Protecting Privacy Through Improved Information Governance

IRON MOUNTAIN®

Privacy Law: US and the European Union

IRON MOUNTAIN®

Cultural Perspectives

- Europeans consider privacy a fundamental right based on the right to associate with others through the protection of their reputations.

- US has no fundamental right to privacy, instead privacy rights are inferred from rights to liberty and freedom, primarily from intrusion by the government.

- US citizens have adopted a more security based view of privacy, knowingly sacrificing privacy to allow surveillance of potential terrorists after attacks in New York and Washington on 9/11/2001.

What Laws Apply?

- US Federal Law applies to specific industries; financial, health related entities (HIPAA), distribution to children, etc.

- Privacy Shield framework implemented by US Department of Commerce in Sept. 2016, and enforced by the FTC, or by state attorney generals, applies to all companies conducting business with any (even one) European Union (EU) resident.

- Privacy Shield is about **Location, Location, Location!**

EU definition of Privacy

Anything likely to be used by a data controller or any natural person including:

- Name
- Email address
- Photo
- Social network post
- Bank details
- IP addresses
- Medical information

Privacy Shield

Interim Measure - Post Safe Harbor:

- Greater cooperation between EU Data Protection Authorities and the Federal Trade Commission (FTC).
- EU residents have avenues for mandatory arbitration.
- Department of Commerce will enhance and supervise compliance and assist in dispute resolution process.
- State Attorney Generals will have jurisdiction over organizations that are not under jurisdiction of FTC
- US companies bound to enhanced contractual privacy protections and oversight.

Privacy Shield Checklist

- Privacy Policy linking to Department of Commerce (DOC) Privacy Shield website and chosen dispute resolution provider
- Dispute resolution mechanism
- Disclosure of Privacy Shield enforcement authority (usually FTC)
- Ability to meet residents' requests/complaints within 45 days
- Annual recertification
- Transparent enforcement actions (compliance reports will be public)

EU Penalties under Regulation effective 2018

- Penalties under the new EU regulation effective May, 2018, are set at up to 20 million euros or 4% of global turnover.

- Doing business with even one EU resident will subject a company to the EU's jurisdiction.

Seven Principles of EU Privacy Law

1) Notice
2) Choice
3) Onward Transfer (Transfer to Third Parties)
4) Access
5) Security
6) Data Integrity
7) Enforcement

States' Definition of Privacy

Most states follow Massachusetts' definition of private information as:

Name, or first initial and last name in combination with one of the following:

1) Social security number,
2) Driver's license or state identification card number, or,
3) Financial account number or credit card number with or without and required code/number/password that would permit access.

State Breach Notification

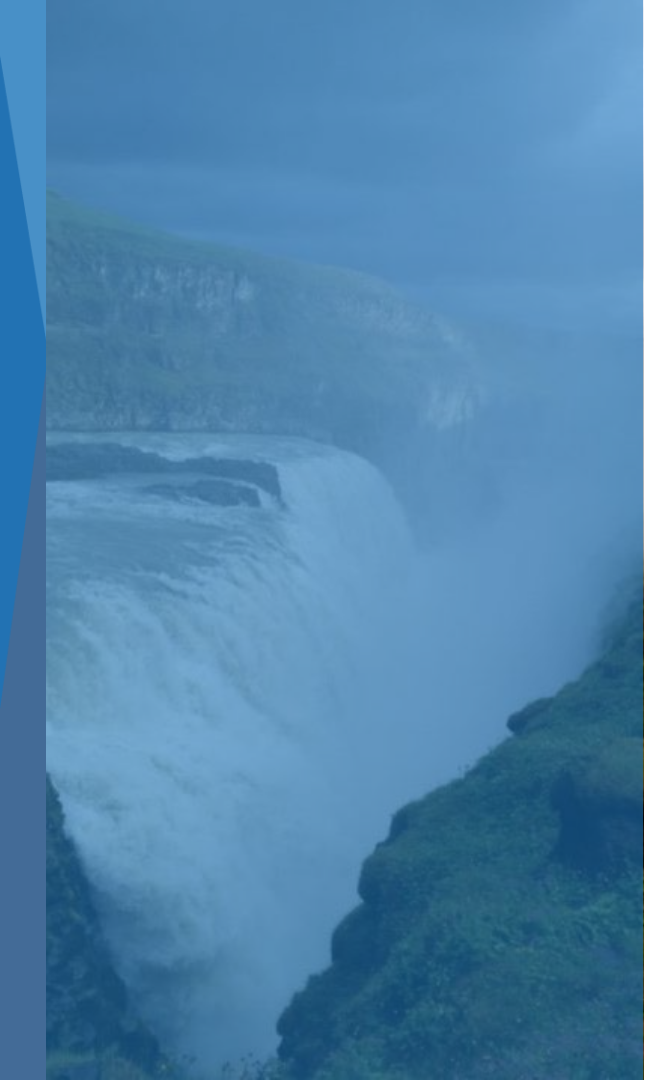
- 47 states have breach notification statutes – applies across borders to protect state citizens. (except Alabama, New Mexico and S. Dakota)

- A breach occurs when PII is disclosed and **unencrypted**.

