing to effectively erase business data prior to sale or disposal. Organizations can be exposed to a variety of quite damaging legal, financial, and public relations-risks including identity/privacy litigation, violations of federal regulations, environmental damage, infringement of intellectual property rights, disclosure of business strategies, breach of software licensing agreements (license harvesting) and negative publicity.

It is, therefore, a critical responsibility of every CIO and IT Director to develop, document, communicate, and implement formal processes that ensure that all sensitive business data is effectively erased from all storage media prior to its disposal.

This white paper is intended to help educate enterprise IT organizations about the essential elements of a formal data erasure policy, so that they can effectively protect themselves from the costly legal, regulatory, financial, and public relations nightmares that can result from incomplete or improper data erasure.

Why Is Data Erasure So Important?

Most information assets contain volumes of confidential data, which organizations have a legal, moral, and fiduciary responsibility to protect. Enterprises without clear data erasure policies or those with poorly designed asset disposal processes can expose their organizations to a variety of risks, including:

Customer, Partner, and Employee Confidence Risks – Customers and employees depend on the security of the personal and business information they entrust to an organization as part of their working relationship. Failure to effectively erase this information upon the disposal of an IT asset or storage device can result in damage to a brand and/or company image, falling stock prices, the loss of customers and business partners, and negative publicity. It can also result in high employee turnover and can impact day-to-day business operations and internal information security.

1. Source: Macworld.com, "Utility's Disk Drives and Data sold on eBay", May 8, 2006.
2. Source: IDC Report, "Trash to Treasure: Old PC Equipment Poses Risks and Opportunities", March 2005

1

Protecting Your Enterprise with an Effective Data Erasure Strategy:
Steps to Ensure the Removal of Sensitive Information When IT Asset Ownership Changes

WWW.BLANCCO.COM

Compliance/Audit Risks - A host of strict industry standards and government regulations require organizations to mitigate the risks of unauthorized exposure of confidential data. Organizations in regulated industries must have a gapless audit trail and evidence of steps taken to prevent leakage of confidential information. Examples of pertinent regulations include:

- **HIPAA** (Health Insurance Portability and Accountability Act) requires safeguards to protect the security and confidentiality of protected health information.

- **FACTA** (Fair and Accurate Credit Transactions Act) requires the destruction of papers containing consumer information such as name, address, SSN, credit information, and data compiled from this information.

- **GLB** (Gramm-Leach Bliley) is a federal law requiring banking and financial institutions across the U.S. to describe how they will protect the confidentiality and security of consumer information.

> *Organizations in regulated industries must have a gap less audit trail as evidence of the steps they have taken to prevent leakage of confidential information.*

- **CAL SB1386** (The California Information Practice Act). The law requires companies that own or have access to personal information of California residents to notify them if their data have (or may have) been accessed illegally.

- **SOX** (The Sarbanes-Oxley Act) mandates corporate governance to stringent accounting and reporting control standards and holds top executives personally responsible for the accuracy and timeliness of their company's financial data — under threat of criminal prosecution. Any data that has not been erased or rendered irretrievable at the end of the life of an IT asset is likely to be a violation of SOX.

Litigation/Legal Risks - Identity theft is one of the fastest growing crimes. According to the Federal Trade Commission, identity theft was the top consumer complaint in 2006 for the seventh year running, accounting for 36% of all complaints filed with the agency that year. A carelessly discarded hard drive containing confidential data (e.g., credit card details, social security numbers, or contact information) can easily result in identity theft and expose an organization to negative publicity and costly litigation.

Software Licensing Risks – Application or system software that remains on a hard drive when an asset changes hands may violate site-licensing terms from the software developer. Also, the reallocation of a server to another department or division can also breach a software license, and can incur costly fines.

