



White Paper

Information-Centric Security and Data Erasure

By:

Jon Oltsik and Heidi Biggar
Enterprise Strategy Group

July 2006

Table of Contents

Table of Contents	i
Executive Summary	2
Regulatory Compliance: The Other Motivator	3
Current Security Practices Cannot Meet These Challenges	4
What's needed? Information-Centric Security	5
Data Erasure: Best Practices for Protecting Confidential Information	5
EMC Certified Data Erasure	6
The Bottom Line	7

Executive Summary

Nonprofit consumer information organization Privacy Rights Clearinghouse estimates that, from February 1, 2005 through mid-June 2006, the personal records of nearly 90 million Americans were exposed as a result of security breaches - a statistic that has not gone unnoticed in the corner offices of corporations nationwide. Look at recent business headlines (source: privacyrights.org):

- **April 27, 2006:** Data tapes containing personal information including names, addresses, Social Security numbers and salary figures, about "virtually everyone" who worked for the agency were lost in transit to an off-site storage facility.
- **May 22, 2006:** The Veterans Administration (VA) announced that a laptop computer containing the personal records of 26.5 million veterans had been stolen from an employee's home. Damage estimates associated with this event are as high as \$500 million.
- **May 30, 2006:** Texas Guaranteed Student Loan Corporation was notified by subcontractor Hummingbird that one of its employees had lost "a piece" of IT equipment containing the names and social security numbers of TG borrowers.

Data breaches can not only cause public embarrassment, but they can also result in huge, unplanned expenses. ESG estimates that the direct costs of a data breach (i.e., customer notification, changes to customer accounts, credit monitoring, etc.) can range between \$30 and \$150 per user record. A data breach compromising the personal data of 1 million Americans could translate into unplanned costs of between \$30M and \$150M! In reality, though, the largest cost of any data breach or non-compliance event is likely to be associated with trying to allay the concerns of the market and consumers about the breach. Unfortunately, after a security incident, the market and consumers associate the company name with the breach.

Given this level of potential exposure, protecting company confidential and private data by developing network security and data erasure policies has become a business mandate for risk-averse CEOs. The penalties for non-compliance, outlined in Table 1, are significant - and, again, this table focuses on the "hard" costs of breaches and non-compliance; however, again, the "soft" costs (e.g., brand and company reputation, etc.) can be just as great, if not more.

Table 1: Penalties for Non-Compliance

Penalties for Non-Compliance with Regulations <i>Source: Enterprise Strategy Group, 2005</i>		
<i>Regulation</i>	<i>Potential Incarceration</i>	<i>Potential Fine</i>
Sarbanes-Oxley (SOX)	10 year prison sentence	\$15,000,000
SEC Rule 17a-4	Suspension	\$1,000,000
Gramm-Leach-Bliley	10 year prison sentence	\$1,000,000
Health Insurance Portability and Accountability Act (HIPAA)	10 year prison sentence	\$100 fine with a maximum of \$25,000 per year
Basel II		Fines
Payment Card Industry Data Security Standard		Loss of credit card privileges and fines.
National Industrial Security Program Operating Manual (NISPOM)		Fines

Regulatory Compliance: The Other Motivator

Protecting private and company confidential information has always been a good thing to do, but the truth is organizations today really have no choice but to do it. Industry-specific and consumer privacy regulations place strict security, access, retention and data destruction demands on consumer records and multiple types of private data. Complying with these regulations goes beyond implementing basic security safeguards. IT must institute measurable controls, address controls gaps in security within reasonable timeframes and document all aspects of policy monitoring, measurement and enforcement. Sarbanes-Oxley (SOX), Gramm-Leach-Bliley, North American Electric Reliability Council (NERC) and Fair and Accurate Credit Transactions (FACTA) are just some of the many regulations that weigh on security and compliance officers' minds. Other specific examples include government and industry regulations such as:

- **Payment Card Industry Data Security Standard (PCI).** PCI members, merchants and service providers that store, process or transmit cardholder data must submit annual audit statements covering 12 sections of requirements, which apply to all "system components," included in, or connected to, the cardholder data environment. These requirements include mandates for the safety of media and call for the destruction of any media containing cardholder information once the media or information is unneeded (Section 9.7).
- **Health Insurance Portability and Accountability Act (HIPAA).** HIPAA is designed to protect health information that matches a patient identity with health status data. HIPAA regulations apply to doctors and hospitals, pharmaceuticals, insurance companies, claims processors and clinical research organizations. HIPAA regulations stipulate that safeguards be in place for any media containing patient records at the time of their disposal or reuse.
- **National Industrial Security Program Operating Manual (NISPOM).** NISPOM protects the disclosure of government classified information by government agencies and contraction organizations. It mandates that these organizations implement security processes to protect the confidentiality, integrity and availability of classified data.

Complying with these regulations goes beyond implementing basic security safeguards. IT must institute measurable controls, address controls gaps in security within reasonable timeframes and document all aspects of policy monitoring, measurement and enforcement. These controls must include media-specific policies and precautions to protect information – and data erasure is a viable part of any comprehensive program.

Current Security Practices Cannot Meet These Challenges

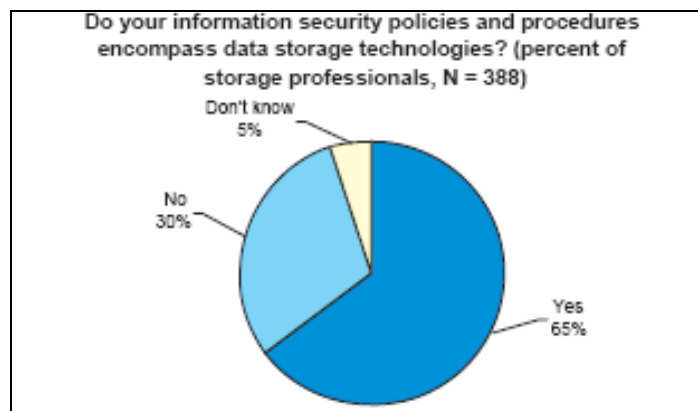
The prospect of additional data breaches and regulatory compliance is driving a new wave of enterprise security spending. Over the last couple of years alone, ESG estimates that IT security budgets have grown between 6% and 10% (year over year). This begs the question: if companies continue to bolster security defenses by sinking more and more corporate dollars into them, why are we still seeing so many data breaches?

The answer: the bulk of security dollars spent have been focused in two areas: network perimeters (e.g., firewalls, gateway filtering devices, etc.) and desktops (e.g., anti-virus, firewalls, anti-spyware, etc.). While these tools are good at protecting devices and infrastructure, they do little to protect the data itself. The result: Sensitive data remains vulnerable.

A recent ESG Research Report *Protecting Confidential Data* illustrates the seriousness of this problem: Only 18% of the security professionals surveyed believed their current security policies and procedures adequately protected ALL their confidential data.

The frightening reality is that storage remains insecure. ESG data suggests that 30% of users do not include storage infrastructure in their corporate security policies and procedures (see Figure 1). While servers provide some storage protection, an inside attack could easily result in compliance issues, intellectual property theft or data corruption; all of which could be devastating. Further, the information and media on these systems are put at additional risk when these systems are routinely relocated, reallocated or serviced.