- Disclosure is required any time there is a **reasonable** belief that unauthorized access has compromised the security of PII.

Privacy Breaches and Penalties Driving IG Initiatives

IRON MOUNTAIN®



Past Organizational Paralysis

- Did not know where to start
- Could not bring all information stakeholders to the table
- Were unable to demonstrate the urgency
- Could not clearly demonstrate negative cost and risk impacts
- Could build a compelling business case

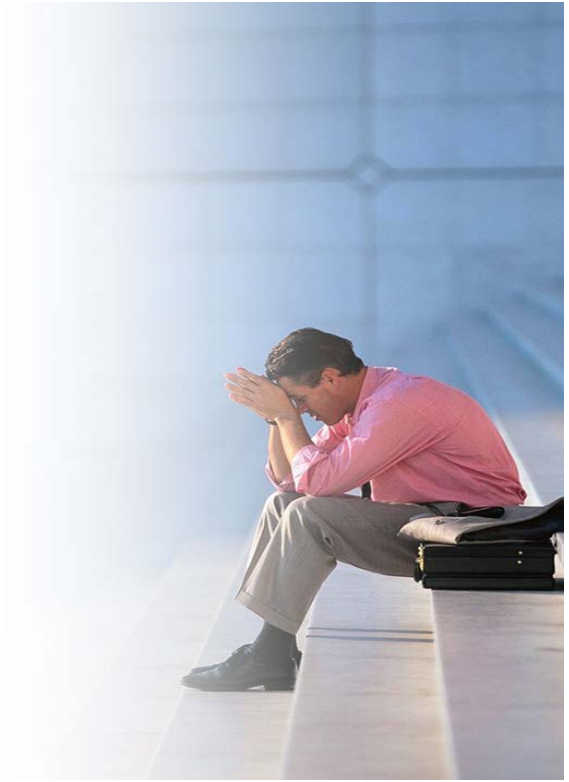
Hacking Has Become Common

Attackers have targeted banks, digital rights, personal photos, webcams, retail data, and government:

- Sony Pictures digital movie stolen, photos released
- Home Depot- 53 million credit card numbers
- JP Morgan Chase- 7 million small businesses and 73 million households
- Google email- 5 million accounts
- Yahoo! – 500 million accounts

Costs from Data Breaches

- Lawsuits
- Fines and penalties
- Loss of customer loyalty
- Loss of revenue
- Share price erosion
- Negative publicity
- “Brand equity” damage
- Damage to company reputation
- Increased operations costs
- Intellectual property loss



Improving RIM to Protect Privacy

IRON MOUNTAIN®

Shifting Priorities

A US insurance company covering data breach claims demanded improvements in the following areas to avoid further increases:

- Better classification of private data;
- Privacy Management Policy and Procedures;
- Records Management Policy and Procedures;
- A Defensible Disposition Plan.

Obtaining Privacy Protection Through RIM

1) *Access*- classification system ensures quick access
2) *Consent* evidence– with record as attachment or link
3) *Retention* schedules ensure deletion after usefulness has passed
4) Timely *breach notification* to government or individuals
5) *Accuracy/Correction* of information more easily tracked
6) *Security* more easily maintained with less information
7) Quick *audit* capability

RIM MATURITY- PRIORITY 1

- Supports event and time-based retention rules based on global, national, providence and local laws *(Retention)*
- Creates structured file plan to organize records and enforce complex policies/rules *(Compliance)*
- Enables legal holds, effective audits and electronic evidence discovery *(Availability)*
- Ensures record authenticity, integrity and contextual relationships *(Authenticity and Integrity)*
- Adequately preserves records and ensures reliability *(Integrity)*
- Enables quick record access and retrieval *(Availability)*
- Prevents unauthorized deletion *(Retention)*
- Ensures timely disposition and complete record deletion when appropriate *(Disposition)*
- Ensures privacy and record security policy management *(Accountability, Transparency and Protection)*
- Supports physical records *(Compliance)*

Privacy Roadmap

IRON MOUNTAIN®

Privacy Management within IG

Strategy

- Ownership, custodianship, location and control of PII
- Standardized data governance throughout lifecycle
- **Understanding of changing law**

People

- **Data privacy awareness and training**
- Precise communication and conformance with culture
- Leverage **suppliers, vendors and counterparties** with specific, enforceable data privacy obligations

Process

- Consistency with local law
- Data privacy dash boarding, analysis and reporting

Privacy Management within IG

Organization

- **Designate responsible party** (**Chief Privacy Officer**)
- Privacy must liaison with security, compliance, communications
- **Must designate person as point of contact in case of breach**

Data/Technology

- Data fields must be organized for compliance readiness
- Vendor support should be maximized through technology
- Data privacy integrity must be tested regularly for “what ifs”

Service Delivery

- Permit employee self-service when possible
- Log, monitor and alert improper access to PII

Privacy Incident Response Plan

Written Plan

- Leadership – Attorney + Privacy Officer + Chief Security Officer
- Insurance
- Forensics – outside pre-vetted response
- Law enforcement
- Public Relations
- Notifications

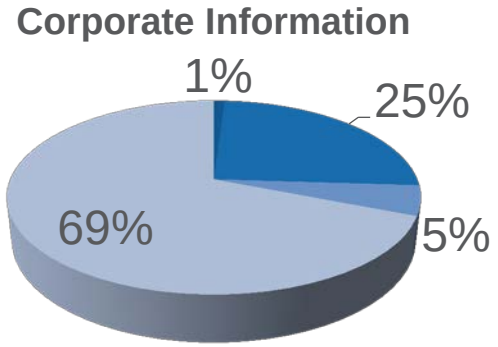
Lean and Clean

IRON MOUNTAIN®

Distribution of Corporate Information

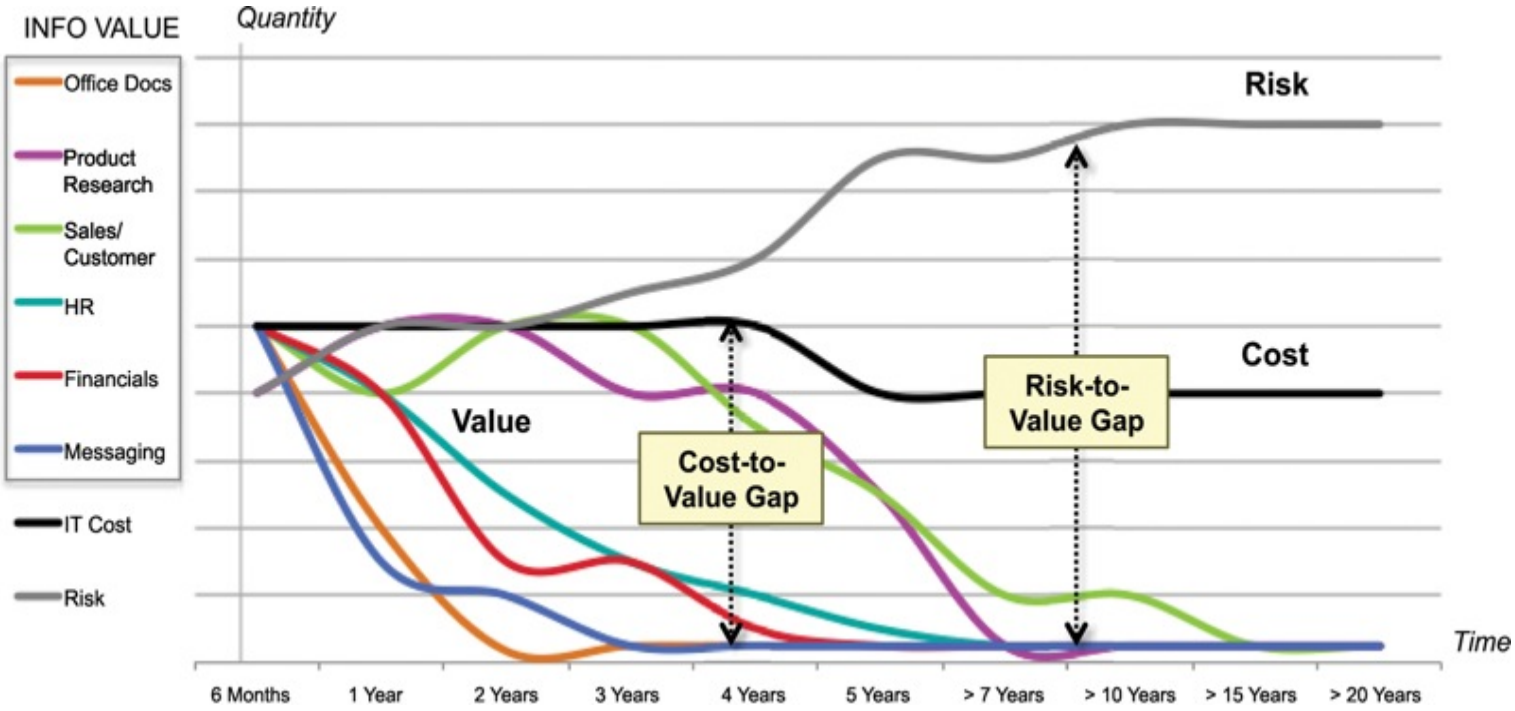
According to a 2012 Compliance, Governance and Oversight Counsel (CGOC) survey, at any given time:

- **1%** of corporate information is on litigation hold;
- **5%** is in a records category; and
- **25%** has current business value.

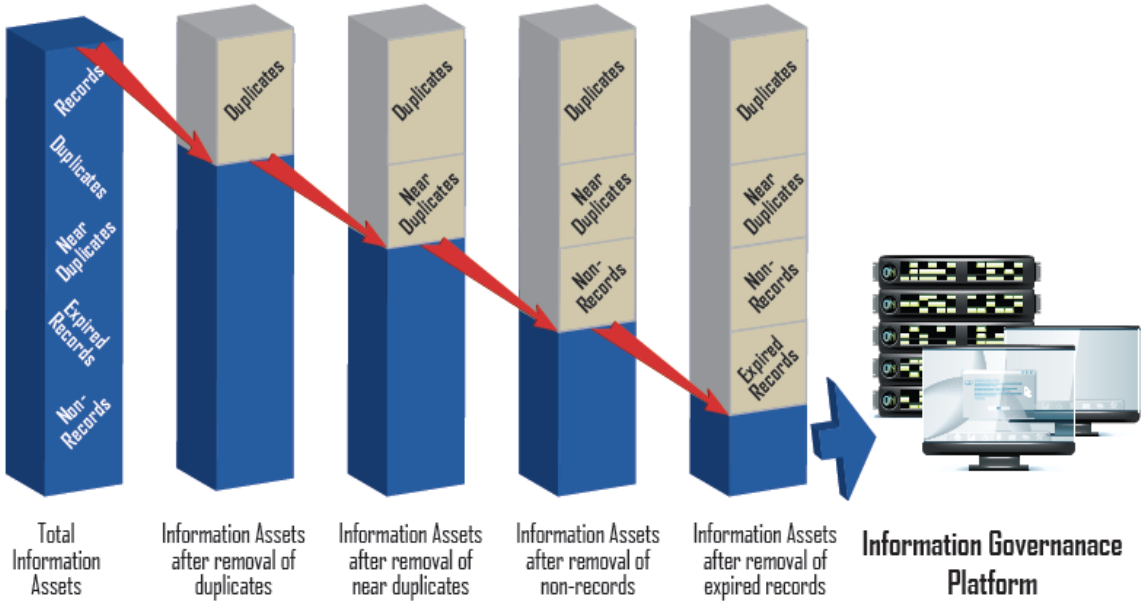


This means that as much as ***69 percent*** of all the data stored in an organization could be ***defensibly*** eliminated, that is, disposed of without increasing the risk to the company of undercutting business initiatives or risking legal or regulatory penalties.

The Risk/Value Assessment



Data Reduction



Less Information is More Privacy

To achieve privacy protection, data must be controlled from capture through disposal requiring:

- written policies and procedures, (including breach plans),
- employee training,
- data classification,
- data quality control,
- easy data retrieval,
- schedules for deletion based on purpose,
- restrictions on access (including logging of activity), accountability for protection, and,
- adequacy of system architecture, intelligent use of corporate information assets and responsible disposition.

The Foreseeable Future

- Quick breach notification requirements mandate that an organization know what it has and have the ability to access its status quickly.
- Right to review data held on an individual requires quick access.
- Right to withdrawal of consent requires access.
- PII must have retention schedules based on intended purpose.
- The Right to Be Forgotten will require deletion of PII whenever it is out of date (no longer accurate).
- Broader definitions of PII and stiff penalties could impact the value of dark data and defeat economic incentives to maintain it.


Questions?