

INDUSTRY DEVELOPMENTS AND MODELS

Best Practices for Protecting Data in Failed and Decommissioned Storage Media

Vivian Tero

IDC OPINION

Data privacy, legal discovery, and IT risk management issues are inexorably intertwined. Corporations should therefore view data privacy issues in the storage media (endpoints, datacenter SANs, servers, backup tapes, etc.) in the context of their broader information management and data privacy initiatives. Data privacy is a critical component of IT operational risk, which, in turn, is a key lever in measuring a corporation's enterprise risk management (ERM) rating. Standard & Poor's is increasingly paying attention to these metrics. It is therefore in the interest of corporations to demonstrate sound data privacy and IT risk management operations. Doing so could enable them to lower their cost of capital as they look to raise funds in the capital markets. Firms that are looking to enforce their data privacy policies in failed storage media and decommissioned computing and storage resources are advised to consider the following actions:

- Audit and inventory your firm's storage media and storage systems, applications, and computing systems that may contain personal and confidential information.
- Identify the options available to manage the probable data breach from the failed media and decommissioned resources. Be cognizant of the trade-offs across your firm's application performance, resiliency, manpower and training requirements, database server and hardware overheads, "green IT initiatives," and technology capital outlay.
- Formalize and document your firm's practices for handling the disposition of data in failed and decommissioned media. Automate the workflows throughout their life cycle. Designate an individual to centrally manage the documentation of the workflows as well as the communications and relationships with service providers.
- Ensure that the process is documented, certified, and compliant with data destruction standards (such as the U.S. Department of Defense [DoD] National Industrial Security Program Operating Manual [NISPOM], NISPOM 8-306, and DoD 5220.22-M and DoD 5220.22-M ECE).

IN THIS STUDY

This IDC document discusses best practices for enforcing corporate data privacy policies in failed and decommissioned storage media.

SITUATION OVERVIEW

A comprehensive data privacy solution must address the protection of data across the enterprise and throughout its life cycle — from the time the data is created and captured to its eventual disposition, and everything in between. In theory, data privacy practices should be incorporated into an organization's broader information management practice. In reality, most corporations' information management and storage practices remain largely disjointed from their data privacy and information security functions.

Too often, corporations fail to recognize the risk of data breaches from improperly disposing of failed drives, old laptops, recycled media, and backup tapes. This failure to assess the risks associated with the physical transport of storage media has resulted in several high-profile data breaches. Several examples are as follows:

- ☒ In 2006, Chase Card Services (a division of JPMorgan Chase) notified 2.6 million current and former Circuit City credit card account holders that computer tapes containing their personal information had been inadvertently sent to the trash. Chase and its partner vendors indicated that it believed the tapes were safely "buried in a landfill" somewhere; however, Circuit City customers were offered one year of free credit monitoring.
- ☒ In 2007, the Canadian Imperial Bank of Commerce reported that it had lost a computer hard drive that featured the personal financial information of approximately 470,000 mutual fund customers. The drive disappeared while being moved from Montreal to Toronto.
- ☒ In 2008, the Bank of New York Mellon reported that "sensitive data" regarding over 4 million people owning shares in listed companies was exposed after a box of backup storage tapes went missing in February.
- ☒ In 2008, U.K. data processor Graphic Data disclosed that its Mail Source subsidiary had used eBay to sell a personal computer that featured unencrypted personal data regarding 1 million bank customers. The data included bank account numbers, phone numbers, mothers' maiden names, and signatures of 1 million customers of American Express, NatWest, and the Royal Bank of Scotland.

This cavalier approach to handling personal and confidential data residing in failed and decommissioned storage media is no longer acceptable. This document provides best practices on how to address data privacy in these hardware computing assets. The document also outlines some of the key considerations that corporations should keep in mind as they select the appropriate technology solution.

The data privacy challenge can be attributed to the convergence of the developments described in the sections that follow.

Continued Explosion of Digital Data

IDC's digital universe study sized the digital universe at 281EB (or 281 billion gigabytes) as of 2007. (For more information on this topic, see *The Diverse and Exploding Digital Universe*, March 2008, sponsored by EMC.) The amount of digital information is expected to increase at a compound annual growth rate of almost 60% and reach close to 1.8 zettabytes in 2011. This growth is underpinned by the explosion of digital cameras, televisions, surveillance, sensor-based applications (such as GPS), datacenters supporting cloud computing, and social networks. The study also concludes that although approximately 70% of the digital universe is created by individuals, enterprises are responsible for the security, privacy, reliability, and compliance of 85% of the data.

High-Profile Data Breaches Continue Unabated

Data thefts and security breaches involving customer data continued unabated in 2008. According to the Privacy Rights Clearinghouse, more than 245 million personal records have been compromised as a result of security breaches since 2005. The Ponemon Institute's *2008 Annual Study: U.S. Enterprise Encryption Trends* estimates that the cost of a data breach averages \$197 per record compromised or an average of \$6.3 million per breach. The actual cost to corporations could potentially be higher as affected customers terminate their relationship or seek legal recourse.

U.S. and International Data Privacy Regulations

Existing data privacy and breach notification regulations in the United States typically include the following categories as personally identifiable information (PII): full name, Social Security number, telephone number, street address, driver's license number, vehicle registration plate number, credit card number, face, fingerprint, and handwriting. PII is captured, stored, and managed across a broad range of databases and records repositories such as healthcare records (including genetic material), financial transactions, criminal justice proceedings, and investigations. These regulations require corporations that maintain PII to protect these records from unauthorized access, disclosure, and use. Examples of regulations that mandate data privacy include the Fair Credit Reporting Act (FCRA), Gramm-Leach-Bliley Act (GLBA), Disposal Rule of the Fair and Accurate Credit Transactions Act (FACTA), Health Insurance Portability and Accountability Act (HIPAA), secure records disposal laws now enacted by at least 28 states, and 44 state breach notification laws.

International countries have a more expanded view of the categories of protected and sensitive data. Non-U.S. jurisdictions also tend to have more stringent rules on the management and disposition of personal data. For example, Article 2 of the European Union Data Protection Directive defines personal data as "any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular, by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural, or social identity." The Directive also stipulates that all data collected should

have a stated purpose, should be utilized only for that stated purpose, and cannot be disclosed to other organizations or individuals unless authorized by law or by consent of that particular individual. The Directive also mandates that data should be deleted when it is no longer needed for the stated purpose.

In Japan, the Law Concerning the Protection of Personal Information went into effect for private sector businesses in April 2005. The definition of personal information is very broad and includes any information specifically identifying a living individual, including information that is not related to what one might normally consider information of a personal or private nature (e.g., personnel records, financial information, and medical information). Personal data may include publicly available information and business contacts, records in an electronic address book, business cards in a file, marketing lists, and email messages displaying names and email addresses. Recorded images in which a specific individual can be identified are also considered personal data.

Corporations doing business overseas would need to be cognizant of the nuances in international privacy laws. The local operations in these countries would be subject to these requirements.

FUTURE OUTLOOK

The developments discussed in the sections that follow will compel organizations to reevaluate their current approaches for managing the disposition and security of data in decommissioned and failed storage media.

Evolving Data Privacy Regulatory Landscape

To date, the U.S. state breach notification laws are perceived to be more reactive and therefore ineffective in preventing these incidents. These laws tend to address actions that corporations must execute after the data breach. There are increased calls from consumers, legislators, and privacy rights groups to adopt legislation requiring corporations that handle personal data to take more proactive approaches. California, Massachusetts, and Nevada are calling for comprehensive and minimum standards that would compel businesses to proactively safeguard personal information. These new state data privacy regulations will require businesses that touch or manage the state residents' PII to identify and assess the internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper, or other records containing personal information. They also compel businesses to proactively develop policies and procedures to define how data/business records are captured, accessed, shared across partners, and transported. These regulations are expected to take effect in 2009.

