COMPLIANCE OFFICERS AND HACKERS ON A COLLISION COURSE

What emerging data protection challenges mean for your organization's culture of compliance

IRON MOUNTAIN®

WHITE PAPER

WHY READ THIS

WITH DATA PRIVACY REGULATIONS CONTINUING TO MORPH CONCURRENT WITH THE INCREASING DANGER OF DATA BREACHES, IT IS IMPERATIVE THAT ORGANIZATIONS REMAIN ABREAST OF CHANGES IN THE DATA PROTECTION LANDSCAPE, TO REMAIN ON THE RIGHT SIDE OF THE LAW.

THE FREQUENCY OF CYBER THREATS IS RISING

Your view on data privacy will probably differ fundamentally depending on where you are reading this. Interestingly, Europeans consider privacy an essential right based on their desire to associate with others through the protection of their reputations. A US citizen has no such fundamental right to privacy. Instead, privacy is inferred from rights to liberty and freedom, primarily from intrusion by the government.

Whatever your view, the severity and frequency of cyber threats is rising. At the same time, there is a minefield of increasingly stringent data protection regulations – led by Privacy Shield and the EU General Data Protection Regulation (GDPR) – which could have a crippling effect on your organization should you suffer a breach of your systems resulting in the theft or compromise of private data. Failure to comply with such regulations could have far-reaching financial and reputational implications. With a greater focus on the comprehensive treatment of personal data and increased risks and fines, comes a heightened need to make sure your data and the policies that surround them are up to date. But, in order to meet your statutory obligations, you first need to know where that data lives.

How do you get to compliant?

ASSESS

- Triangulate risks/ opportunity/cost
- People/Process/ Governance/ Technology root causes
- Risk appetite leads to the best roadmap to remediate

IMPLEMENT

- Simplify and clarify policy and process as job #1
- Construct your program in phases
- Bridge 'the last mile' for some, manual for others

MONITOR

- In accordance with your policies and control points
- Operating against your content
- Dynamically as policy and content change

OPERATE

- Consistently across the business around the globe
- Internally and with 3rd parties
- Gathering live data for continuous improvement & audit

We are on a collision course, and a perfect storm is brewing

- **Privacy/security:** Data breaches are increasing as hackers get more sophisticated. The C-level is being held accountable. There are now more stringent laws to protect individual privacy worldwide.
- **Records management:** There are more aggressive audits by agencies, attempting to offset reductions in tax revenues.

Courts continue to impose harsh sanctions for the inability to locate evidence.

- **Information disposition:** Fear of not keeping information for business or legal reasons has created massive data repositories often with no knowledge of contents. Costs are becoming problematic. Organizations have difficulty producing relevant data for business needs, eDiscovery and/or post data breach.

QUESTIONS TO ASK NOW

- **How have the recent announcements about Privacy Shield, GDPR regulation and state data breach laws affected how information should be transferred, stored, accessed and deleted?**
- **How are changing regulatory requirements affecting information management strategies; particularly eDiscovery, records management, privacy management, security and defensible disposition?**
- **How is the current cyber threat landscape affecting how I must hold and protect my data?**

EU-US PRIVACY SHIELD

Businesses are currently scrambling to ensure that they adhere to the new EU-US Privacy Shield, with self-certification (started August 1, 2016) mandatory for any organization that undertakes business with even one EU resident. It is not a regulatory framework to take lightly; the Federal Trade Commission (FTC) has stated it is making enforcement a priority, even adding extra staff specifically to enforce it. Risks are very real for those organizations that don't comply.

Privacy Shield reflects the requirements set out by the European Court of Justice in its ruling on October 6, 2015, which declared the existing US Safe Harbor framework invalid. The new EU/US agreement places safeguards on how US authorities can access the data of European consumers, and creates a framework for resolving cases where Europeans believe that their personal data has been misused.

