

# Information Governance Toolkit



FTI  
CONSULTING™

TECHNOLOGY



# Table of Contents

---

ARTICLE

3

**Achieving Information Governance Enforcement: Engagement, Enablement and the Change Journey**

*By T. Sean Kelly, FTI Technology*

---

ARTICLE

5

**Achieving Information Governance Enforcement: Ensure Policies Aren't Left to Collect Dust**

*By T. Sean Kelly, FTI Technology*

---

ARTICLE

7

**Skills Your Need To Climb the Mountain of Data Challenges**

*By Sonia Cheng, FTI Technology*

---

ARTICLE

9

**How to Safeguard the Crown Jewels in the Age of Information Security Threats**

*By Jake Frazier, FTI Technology*

---

ARTICLE

15

**Preparing for the Breach: A Look Into Essential Cyber IG Practices**

*By Ricci Dipshan, Law.com*

---

WHITE PAPER

18

**Tackling Data Security Risks**

*Advice from Counsel*

---

WHITE PAPER

28

**Identifying & Protecting the Corporate Crown Jewels**

*By Jake Frazier, Senior Managing Director, FTI Technology*

---

ARTICLE

40

**Why Data Deletion Makes Sense (and Dollars)**

*By Jake Frazier, FTI Technology*

---



# CORPORATE COUNSEL

An **ALM** Website

corpcounsel.com | March 3, 2017

## Achieving Information Governance Enforcement: Engagement, Enablement and the Change Journey

*T. Sean Kelly*

After years of wading through increasing data challenges and the unpredictable evolution of cyber security threats, corporations are increasingly considering the importance of information governance. We're seeing meaningful progress in the ability of legal, IT, records, compliance and security teams to work together and establish internal cross-functional IG committees. And with this progress is a growing eagerness among these groups to maximize and measure their investments.

Most large companies today have either implemented an IG program, hired IG personnel or have plans to do so in the near future. Those that have taken the step of getting programs up and running have typically spent a sizeable portion of resources to do so, and are accountable to garner some ROI from them. All too often, even after an investment into IG has been made, many projects are not monitored for compliance and success or kept evergreen, thus falling short of leadership's expectations for success.

Policy enforcement is a challenging task for most organizations—more so for those in regulated industries that have a highly complex



Credit: ranjith ravindran/Shutterstock.com

legal and compliance profile. The more regulated or more geographically diverse a corporation, the more burdened it will be with nuanced policies and compliance requirements. Legal hold is one common area where these challenges play out, as it can be very difficult for organizations to scope the correct individuals that need to be under legal hold, and limit retention to only those individuals, so excessive data isn't retained unnecessarily.

While technology is a necessary piece in ensuring that IG programs are sustainable and enforceable, there are best practices that should

be taken into consideration at the outset of any IG effort. Following is an outline of some guiding steps that will allow IG teams to build enforcement into policies from the ground up. Additional best practices will be discussed in a follow-up article.

- **Cross-Functional Support:** To be successful, IG must be a cross-stakeholder initiative with sponsorship from top company leadership. Legal, compliance, security, IT and records departments should work together to determine enterprise wide initiatives that need streamlining. Stakeholders can partner to

achieve their range of unique goals through the implementation of a single IG effort. But before creating a laundry list of needs, the team must work together to understand the confines of the internal landscape, such as the corporate culture as it relates to risk and changing business processes.

By evaluating each group's varying motivators through the lens of the company's culture, stakeholders can begin to understand the 'gives' and 'gets' involved in building new policies and implementing new technology. During these discussions, stakeholders should come to the table prepared with a risk analysis and ROI calculations for proposed projects.

- **Executive Sponsorship:** An IG project simply cannot be successfully implemented—or enforced—without C-level involvement. The key to gaining their buy-in is communicating the program's benefits that will specifically address their pain points. If the executive sponsor is the general counsel, building the risk case for that person is critical—this includes the risk of not disposing of data that has met its retention requirement, and is not subject to legal hold. If sponsorship is solicited from the CIO or another IT leader, they may be more likely to embrace a project that addresses data minimization and defensible disposal. Business leaders or board members will be more focused on the costs and overall impact to the bottom line and mitigated risk. Quantify what the business will save in the long run, the risks involved and how those risks will be mitigated. Generally, starting with small projects can show value

quickly and grow in scope (and ROI) over time.

The corporation's existing risk framework, which prioritizes the organization's highest risks, such as regulatory/sanctions, reputational, etc., can help the team evaluate which risk categories IG will impact, and make a business case for IG investments that can mitigate key risks without becoming financially prohibitive. This business case should also take into consideration the cost avoidance of possible penalties for failing to comply with various regulations in any region where the company does business.