Connecticut's new Act Concerning the Confidentiality of Social Security Numbers, which took effect on October 1, 2008, imposes substantial new obligations on businesses that collect Social Security numbers and other personal information — and substantial new penalties for privacy violations. This regulation requires any person who possesses personal information of another to safeguard the data from misuse by third parties and to destroy, erase, or make unreadable such data prior to disposal. This means that any electronic file or document that contains any personal information must be safeguarded and made unreadable when it is disposed.

As a result of increased vigilance among consumers, legislators, and privacy advocates, the regulatory environment is expected to place more stringent requirements on the disposition, security, and destruction of personal and confidential data. To date, California, Massachusetts, Nevada, and Connecticut are leading the pack. The increasing sophistication of search and analytics applications and the introduction of new applications and devices are also raising concerns around the disposition and security of an individual's digital shadow. These developments illustrate that data privacy, legal discovery, and IT risk management issues are inexorably intertwined. They also suggest that a decoupled information management and data security practice is not a sustainable strategy for corporations. Therefore, corporations should view data privacy issues in storage media (endpoints, datacenter SANs, servers, backup tapes, etc.) in the context of their broader information management and data privacy initiatives.

Enterprise Risk Management and Creditworthiness

Standard & Poor's began to evaluate ERM processes with nonfinancial companies in the third quarter of 2008. It also began to consider ERM program maturity and capability in determining ratings as of the fourth quarter. Risk experts anticipate the scope of these efforts will expand beyond financial topics related to credit risks, market risks, and financial liquidity to operational risk issues (such as IT risks, data retention and compliance, disaster recovery, security, and data privacy). It is therefore in the interest of corporations to demonstrate sound data privacy and IT risk management operations. This would enable them to lower the cost of capital as they look to raise funds in the capital markets.

The high-profile data breaches resulting from the improper handling of failed and decommissioned storage media point to weaknesses in many firms' risk management practices. Although financial data privacy breaches receive the most press, these concerns also apply to medical, political, lifestyle, religious, and ethnicity issues. Beyond the protection of personal information, it is also in the interest of corporations to apply this risk management discipline to its intellectual property.

ESSENTIAL GUIDANCE

The following best practices are recommended for corporations looking to secure the privacy of personal and confidential records:

- ☒ **Establish organizational governance infrastructure.** Corporations should establish an organizational structure that includes representatives from different functions within their organizations. In the case of data privacy projects for failed and decommissioned storage media, they should designate an individual to operationalize, manage, and maintain the program. But they should include representatives from IT compliance and risk management, internal audit, IT security, and IT/datacenter operations when forming the project team responsible for defining policies and technical procedures, building requirements, and selecting the technology solution. When cross-border data transfer issues and collection are potentially involved, it may also help to include the legal function.

Legal could assist the project team in navigating the complex issues associated with international data privacy regulations.

The data privacy project for failed and decommissioned storage media would typically be a subgroup within a corporation's broader data privacy program. Ideally, a corporation's data privacy program would increasingly coordinate its efforts with the team responsible for its information management practice. At the corporate level, the information management and data privacy teams are responsible for defining the policies and control objectives around data retention and disposition, acceptable use and communications, and data privacy and information security. This team also facilitates the identification and scope of the multiple projects under the broader information management and data privacy umbrella. This approach facilitates buy-in and support for additional data privacy and intellectual property protection initiatives.

- ☒ **Leverage information management and litigation-readiness efforts to define data privacy policies.** A corporation's information management program typically includes documented guidelines on the classes of business and personal records. These guidelines define the retention, disposition, acceptable use, and communications of both records and nonrecords (which include convenience copies and work-in-progress documents). The information classification is useful for deciding the classes that are mission critical to the core business process operations.

Today, retention, disposition, and data privacy policies are still predominantly application and storage media specific. However, many corporations recognize that going forward these retention, disposition, and data privacy policies will need to be more "content aware," identity aware, and application and storage media agnostic. For example, corporations are aware that PII and corporate intellectual property may exist as attachments to emails. Copies may also exist in a network file share, on an employee's laptop, in a disk drive in SAN storage, and in backup tape media. Legal discovery challenges are already compelling many corporations to take steps to ensure that retention and disposition policies are consistent across applications and storage media. Corporations can make use of these existing and planned investments to drive their information security and data privacy guidelines.