Figure 1: Storage Security Is Still an Island



What's needed? Information-Centric Security

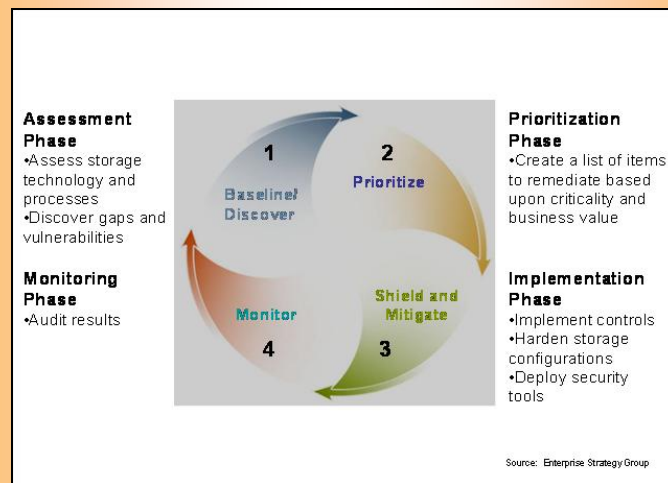
When it comes to fighting data breaches or complying with regulations, organizations must implement an information-centric security infrastructure – one that protects confidential information, not just desktops, networks and servers. This type of approach has several key components:

- **Risk assessments and strong controls.** Large organizations must examine the processes and technologies for protecting confidential data with the objective of uncovering and remedying technology and process risks according to the business value of the data. Enterprises must also implement formal processes that can be measured and enforced.
- **Data classification.** Data classification marries the right level of security (e.g., encryption, access control, rights management, auditing, etc.) to the value of the data over its lifecycle. It is a foundational element of an information-centric security approach to data protection.
- **An information-centric security infrastructure.** Rather than relying on security “add-ons,” information-centric security must be built into core products, applications and services. Doing so will make IT infrastructure a security “underpinning” rather than a series of vulnerable “piece parts.”
- **Partnerships with information-centric security vendors.** When it comes to security and regulatory compliance, IT should no longer be forced to “go it alone.” Rather, CIOs should embrace vendors that view information-centric security as part of their culture, products, processes and service offerings, and avoid those that don't have this philosophy.

The Role of Storage in Information-Centric Security

Information-centric security must be addressed from the data center to the desktop – and it must span the entire technology stack. Information-centric security is a closed-loop process; it requires continual evaluation and adjustment. ESG refers to this process as the “storage security lifecycle.” It is broken into four distinct phases (Figure 2).

Figure 2: The Storage Security Lifecycle



Data Erasure: Best Practices for Protecting Confidential Information

When it comes to securing information, many organizations realize they need to do something about online storage infrastructures. However, they often overlook data residing on storage infrastructures that are at the end of their life-cycles -- i.e., on equipment that is being re-leased,

repurposed or otherwise re-allocated. Organizations need to ensure that the data on these devices has no opportunity to be “lost” or subject to breach.

Data erasure is the *process* of permanently erasing data from disk media. It is not the same as file deletion. File deletion and removal of the Volume Table of Contents (VTOC) simply erases the “pointers” to the data stored on the media so the data is not viewable in directories. It does not physically erase the data from the media. Many firms physically destroy hard drives or use various software utilities to “erase” data using these methodologies. However, these solutions are inadequate and can potentially lead to data breaches, public disclosure and, ultimately, unplanned expenses as described above.

True erasure involves overwriting data multiple times with random bits and bytes using proper protocols so that the data that was once written to them cannot be restored or read under any circumstance. Simply put: data erasure ensures that data cannot be recovered from disk drives or systems should these devices fall into the wrong hands; file deletion does not.

An information-centric security environment requires enterprises to physically erase, or overwrite data as described above, when any adds/moves/changes are made to the storage environment. Again, examples include:

- **End of lease:** Data erasure ensures that storage devices do not contain any “readable” information when they come off lease and are returned to the vendor or reseller.
- **End of life:** Data erasure ensures that all data is “disposed” of properly at the end of an array’s lifecycle allowing for secure resale on the open market.
- **Repurpose:** Data erasure ensures that confidential data on storage systems or drives that are being repurposed or re-allocated is unreadable. Storage systems in transit from one location to another can be especially vulnerable and should be subject to data erasure prior to movement and restoration upon secure arrival at their new location.
- **Break/fix:** When storage systems break or drives fail, they should be treated as systems that are being re-leased or retired. Data erasure ensures the confidentiality of the data on these systems by rendering it unreadable—ideally prior to leaving the site.
- **Outsourcing:** Data erasure also plays an important role in an outsourcing environment where storage assets are often shared and reallocated or repartitioned as each customer’s requirements change over time.