- **Change Management:** In IG, the course of changing business processes should be rooted in compliance. Change is difficult for many people and becomes exponentially more so in large organizations where a wide range of varying priorities and personality types exist. Understanding how to effectively manage and enable change—and approaching it as a journey—is essential for anyone looking to drive IG. Legal and compliance departments have the opportunity to help their IG cohorts and the rest of the organization understand the fundamental legal and regulatory drivers behind the proposed changes.

One of the most widely accepted methods for implementing change management is the Kotter 8-Step Change Model, which was developed to help organizations become adept at progress. Some of the key tenets of this model, which will help with managing data challenges,

include creating urgency, clearly communicating the vision, identifying and eliminating obstacles, setting short-term realistic goals that foster a sense of achievement among those involved, and making changes permanent by solidifying adoption and addressing opposition head-on.

When in-house counsel work strategically with the IT and records departments, they can make a huge impact in implementing technology to enforce and support the policy and track company-wide compliance thereof. Establishing a cross-functional team to spearhead these issues with executive sponsorship is the critical first step in the right direction. Part 2 of this article—"Achieving Information Governance Enforcement: Ensuring Policies Aren't Left to Collect Dust"—will outline additional best practices that lead to IG enforcement and prevent important policies from falling to the wayside.

*T. Sean Kelly is a senior director within FTI Technology's information governance & compliance services practice.*



# CORPORATE COUNSEL

An **ALM** Website

corpcounsel.com | March 6, 2017

## Achieving Information Governance Enforcement: Ensure Policies Aren't Left to Collect Dust

*T. Sean Kelly*

A lot of organizations have created general information management policies, which are typically owned by the records or knowledge management teams. These policies include a retention and deletion schedule that in theory should be defensible, and address legal hold and compliance needs. But in practice, these policies typically cannot be executed upon or maintained. FTI's Information Governance & Compliance Services practice helps corporations figure out why their policies, well-thought-out implementations and information governance investments have been left to do nothing more than collect dust.

Legal hold is one common area where these challenges play out, as it can be very difficult for organizations to scope the correct individuals that need to be under legal hold and limit retention to only those individuals. This process requires close compliance monitoring to ensure that the process is defensible and safeguards against possible spoliation charges in litigation, which can come with steep penalties. Similarly, migrating to a new system—such as Microsoft Office 365—is another endeavor where the need to proactively



Credit: ranjith ravindran/Shutterstock.com

address and enforce IG becomes apparent. When corporations think about these issues strategically, IG parameters and legal hold needs can be built into new systems as they are integrated into the IT infrastructure.

Technology that allows the legal team to monitor data deletion and retention activities is a critical element. There are also best practices that can help ensure IG programs are sustainable and enforceable. Part 1 of this article—"Achieving Information Governance Enforcement: Engagement, Enablement and the Change Journey"—discussed the importance of cross-functional teams, executive

sponsorship and change management. Below are additional best practices that will enable the company's IG stakeholders to achieve long-term policy enforcement.

- **Training:** When rolling out a new legal hold program, Microsoft Office 365 migration or any other IG initiative, it is imperative to have a computer-based training module in place for all users. Executive sponsors can be particularly helpful in ensuring that the training is mandatory for everyone in the organization—a key factor in maintaining long-term viability of IG policies. Outside advisors can be particularly useful



at this stage, as they are able to help the internal teams outline the critical components of the program, develop audience specific training materials, identify what users will need to be trained on and determine what the depth of that training should be.

Training should not be out of the box from software providers, nor should it necessarily be the same for everyone in the organization. Training collateral should be tailored to the organization's unique needs and show users what the new policies look like within the context of their work environment. For example, for legal hold projects, it is important to establish if users understand which records and individuals may be subject to legal hold vs. which won't. It's also useful to build a dedicated page available to all internal users that offers reference guides and FAQs dedicated to explaining new policies and tools that are being used.

• **Strategic Technology Implementation:** Every technology evaluation that impacts the company's data in any way should involve the legal and/or e-discovery team, in addition to records, IT and compliance. This is particularly important when it comes to legal hold implementations. The process should start with clear goals for the project, such as, thoroughly retaining data for any custodians that are under legal hold, monitoring activity per compliance requirements and escalating events of non-compliance to stakeholders. The most critical feature a product should offer is the ability to monitor and flag activity—this will make

the biggest impact in achieving and maintaining IG enforcement. