# DREAM THE IMPOSSIBLE DREAM

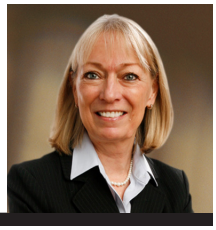
## A Unified Approach to Information Security

**Astounding opportunities arise from the technical ability to collect vast** amounts of data from traditional computing environments, cameras, sensors and geospatial technologies, and the subsequent ability to process and analyze that data at near real-time speeds. Better, faster, smarter decisions can be made by tapping into enormous stores of data to make meaningful connections, identify emerging trends and develop new insights into customer behaviors and business performance.

The problem legal organizations are experiencing isn't with the information itself, but with the inability to safeguard, manage and govern information in a manner that controls and protects it from external threats, intentional breach by rogue employees or accidental disclosure.

**About the Author**

Laurie Fischer, Managing Director at Huron Consulting Group Inc., has more than 23 years of experience in the design, development and implementation of records and information management programs for organizations of all types and sizes, including large, complex, highly-regulated companies. As a Certified Records Manager (CRM), her engagements have included the development of RIM policies and procedures, legally-compliant retention schedules, electronic records and information management programs, audits and assessments, vital records programs, and RIM training and education.



## A UNIFIED APPROACH

Typically, the management and control of an organization's information fall under the responsibilities of the following business functions, often operating in a very siloed manner:

- The records and information management department defines policies and procedures used to manage an organization's records and information. They identify regulatory retention requirements for records.
- The legal department's oversight and management of litigation, claims, government investigations and other legal actions and disputes heighten its concern related to e-discovery and the ability to find responsive information in a timely manner, and to preserve related data.
- The information security department within the CIO's organization protects the confidentiality, integrity and availability of information, ensuring access to systems only by authorized persons.
- The privacy office is charged with responding to privacy-related issues and investigates privacy breaches and complaints involving unauthorized access or disclosure of personally identifiable information.

**One of the first mandates of the information governance steering committee should be the development of an all-inclusive information map.**

These distinct organizational functions focus on specific aspects of information management and protection, typically with limited interaction. Many organizations are coming to understand that a comprehensive and unified approach to managing information across the enterprise can only be realized through a coordinated interdisciplinary approach. Such an approach aims not only to manage the risks of inadequate information management and protection, but also to optimize information value as an asset.

Establishing an information governance steering committee, with executive sponsorship at the highest level, provides a top-down framework for the strategic governance of an organization's information assets that considers and accounts for all interests. The most successful committees are those that comprise not only representation by the legal, privacy, IT and records and information management departments, but representation by key business stakeholders as well.

## THE IMPORTANCE OF AN INFORMATION MAP

Each of the traditional disciplines has a distinct view into the organization's information:

- Often, the legal department will develop a data map as its view into those systems most commonly relevant to discovery requests, legal holds and/or needed for meet and confers.
- Records and information management focuses on the defensible disposition of records as defined by their regulatory, legal and operational value, depicted by a records retention schedule.
- Information technology could maintain an application profile that shows the overall infrastructure of systems under the management of the central technology group.
- The privacy office's view of information within the organization is often limited to lists of systems that contain personally identifiable information or other sensitive data.

Although each of these tools serves a key purpose, none alone provides a comprehensive view of an organization's information landscape. Without this unified view, an organization's governance strategy is likely to have gaps and disparities.

One of the first mandates of the information governance steering committee should be the development of an all-inclusive information map that serves as a starting point in assessing whether comprehensive information governance requirements are being met. The organization's records retention schedule might be a starting point since it should already identify what the organization considers "records" and related retention requirements.

To evolve the retention schedule into an information map, remember that most retention schedules are adept at addressing the world of physical paper records, but

often do not adequately address the ocean of electronically stored information. Although many of the categories on a traditional retention schedule relate to structured data systems, this poses two concerns:

1. A hard-copy-centric retention schedule that addresses "distinct physical objects" might not be portable to the structured data environment, where "distinct digital objects" do not neatly exist.

2. A vast amount of unstructured content is not included in traditional retention schedules.

To address these concerns, the retention schedule should be expanded to include reference to both "records" and "information" that might not fit the description of an official company record, yet has business value and serves an administrative or operational purpose.

**In addition to ensuring the records and information categories are thoroughly defined, additional fields of information to note include:**

1. The identification of an unstructured content storage location or repository, such as a network drive designation or a document management system
2. The identification of a structured data system or application name
3. Indication whether the repository or system is cloud-based or on-premise
4. The security classification of the information, such as "company confidential" or "public"
5. Whether the information contains personally identifiable or otherwise sensitive data
6. Data flow information that might be important to know from a security perspective

After updating the retention schedule, the regulatory research that supports the time periods assigned to each record class should be refreshed to ensure they are comprehensive to all (including international) jurisdictions in which the organization operates. Besides reviewing retention time period requirements, research should include:

- **Storage Location:** There might be requirements for information to be stored in a specific jurisdiction.
- **Data Transmission:** Requirements might exist that restrict the transmission of data outside a specific jurisdiction.
- **Disposal Dates:** There might be a stipulation that certain data are to be disposed of as soon as they have served their business purpose.

Once an organization has a complete understanding of the information it retains and its related sensitivity and classification, appropriate protection tactics can be applied. Additional considerations of an effective privacy and security approach include:

**Privacy Policy:** A comprehensive privacy policy includes both internal and external versions. Internal privacy policies should cover everything from employee handling of sensitive information to IT security controls and reporting breaches. External policies are customer-facing, and have both practical and marketing/PR considerations. Global policies require additional attention due to the sometimes conflicting interests of various jurisdictions.

Once the policy has been drafted and approved, a training program will help facilitate employee compliance, including that of senior executives, with policy requirements. Training should be refreshed at regular intervals. Further, consider strengthening language in employee agreements with more restrictive covenants regarding the use of company data — both during employment and after separating from the organization.

**Data Loss Prevention:** Data loss prevention refers to a system designed to detect a potential data breach and to prevent it by monitoring, detecting and blocking sensitive data. Sensitive data might include private or company information, intellectual property, financial or patient information, credit card data and other information, depending on the business and industry. Data loss prevention software solutions can play an important role if an organization handles this sensitive data.

**Data Minimization:** Data minimization refers to reducing the amount of sensitive data retained. Questions to ask that can help you identify when fewer data will suffice include:

1. Does the organization really need to keep the data? Some data are transitory and might be needed at the moment, but not for the long term. Information deemed transitory should not be stored or archived.

2. Would only a part of the data be as useful as the whole for the organization's purposes? For example, storing the last four digits of a Social

Security number might be as useful as storing the entire number. The damage associated with disclosing just those digits is minimal compared to the entire number.

3. Could less sensitive data be used? For example, instead of storing a value such as a driver's license number, a customer ID only used by the organization might suffice.

## CLOUD STORAGE

An organization's obligations for data protection and security do not cease if the information is stored with a third-party provider of cloud storage. Additional diligence must ensure cloud storage suppliers provide enforceable measures to preserve confidentiality and security. Attention should be paid to:

- Include in your cloud storage provider contract verbiage about ownership of data, access to data, ability to purge data at customer-specified dates, indemnification if a data breach occurs and procedures should the vendor go out of business. Periodically confirm vendor compliance.
- Assess the provider's security measures, policies, recoverability methods and other procedures to determine their adequacy. At regular intervals, confirm that the measures remain effective in light of technological advances.
- Address regulatory obligations. For example, the Health Insurance Portability and Accountability Act requires that third parties with access to protected health information sign a business associate agreement.
- Know where the organization's data will be stored. In some jurisdictions there are laws prohibiting the storage of data outside the country. If based in the United States and your data are stored outside of the country, the federal government might not help if problems occur or there are issues with the vendor.

## BRING YOUR OWN DEVICE

Most organizations have realized significant benefits when adopting a policy that allows for the use of personal devices, including increased productivity, lower costs and increased employee satisfaction. However, most experts agree that the capabilities of mobile devices far exceed the current technology to secure them. With sales of smartphones and tablets increasing rapidly and personal computer sales on the wane, it is predicted that the majority of security breaches in the future will be caused by mobile device attacks via hackers bypassing authentication methods. Application-level encryption, for example, and segregating enterprise data from the rest of the device can help minimize threats.

## BREACH RESPONSE PLAN

Although these preventive measures will help you avoid a data breach or cyberattack, an organization is wise to develop a comprehensive breach response plan … just in case. If a breach should occur, immediately enacting a comprehensive breach response plan can help minimize the impact and damage. Too often, an organization can go from being a victim to a defendant due to a lack of a proper breach response process.

The plan should include an immediate assessment of the size and scope of the breach and the location and entry points to determine the source of attack. Engaging a third party to work with law enforcement to supplement the investigation should be considered. The breach response plan should include an assessment of the damage done, both from a financial and reputation standpoint, and the immediate management of both. A communication strategy is key. P2P


*This article was first published in ILTA's Fall 2014 issue of* Peer to Peer *titled "Security Is Everyone's Business" and is reprinted here with permission. For more information about ILTA, visit www.iltanet.org.*