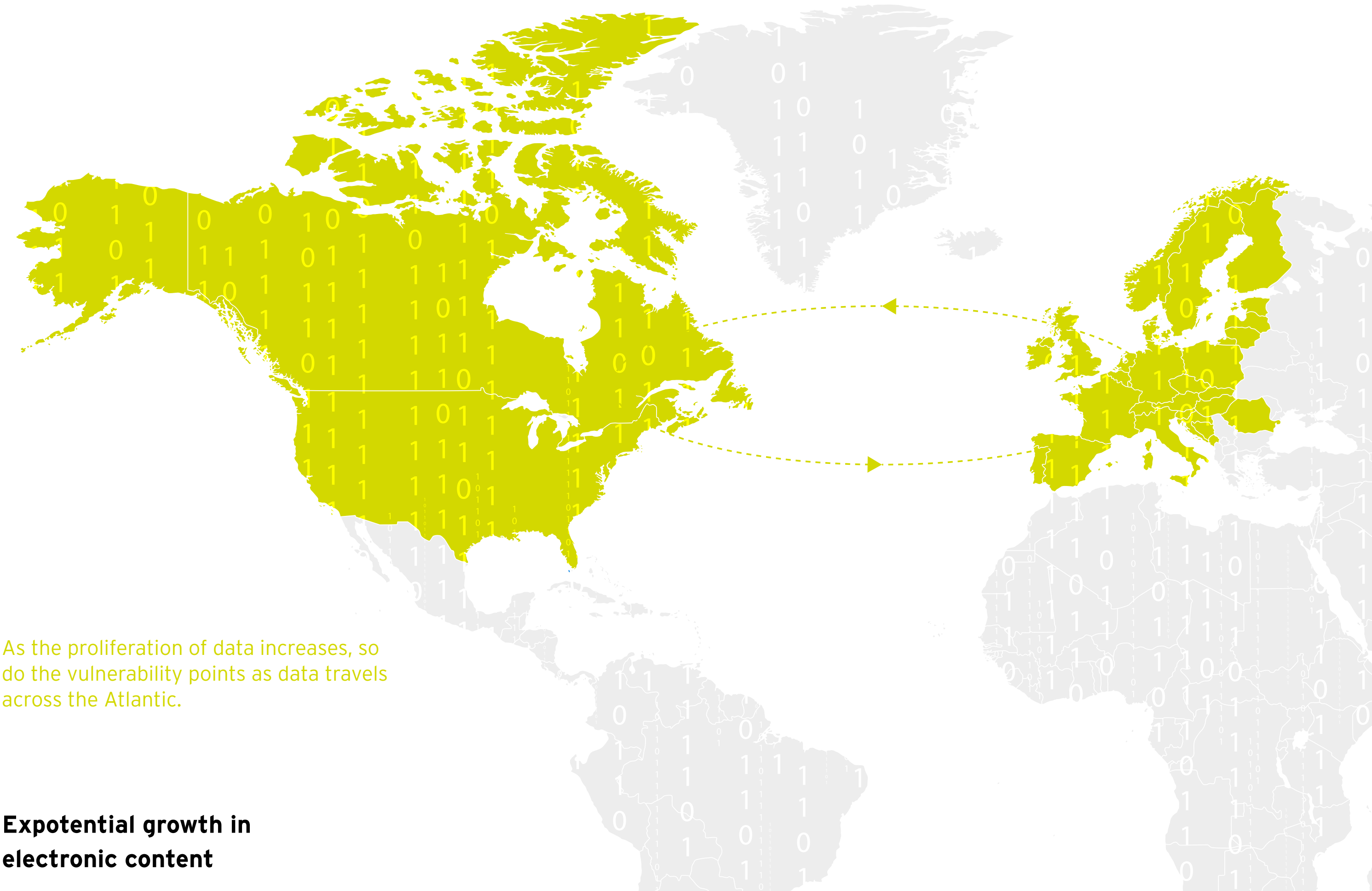
Privacy Shield is seen as critical to facilitating the cross-border data flows upon which major tech companies and other industries rely to carry out trans-Atlantic business, currently the largest trade route in the modern world.

GDPR

It's not just Privacy Shield that multi-national businesses need be wary of, but also the impending EU General Data Protection Regulation (GDPR) which is due to come into force May 25, 2018. The GDPR is a heavyweight, EU-wide legislation that will have far-reaching implications for organizations and their use and storage of EU personal data – in whatever form that might be, and wherever it is.

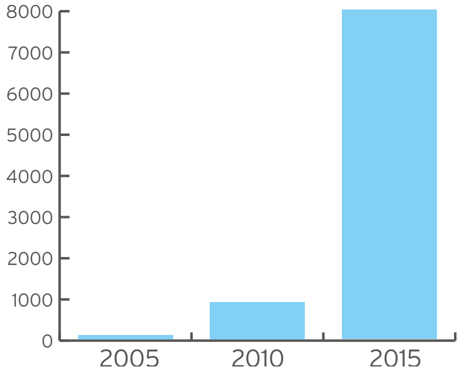
The GDPR will protect the right of a European resident to determine whether, when, how and to whom his or her personal information is revealed and how it can be used. It will apply to EU-based organizations as well as the data processing activities of those companies that target EU data subjects, regardless of location, and will control the acquisition, use, transmission, storage, destruction and breach of personal data.

The regulation requires that an organization seek permission from a local data protection authority prior to disclosing information to any governmental entity, with breach notifications required within 72 hours. Core to the regulation is that "sensitive information" (religion, national origin, medical history, sexual orientation) must be guarded more stringently.



As the proliferation of data increases, so do the vulnerability points as data travels across the Atlantic.

Expotential growth in electronic content



A decade of Digital Universe Growth: Storage in Exabytes[2]

Once GDPR comes into being, breached organizations will find the fines they face increasing dramatically. From a theoretical maximum of £500,000 (over $664,000) that the Information Commissioner's Office (ICO) can currently levy, penalties will reach an upper limit of £20 million (over $22.4 million) or 4% of annual global turnover – whichever is higher[1].

> FOR MANY BUSINESSES, THE THREAT OF INSOLVENCY OR EVEN CLOSURE AS A RESULT OF GDPR PENALTIES WILL SOON BE VERY REAL.

US state data breach laws

Finally, organizations need to ensure they adhere to US states' statutes relating to privacy breaches. California has been setting the standard by mirroring its statute on the existing EU requirements. Now, 47 states – as well as the District of Columbia, Guam, Puerto Rico and the Virgin Islands – have all enacted legislation requiring private, governmental or educational organizations to notify individuals of security breaches of information involving personally identifiable information. This personal information could be a name combined with social security number, a driver's license or state ID, or bank account numbers.

[1] http://www.itgovernance.co.uk/dpa-penalties.aspx
[2] IDC. "Extracting Value from chaos." June 2011

BUSINESS IMPLICATIONS OF A BREACH

- LOST REVENUE FROM SYSTEMS SHUTDOWN
- COSTS TO PROVIDE BREACH NOTICE
- FUNDING CREDIT MONITORING FOR EMPLOYEES AND CUSTOMERS
- BROKEN TRUST WITH CONSUMERS
- GOVERNMENT FINES FOR THE BREACH
- INCREASE CALL CENTER VOLUME
- EXPENSIVE REACTION SERVICES FOR CYBERSECURITY PROTECTION
- LITIGATION EXPENSES
- INCREASED INSURANCE PREMIUMS COSTS

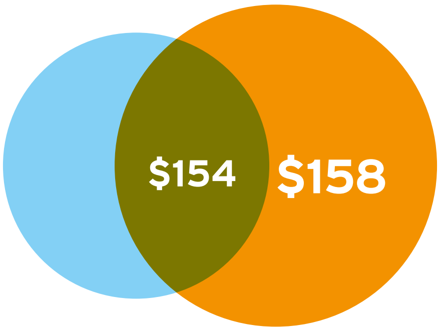
Tough realities of breaches

Data privacy breaches are now an unfortunate component of the modern business landscape. According to the Ponemon Institute's recent 11th annual Cost of Data Breach Study[3], the average consolidated total cost of a data breach grew from $3.8 million to $4 million. The study also reported that the average cost incurred for each lost or stolen record containing sensitive and confidential information increased from $154 to $158.

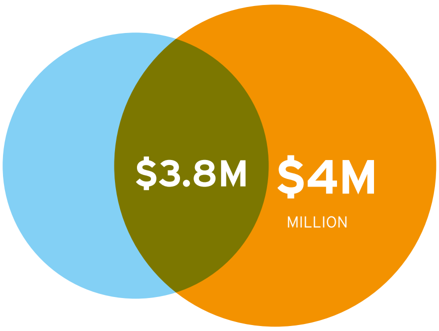
The threat is very real, with the global study putting the likelihood of an organization suffering a material data breach involving 10,000 lost or stolen records in the next 24 months at 26 percent.

The report cited that improvements in data governance initiatives will reduce the cost of data breaches. Incident response plans, employee training and awareness programs and a business continuity management strategy all result in cost savings.

Because of this, *insurers* are increasingly performing their own audits of a company's information governance framework when determining the cost of privacy breach coverage. The resulting rising insurance costs based on weak information governance will likely increase focus on improvements, particularly in areas of information retention and classification.



The average cost incurred for each lost or stolen record containing sensitive and confidential information increased.



The average consolidated total cost of a data breach grew.

[3] http://www-03.ibm.com/security/data-breach/?ce=ISM0484&ct=SWG&cmp=IBMSocial&cm=h&cr=Security&ccy=US&cm_mc_uid=58865641480014719419267&cm_mc_sid_50200000=1471941926

Responsibility lies at the top while successful organizational change requires all hands on deck

In certain countries, such as Germany, the board is already liable if a breach occurs. In 2014, the CEO of a US-based retailer with a national footprint stepped down after the company's high profile data breach. With this renewed focus on the CEO, and the multifaceted changes in processes required to adequately protect personal privacy, a fundamental cultural change is mandatory.

Worryingly, recently conducted Iron Mountain research on information management and security practices in the mid-market has highlighted how company executives are often the most cavalier about following processes designed to protect the integrity of information, ensuring it is managed securely and remains compliant with legal requirements. One in five (21%) executives responding to the Iron Mountain research say they find the processes too complex and look for a workaround. A further one in seven (14%) don't follow company policies governing information security because they find the policies too complicated, while 6% say they are completely unaware of any policies in this area.

Over half (57%) of the executives questioned say they have left business-sensitive or confidential information on the printer for all to see: just under half (49%)[4] have used a personal email account to send sensitive business information; 40% have sent information over an insecure wireless network; 43% have disposed of documents in a potentially insecure waste receptacle, and 39% admit to having lost business information in a public place.

It is imperative that company executives eliminate bad habits when handling private data if they are to minimize the risk of inadvertent data leaks and breaches of data regulation.

No time for excuses

With many organizations fearful of non-compliance, the retention policy often defaults to "keep it all just in case." In essence though, they are experiencing data clutter to the point of hindering their ability to manage daily activities. The justification will inevitably include the excuse that attorneys are fearful of litigation or bureaucratic sanctions for non-compliance. Yet, these businesses face tremendous information storage costs and are at risk of both violating new regulations requiring the deletion of private information and multiplying the entry points for hackers.

[4] "Business leaders revealed as biggest risk to information confidentiality", Iron Mountain mid-market research press release, Sept 2016

CREATING A CULTURE OF COMPLIANCE GOES BEYOND HAVING POLICIES IN PLACE. LEADERS MUST FOSTER AN ENVIRONMENT WHERE ETHICS, INTEGRITY, AND ADHERENCE TO POLICIES ARE REINFORCED IN THE DAILY BEHAVIOR OF ALL DEPARTMENTS AND DIRECT-REPORTS, INCLUDING:

- LINE-OF-BUSINESS EMPLOYEES
- CUSTOMER-FACING STAFF
- ACCOUNTING & PAYROLL
- HUMAN RESOURCES
- INFORMATION TECHNOLOGY
- SALES & BUSINESS DEVELOPMENT
- RESEARCH & DEVELOPMENT
- LEGAL

NEED FOR A CULTURAL SHIFT

Once an organization understands the facts surrounding its privacy management, records management and information storage costs, it will not be difficult to develop a compelling case for the need for a solid information governance framework. However, in order for the information governance framework to be adopted, there will need to be a fundamental change in processes throughout the entire organization.