The data privacy guidelines should be documented and disseminated to employees. In addition to the standard information security policies and procedures, the guidelines should clearly address:

- ☐ Incentives and accountability for employees, records custodians, and system custodians
- ☐ Controlled access and limits on the amount of time data is retained in the storage media and applications throughout the life cycle of the personal and confidential information — from its creation and capture to its eventual destruction (Too often, corporations overlook data privacy issues in failed and decommissioned storage media devices.)

- ☒ **Discover and scope assets.** Corporations need to understand "what" and "where" critical assets are located, taking into account that specific content can reside in multiple applications and across different forms of storage media. They should audit and inventory their storage media and storage systems, applications, and computing systems that may contain PII, confidential business records, and intellectual property.

When possible, they should utilize existing investments in asset management, CMDB, security incident and event management, problem management, records management, enterprise resource management, HR and financial applications, and any database repositories, which track the physical and logical location of personal and business records.

Data loss prevention (DLP) applications also provide valuable information on the location and use of personal and business records and security vulnerabilities across the corporate network. Corporations that have invested or are planning to invest in creating data maps as part of their litigation-readiness program should consider leveraging these investments to support their data privacy audit and discovery efforts.

Many corporations today organize their datacenter operations into different tiers, depending on the criticality of the applications and processes to their core business. Beyond current initiatives to protect data in the endpoints and periphery of the network, datacenters with the highest-priority and mission-critical processes are typically the initial targets of a firm's data privacy project for failed and decommissioned media. Over time, and depending on their risk profile, some corporations would extend these efforts to the lower-tier datacenters. These datacenters typically manage development and testing and less frequently accessed legacy applications.

- ☒ **Conduct risk assessments.** Corporations should use existing information management and data privacy directives as a jumping-off point to align their corporate retention and disposition guidelines with their information security and data privacy controls. The information management and privacy guidelines also serve to provide a baseline for conducting risk assessments and defining their risk tolerance.

In addition, corporations should understand their information, storage, and security architectures and identify the potential process and technical gaps. For example, a large financial institution conducted a risk assessment after a security breach involving backup tapes that were shipped via courier to its disaster recovery service provider's facilities. The evaluation also pointed to the risks arising from sending out failed disks for exchange or repair to the manufacturer, as well as the vulnerabilities in the endpoints.

The ability to identify risks and build a risk profile for the various asset classes and storage media assets is useful in defining the appropriate data privacy controls. Corporations can also use this information to narrow down the appropriate architecture and technology solutions to enforce their data privacy controls.

In many instances, the results of the risk assessment have compelled corporations to adopt a blanket policy. This policy requires the DoD-compliant destruction of the data stored in failed or decommissioned storage media, which is about to leave the control of the datacenters. Data destruction certificates are issued and managed to document compliance with this blanket policy.

☒ **Define the technical procedures and workflows for enforcing data privacy in failed and decommissioned storage media.** Corporations should formalize and document the practices for handling the disposition of data in failed and decommissioned media. They should consider the following:

- ☐ Define and automate the workflow from the time a trouble ticket is issued for the failed and decommissioned media to the logging of the media serial/tracking numbers, the quarantine and physical security of the media, and the actual execution of the data destruction. These processes should be consistently enforced across all datacenters.
- ☐ Ensure that business partners that operate segments of the datacenter operations are also compliant with these processes. Compliance with these processes should be baked into the service-level agreements with business partners.
- ☐ Document policies and implement procedures for the physical access and control of the storage media. Quarantine and secure the physical storage of the failed and decommissioned storage media.
- ☐ Document the certification and sign-offs involved in the actual destruction of the data. If possible, centralize the management of the workflows, as well as the capture and management of the destruction certificates across datacenters. Documentation and automation facilitate the consistent enforcement of the data privacy technical procedures. They are also valuable in demonstrating a corporation's risk management practices to internal and external audit teams. Documentation and automation also provide useful information during a corporation's annual risk assessment, review, and planning, especially as the datacenter scales up, and when new media and applications are introduced into the environment.
- ☐ Ensure that data protection practices are compliant with any or all of the following data destruction standards: DoD NISPOM, NISPOM 8-306, and DoD 5220.22-M and DoD 5220.22-M ECE. Increasingly, some corporations are also looking at data destruction approaches that support corporate green IT initiatives.
- ☐ Designate an individual to centrally manage the documentation of the workflows as well as the communications and relationships with business partners. These business partners may be managing specific sections of the datacenter operations, or they may be providing the service that destroys the data.
- ☐ Identify the options available to manage the probable data breach from the failed media and decommissioned resources. Be cognizant of the trade-offs across application performance, resiliency, manpower and training requirements, and technology capital outlay.