EMC Certified Data Erasure

CIOs with neither the time nor the inclination to become data erasure experts would be well-served by hiring third-party professional services organizations who would be responsible for completing the task and certifying the completion of the data erasure process for auditing purposes.

Specifically, ESG recommends organizations look for data erasure services providers that:

- Are certified as independent agents.
- Offer configurable overwrites to the drive level that are not application-driven or filtered – and validate the process post-overwrite.

- Offer solutions that have been verified and validated by independent parties.
- Provide a chain-of-custody procedure for any offsite activity.

EMC Corporation's Certified Data Erasure service meets all of the above requirements as well as the standards for data erasure set forth by the US Department of Defense in DoD 5220-22.M.

EMC experts use host- and non-host-applied processes with specialized tools, proprietary software and certified methodology to overwrite storage arrays to customer-specified levels of erasure. Customers can select 3x, 5x, 7x, a custom number of overwrites or DoD 5220-22.M overwrite levels. The data erasure process overwrites all addressable locations with a sequence of variable bit patterns, rendering data virtually unrecoverable.

EMC also provides a full report and a Certificate of Completion for the specific drives erased and the level of erasure achieved, which proves compliance with regulations or guidelines for the protection of customer or patient information. EMC's methodology is the only solution available today that has been independently certified and validated by a third party. Kroll Ontrack, a leading data recovery audit firm, has certified and validated the EMC methodology.

It's important to note that, unlike shredding or degaussing, EMC Certified Data Erasure can be utilized without destroying the inherent value of the storage infrastructure or media from which the data is being erased. This is an important distinction: It allows companies to reuse the media. In the case of failed media, most media can be safely erased and returned for a warranty replacement by the vendor. This eliminates the exacerbation of the compliance dilemma by having to stockpile or destroy failed media while incurring charges for non-return.

By leveraging EMC Certified Data Erasure services, ESG believes organizations can achieve compliance with corporate governance policies and regulatory requirements, mitigate the risk of data loss and misuse and even boost their return on investment (ROI) by maximizing the safe re-use/repurposing of storage assets. Data erasure is not only good security, it is good business.

The Bottom Line

As information and dynamic business processes proliferate, the number of government and industry regulations to ensure proper information protection is also increasing. Non-compliance can have costly consequences. Patient records, prescription data, stored X-ray images and bank and credit card account information are just a few examples of sensitive data types.

Government and business intellectual property all necessitate the same level of vigilance. Any important company data, whether it is classified information, executive e-mails or financial data about publicly traded companies, should be erased permanently from storage resources that are being retired, repurposed, re-released, etc. It's just good business sense. Data erasure, which renders data unreadable, is a necessity in today's highly regulated world for both active and inactive information. Its counterpart already exists as "shredding" in the paper world.

For the same reasons that IT operations outsource tape vaulting to third parties and use outside auditors, outsourcing data erasure makes good business sense. Doing it internally requires extremely well-defined policies and procedures, opens the door to human error and raises the issue of accountability. Compliance is about *knowing* the rules, *adhering* to the rules and *proving* that you can comply with the rules. The role of third-party execution and certification of any compliance standard cannot be overlooked. Industry trends indicate that storage security, including policies for media and storage certified data erasure, will be an emerging area of focus and we believe auditors will force corporations to have a full-scale plan for compliance.

EMC's Information-Centric Security methodology continually evaluates and adjusts to ensure optimum security and compliance throughout the data, or information, life-cycle, including,

importantly, end-of-life media and storage infrastructures frequently overlooked by organizations today. EMC's Certified Data Erasure far exceeds current minimum service quality requirements *and* it is the only solution currently available that delivers independent certification of data erasure.