Implementing such a cultural shift can foster a shared responsibility that provides the basis for future compliance. Iron Mountain can help identify the primary stakeholders required to participate in the transformation of processes and ensure they are aware of exactly what steps they need to take in order for successful transformation.

The cost of inaction

Attempting to meet the shifting compliance regulations while maintaining large data stores that have yet to be identified or classified creates an extremely difficult environment. With the dawn of Privacy Shield and GDPR, companies will see the timelines for notifications decrease, personal data collection more strictly controlled, and potential sanctions significantly increase. Instead of returns on investment, organizations should assess the costs of inaction to more accurately reflect the impact of inadequate information governance.

Information disposal

An important aspect of maintaining compliance through information governance is the defensible disposition of data no longer of value to the business or without legal requirement of maintenance. With information governance, less is more. With less information, it is easier and faster to retrieve relevant information, costs less to maintain, and limits liability to those whose information is deleted as soon as it no longer has business value.

According to a CGOC survey[5] of 1,300 Legal, RIM and IT professionals, more than two thirds (69%) of their corporate content was not required to be retained for either legal or business value reasons. A similar survey by AIIM put the number at 58%[6] and Iron Mountain regularly finds 40%-60% redundant, obsolete or trivial files (ROT) when conducting purges.

A classic study by DuPont's legal department[7] of nine litigations found that 50% of the electronically stored information (ESI) produced should have been destroyed prior to a preservation obligation arising. This failure doubled DuPont's eDiscovery costs.

[5] https://informationgovernance101.com/tag/regulatory/
[6] https://www.aiim.org/pdfdocuments/IW_RM-StratChanges_2011.pdf
[7] http://www.ittoday.info/Articles/Proactive_eDiscovery.htm

On a collision course

There are ever more stringent regulations coming into force in regard to protecting data, with the fines for not adhering to them now at business crippling levels. At the same time, the threats from cybercriminals are becoming ever more sophisticated. These challenges are colliding, creating the need for a paradigm shift within organizations to administer a robust default data retention policy.

The current paralysis existing in organizations on where to start requires organizations to quickly adapt to a new paradigm of "lean and clean" information to meet the privacy protection requirements and ensure they are not at a high risk for costly data breaches.

LEAN AND CLEAN

- **LEAN** REFERS TO ONLY MAINTAINING PERSONAL INFORMATION FOR THE AMOUNT OF TIME REQUIRED BY REGULATION
- **CLEAN** REFERS TO THE DATA SUBJECT HAVING THE RIGHT TO VIEW THE DATA BEING MAINTAINED TO DETERMINE ITS ACCURACY

Data Protection Officers

With the tsunamic rise in information growth in the past few years seen across all industries, the complexity of managing this information has resulted in newly defined roles such as Data Protection Officers, in fact with Privacy Shield there is a requirement for businesses of over 250 employees to employ one. However, with the role revolving around putting out fires as data growth leads to potential liability in courts of law, it is often a thankless task. In fact, it is a role that is often referred to as being hired to be fired, so help must be given through tools that aid in their ability to stay on the right side of compliancy laws.

PROTECT YOUR COMPANY AND YOUR CUSTOMERS' PERSONAL DATA BY:

- DEVELOPING CLEAR POLICIES AND PROCEDURES REFLECTING CHANGING LAWS, INCLUDING DEFENSIBLE RETENTION SCHEDULES
- ADOPTING A WRITTEN PRIVACY BREACH PLAN
- TRAINING AND TESTING STAFF
- NOT OVER COMPLICATING
- HAVING A CLEAR COMMUNICATION PLAN
- RAISING AWARENESS OF PERSONAL ACCOUNTABILITY AND COMPANY RISK
- KEEPING METRICS
- ENSURING ADEQUATE TECHNICAL MEASURES FOR DATA SECURITY

Producing a data map

An organization is required to retain different categories of information for various periods, depending on which jurisdictions apply. Determining the retention schedule through traditional methods of legal research is labor-intensive and expensive.