Data Erasure Methods

Enterprises have traditionally approached data erasure from a tactical, ad-hoc, or "point-solution" perspective. Unfortunately, the complex issues associated with data erasure require a more strategic approach that involves multiple decisions across several important areas to meet the needs of today's enterprise business environment. Advantages and disadvantages that are associated with these issues include:

Physical Destruction - With physical destruction, hard drives and other storage media are destroyed to prevent access to data. This involves either shredding the drive into tiny pieces or drilling a series of holes into the hard drive platters. This approach doesn't always destroy the data, but makes the drive inoperable, thereby preventing data recovery by ordinary means.

<u>Advantages</u> - This approach is an effective way of preventing any subsequent data recovery if the procedure is carried out correctly. Large amounts of media can be destroyed at once, and different forms of media (such floppies, CDs, DVDs, or removable drives) can be destroyed simultaneously with the magnetic hard drives.

<u>Disadvantages</u> – Physical destruction neglects to recover any residual value for the hard drive; so this approach is not viable with expensive, large-capacity drives that could be reused within the enterprise or sold on the secondary market. Due to the cost of the equipment required, destruction is typically outsourced, thereby increasing the possibility of exposure of confidential data. Physical destruction also poses an environmental risk due to the toxic debris created, possibly breaching EPA regulations. Finally, if performed incorrectly, data can still be recovered from the remaining fragments of the storage media.

3. Source: FTC, "U.S. Senate Special Committee Report on Aging", May 2006

Degaussing - Degaussing a hard drive uses strong electromagnetic fields, ideally destroying all the magnetically recorded data on the drive and renders the drive inoperable.

Advantages – Degaussing is fast and capable of destroying all data on a hard drive or other magnetic media. The purchase of a degaussing machine is usually a one-time investment, which mitigates costs.

Disadvantages – While degaussing ensures the destruction of older drive technologies, newer drives with thicker shielding require a stronger electromagnetic field to ensure complete erasure. Unfortunately, with variances in drive designs, there isn't a uniform way to guarantee that degaussing will completely erase all of the data and protect the enterprise from a security breach.

Also, this option can only be used on magnetic media, which will not reliably destroy all the data if procedures are not carefully followed. Due to the nature of magnetic fields, care must be taken to prevent nearby components and equipment from being damaged.

> *"Format" commands only change the drive's File Allocation Table (FAT) and do not erase any data. The data is still intact and can be easily recovered using commercial software solutions.*

Re-Formatting the Drive – Despite the growing awareness of the ineffectiveness of re-formatting as a data erasure method, many organizations still remain ignorant of its security risks.

Advantages – There are no advantages to this method since the data is not completely erased.

Disadvantages – All "Delete" and "Format" commands only change the drive's File Allocation Table (FAT) and do not actually erase any data. Only the address tables pointing to the data files are erased. The data is still intact and can be easily recovered using software utilities, readily available on the Internet.

Until the "deleted" data is completely overwritten with new data, it still exists and poses significant security risks for identity theft, litigation and lawsuits, and possible incarceration. As a result, this method of data destruction should be avoided.

Software Overwrite Solutions – Software solutions that overwrite data on top of existing information employ a process of writing patterns of meaningless data into each of the drive sectors using a combination of 1's and 0's.

Advantages – This option is the most effective and convenient way of permanently destroying data. Once the device has been erased, it can be reused or resold, preserving the functional and remarketing value of the asset. In some cases, the tool can also be deployed over a network to target specific computers or drives. It can also produce reports verifying proper completion and including a defect log that lists any bad sectors that could not be overwritten by the software. Reports satisfy compliance requirements and often include the drive serial number, extent of data erasure, name of the erasure procedure, the technician, and any errors that occurred during the erasure process.

Disadvantages – Many organizations still rely on older standards and recommendations for *three* to *seven* overwrite passes, which combined with inadequate software tools, makes the process of wiping a standard PC drive take several hours. In addition, not every overwrite program offers complete security. For example, freeware overwriting tools available on the Internet are unable to access the entire hard disk which might include hidden/locked directories or remapped sectors of the drive. In the event of incomplete results, some data may remain intact, compromising security. Also these solutions cannot be used if the storage media is damaged or can't be over-written.