Evaluating Options for Protecting Data in Failed and Decommissioned Storage Media in the Datacenter

The following options are typically employed to secure PII and confidential data in failed and decommissioned media:

- ☒ **Encryption (full disk, file, tape, server, host based).** Encryption imposes server, storage, application performance, database, key management overheads, and physical hardware overheads. Additional physical hardware taxes the datacenter's power and cooling efforts and conflicts with a corporation's green IT initiatives. From an ediscovery standpoint, a corporation would have to consider how it could effectively facilitate search and retrieval of data to meet its legal hold obligations. A corporation therefore needs to consider the trade-offs between security, performance, green IT, and a financially viable cost model.
- ☒ **Physical destruction of the storage media.** A disk drive can cost between \$600 and \$3,500. When a drive fails, the options are to destroy the failed drive (and write off the cost) or send it out to the manufacturer (as defined in the service contract) for replacement (which exposes the bank to data loss). Data continues to grow at exponential rates for most corporations. Absorbing the costs of the destroyed storage media and keeping these locked up in a secure vault within their datacenters are therefore not economically sustainable strategies. The physical destruction of the media may also not meet data destruction standards such as DoD NISPOM, NISPOM 8-306, and DoD 5220.22-M and DoD 5220.22-M ECE.
- ☒ **Degaussing.** This option destroys the boot prompt and the configuration of the architecture, but it may not actually destroy the data inside the disk. The approach limits a manufacturer's ability to fix the drive. A manufacturer may be less likely to honor warranty and service contracts with this option. Also, new storage media are increasingly installed with magnetic shields that limit the effectiveness of the degaussing process.
- ☒ **Employing onsite disk eradication.** A corporation would need to decide if this is a process its internal IT operations and security functions would provide or if it would employ an outside service provider expert. The internal investments would take into account the manpower training and DoD-compliant certifications. A corporation would also need to ensure that its process and technology investments would support data eradication across different hardware and storage media systems.

Outside of the acquisition cost of the solution/technology, a corporation should clearly define its requirements across the following attributes: application performance, current and planned technology architecture, resiliency, financial management (operating versus capital expense issues), and manpower investment requirements. A corporation needs to be cognizant of the trade-offs across these "requirements" when making a technology decision.

LEARN MORE

Related Research

☒ *Date Privacy: It's Not Just About Security!* (IDC #lCUS20833107, August 2007)

Synopsis

This IDC study provides best practices for enforcing corporate data privacy policies in failed and decommissioned storage media.

"Data privacy is a critical component of IT operational risk, which, in turn, is a key lever in measuring a corporation's enterprise risk management rating," says Vivian Tero, program manager, Compliance Infrastructure, IDC. "Standard and Poor's is increasingly paying attention to these metrics. It is therefore in the interest of corporations to demonstrate sound data privacy and IT risk management operations. Doing so could enable them to lower their cost of capital as they look to raise funds in the capital markets."

Copyright Notice

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, telebriefings, and conferences. Visit www.idc.com to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit www.idc.com/offices. Please contact the IDC Hotline at 800.343.4952, ext. 7988 (or +1.508.988.7988) or sales@idc.com for information on applying the price of this document toward the purchase of an IDC service or for information on additional copies or Web rights.

Copyright 2009 IDC. Reproduction is forbidden unless authorized. All rights reserved.