Organizations need to create a data map so they know what proprietary data they have, where is it physically, how sensitive it is and who has access. They should then only collect and store the information needed to remain compliant, so as not to fall foul of any data protection regulations.

Fostering a culture of compliance

Organizations are finding themselves on front-page news time and again for the wrong reasons. With the potential regulatory fines from exposing personal information via a breach running into the millions, remaining compliant is crucial. The best defense is implementing a broad set of operational and technical best practices that ensures you remain compliant.

It is important to understand that effectively handling private data, including a breach, is a shared responsibility of everyone in the organization from the CEO down. You need to create a culture of loyalty and accountability at all levels in a business; i.e., a firm wide moral code so that those throughout the organization will, in essence, self-police. A key to success is moving from a compliance perspective to one of stewardship. This perspective recognizes the long term impact to a brand, the importance of consumer trust and implications and considerations with vendors and business partners.

Next steps

Taking a broad-brush approach to meeting morphing regulatory obligations is not an option. **Iron Mountain's Global Research service and Policy Center solution**[8] can help your organization automate the development and maintenance of your retention schedule. Our Professional Services experts use a proven consulting methodology to define and build a research library tailored to your organization's risk profile and sized to your global footprint. As part of this process we can capture a data map for your information estate, highlighting where critical, sensitive and personal data exists. This will allow you to respond more quickly to requests from individuals about information you maintain about them, apply encryption technology, accurately identify candidates for destruction in a timely manner or tackle a breach in a more contained way.

Once your library and data map have been created and retention schedule developed or refreshed, you'll receive go-forward, up-to-date retention guidelines from the localities in which you operate through our Policy Center solution, a cloud-based portal where your retention schedule lives. You can update your policies to stay continually current so you can confidently destroy information when it reaches the end of its retention period. Experts are on hand to help explain what the changing regulations mean and empower you to keep control and mitigate risk at every stage of the information lifecycle – to drive policy adoption and reinforce proper handling of information in your new culture of compliance.

GET HELP NOW

If you want to learn more about this topic, Iron Mountain's Professional Services experts and the Global Research service and Policy Center solution can help your organization prepare to fully comply with applicable regulations. Iron Mountain can review or create your Privacy and Security Policies, assess the adequacy of your current data security, design a Privacy Breach Plan and identify retention schedules around applicable data protection regulations and map them to your current records.

In addition, Iron Mountain can help locate the PII you currently house and mask, encrypt or otherwise render it unusable, unreadable, or indecipherable to unauthorized viewers.

For more information please call:

1-800-899-4766

or visit
www.ironmountain.com/policycenter

[8] http://www.ironmountain.com/policycenter

ABOUT IRON MOUNTAIN
Iron Mountain Incorporated (NYSE: IRM) is a leading provider of storage and information management services. The company's real estate network of over 69 million square feet across more than 1,100 facilities in 37 countries allows it to serve customers with speed and accuracy. And its solutions for records management, data management and document management help organizations to lower storage costs, comply with regulations, recover from disaster, and better use their information for business advantage. Founded in 1951, Iron Mountain stores and protects billions of information assets, including business documents, backup tapes, electronic files and medical data. Visit: www.ironmountain.co.uk for more information.

About the author

Teresa Schoch, MSLS, JD, is a Principal in Iron Mountain's Information Governance & Digital Solutions practice. Ms. Schoch has worked in the RIM industry for decades combining her former litigation and e-discovery skills with records management and privacy management to address current information governance needs on a global scale. She has worked with large, global companies, as well as the US Federal Government, to address IG issues pertaining to legal holds, privacy and security, records management, and defensible disposition. She is a widely published author and is a frequent speaker at many information management professional association events.

IRON MOUNTAIN®