Dead Storage – Unable to make a decision from fear of a security breach or from simple lack of awareness of the alternatives, many companies simply store their hard drives and computers to ensure that data doesn't fall into the wrong hands.

In fact, a large segment of enterprise organizations choose storage as their primary method of asset disposal. According to a survey of 320 IT professionals conducted by Gartner Research during a recent IT conference, *storage was the third-most-common method* of dealing with obsolete PCs and servers. Of the companies that were surveyed, approximately one-quarter indicated that they store over 30 percent of their obsolete PCs and servers.

3

Protecting Your Enterprise with an Effective Data Erasure Strategy:
Steps to Ensure the Removal of Sensitive Information When IT Asset Ownership Changes
WWW.BLANCCO.COM

Advantages – Stored equipment and hard drives can be re-purposed to other departments quickly and easily, which can reduce installation time and acquisition costs.

Disadvantages – When computer equipment is stored, there is a tendency for employees to pilfer that equipment — particularly hard drives— thereby creating the very security risk that the storage was intended to avoid. Stored equipment can also yield a negative value due to the rapidly depreciating nature of technology equipment. This disadvantage grows as the cost of storage increases and the value of the equipment plummets. Further, if the application and system software is not de-installed upon asset transfer, the enterprise could be out of compliance with the terms of their software license.

> *Approximately one-quarter of companies surveyed indicated that they store over 30 per-cent of their obsolete PCs and servers.*
>
> *- Gartner Research "I.T. Asset Management and Asset Disposition" November 2005*

A matrix of the advantages and disadvantages of data security measures is illustrated below in Figure 1.

Figure 1: A Data Security Measures Matrix

Advantage	Do Nothing	Format Drive	Physical Destruction	Software Overwrite	Storage
Peace of Mind	No	No	Yes	Yes	No
Reduced Risk	No	No	Yes	Yes	No
Auditable Compliance	No	No	Yes	Yes	No
Proven Solution	No	No	Yes	Yes	No
Reputation	No	No	Uncertain	Yes	No
ROI	No	Yes	Uncertain	Yes	No
Future Proof	No	No	No	Yes	No

Data Erasure Methods

In order to mitigate the risks of information fraud while ensuring compliance with government regulations, privacy concerns, and intellectual-property rights issues, it is the responsibility of every company to design effective data leak prevention policies and data erasure procedures for IT assets destined for disposal or re-sale.

Here are seven important steps to formulating a corporate-wide data erasure policy:

1. Determine the Most Feasible Solution – Each company's data erasure policy should be based on several business factors such as the size of the organization, the frequency of data erasure and disposal, and specific industry requirements. For example, purchasing expensive data erasure equipment may not be financially feasible for a small business. On the other hand, storing thousands of outdated computers is never feasible for a large enterprise since it usually presents a security risk. To determine the most effective solution, businesses should assess their existing resources and add outside expertise where resources are lacking. Enterprises should also plan for future needs as organizational expansion and/or acquisition can alter requirements and deployment options.

> *Most enterprises have a budget for IT equipment and services, but few have one for data erasure and asset disposal.*

2. Calculate Costs and Formulate a Budget – Most enterprises have a budget for IT equipment and services, but few have one for data erasure and asset disposal. While there are several alternatives, each has risks which carry a cost. By deploying an effective data erasure strategy, an enterprise can often recoup the remaining value on equipment by reselling it within two to three years after acquisition. Typically IT assets are fully amortized in three years. The remaining remarketing value (RMV) is not related to amortization schedule. However, somewhere after 3 to 5 years (servers and storage hold their value longer) the RMV will go to zero (but the disposal cost remains) and the asset becomes a liability.

4. Source: Gartner Research, "IT Asset Management and Asset Disposition", November 2005

Protecting Your Enterprise with an Effective Data Erasure Strategy:
Steps to Ensure the Removal of Sensitive Information When IT Asset Ownership Changes
WWW.BLANCCO.COM

3. Assign Roles and Responsibilities – Where will the ultimate data erasure decision lie? Will it be with a "C-Level" business executive, an IT Director, or a Purchasing Manager? Data erasure is not a technical or operational issue; it is a risk and liability matter. As a result, the decision-maker should be the individual most impacted if something goes wrong, such as a corporate risk manager or security architect. In either case, data erasure is a process that requires an owner. Additional personnel matters include determining the number of people required for data erasure, where they will be located and what role Human Resources will play. Since personnel costs can be significant, staffing requirements should be considered equally with technical and procedural issues.

4. Pick the Disposal Location – The facility where data erasure is performed can impact both the quality and security of the erasure process. For example, on-site data erasure provides the most secure option by ensuring that sensitive data doesn't leave the enterprise. Using an off-site or third party facility to perform the data erasure adds steps to the process, which require verifiable facility security and documentation. Important questions to ask include: Does the location provide a Statement of Work (SOW) detailing the steps in their erasure procedures? Can they provide certificates for regulatory compliance reporting? Have they installed security cameras for surveillance in designated work areas? Do they use sealed and secure containers to prevent unauthorized access during shipping? One effective option is to use a combined approach where both on-site and off-site facilities are employed. For example, an enterprise could designate storage media with the most sensitive business data for internal erasure, while allocating media with less-sensitive information for off-site erasure and disposal.

5. Choose A Qualified Service Provider – When considering the person or company responsible for data erasure, two factors to consider are control and cost. A policy that uses internal employees or brings outside service providers on site, provides the greatest control, but incurs higher costs. Shipping media to an off-site location affords a lower cost, but yields less control. Both options are viable, but risk versus cost considerations must be weighed.

6. Plan Desktop/Data Center Device Management – Data Center equipment is deployed, run, and managed differently from desktop PCs and notebooks. As a result, the process of removing storage devices from equipment such as a network server or array to replace the storage media designated for erasure can impact essential business functions. Servers or storage arrays that are running mission-critical applications can't be easily powered-down or decommissioned without costly time-consuming procedures to bring them back online. The sheer volume of this task may make it more cost-effective to bring in qualified experts rather than risk disruption of crucial business functions that might be caused by inexperienced employees trying to perform the task. Before deciding, ask: Do internal employees have the skills and the time to properly perform the tasks given their existing priorities? Might it be more cost effective to pay outside experts if they can complete the process more quickly and with less or no down time? Will using outsiders yield more effective results or create additional, more costly problems?

> *The way in which devices are removed from a network to access storage media designated for erasure may impact essential business functions.*

7. Research Regulatory and Reporting Requirements – Any public and private company in a regulated industry that handle sensitive information must understand the necessity of generating an audit trail and producing the reports required to comply with federal and/or state regulations regarding asset disposal and data erasure. Reports should include lists of the disposed or erased items, their serial numbers, how the data was erased or the asset was destroyed, and the disposal procedure(s). The advantage of enterprise-grade software overwriting solutions is that they can generate these reports and help protect enterprises from compliance litigation.

Protecting Your Enterprise with an Effective Data Erasure Strategy:
Steps to Ensure the Removal of Sensitive Information When IT Asset Ownership Changes

WWW.BLANCCO.COM

Considerations When Determining an Enterprise-Class, Data Erasure Strategy

There are several components that comprise an effective en-terprise-class data erasure strategy. Some of the critical ques-tions to ask and essential criteria to consider when developing data leak prevention and asset disposal policies include:

- Regulations - What specific industry regulations or legisla-tion (e.g. GLB, PCI, HIPPA, and FACTA) is our organiza-tion subject to and what are their requirements for data and IT asset disposal?
- Internal Policies - Do we have written policies that reflect these requirements? Is our organization able to effectively enforce those policies?
- Audit-Related Factors - Are any of our existing policies and practices auditable?

Many corporate IT departments use simple overwriting func-tions available in many disk utilities. However, these tools may have significant drawbacks which could compromise an organization's security. Highly effective enterprise-grade overwriting software must have the following functions and capabilities in order to ensure the integrity of the data sanitiza-tion process:

Security & Performance:

- Compatibility - A compatibility with, or capability to run independent of, the OS loaded on the drive.
- Independence – The capability to run independent of the type of hard drive being sanitized (e.g., Advanced Technology Attachment (ATA)/Integrated Drive Electronics (IDE) or Small Computer System Interface (S CSI) type hard drives).
- Overwriting - A capability to overwrite the entire hard disk drive independent of any Basic Input/Output System (BIOS) or firmware capacity limitation that the system may have.
- Detection - A capability to detect, report and overwrite locked and hidden sectors such as HPA, DCO, remapped sectors as well as wiping hot spare hard drives in RAID configurations.

Reporting & Auditability:

- Certification - A capability to provide the user with erasure certificate/report indicating that the overwriting procedure was completed properly.
- Hardware Configuration - A capability to identify and report vital HW configuration information with com-puter serial numbers and asset tags.
- License Harvesting - A capability to identify and report e.g., main SW serial keys for license harvesting.
- Digital Signatures - A capability to ensure report's integrity with digital signatures.
- Integration of Data - A capability to provide means for easy report integration e.g. to asset management systems.

Finally, a qualified service provider should have the follow-ing attributes:

- They must be insured (a minimum of USD 1 million).
- They must be reputable and use proven software and operational techniques.
- They must have certified engineers for onsite and support.
- They must be able to provide certificates that include serial numbers.
- They must be able to provide erasure reports to verify each disk that has been erased.
- They must provide alternatives for both software-based erasure and data destruction with an ability to combine solutions to keep operating costs low.
- They must be able to provide references.

Summary

The rapid rise in corporate information theft and fraud has made the issue of data erasure and IT asset disposal as important to an enterprise as the integrity of their corporate networks. An organization that fails to properly secure its business information when assets leave the premises risks severe penalties on a variety of legal, financial, and marketing-related fronts.

A sound and well planned end-of-life IT asset and data policy should be an essential component of every organization's corporate information strategy. Disposal and erasure methods should not be chosen on price alone. There are advantages and disadvantages to different disposal alternatives which should be carefully evaluated in light of each organization's unique requirements.

The three most important business advantages of a well-structured data erasure and asset disposal policy are:

- **To Reduce Business Risks** - A well-planned data erasure policy reduces the potential for costly risks, liabilities, regulatory requirements and public embarrassments that can occur when business data falls into wrong hands.

- **To Ensure Data Security** - A well-orchestrated data and asset disposal policy ensures the security of business information, thereby protecting existing relationships with customers, employees, and business partners.

- **To Achieve Greater ROI** - A thorough and regular data erasure policy enables an organization to safely remarket their aging IT equipment, thereby reducing the costs associated with implementing data leak prevention and asset disposal policies.

In order to protect themselves from the risks and liabilities of proprietary data getting into the wrong hands, businesses should create and implement a formal data erasure policy and should align themselves with qualified and experienced data erasure and asset disposal resources who can provide the most cost-effective, secure, and best protection options.

For more information about data erasure, please visit the Blancco website at www.blancco.com.

blancco

Blancco Oy Ltd.
Länsikatu 15
80110 Joensuu
Finland

Tel. +358 207 433 850

Protecting Your Enterprise with an Effective Data Erasure Strategy:
Steps to Ensure the Removal of Sensitive Information When IT Asset Ownership Changes

WWW.BLANCCO.COM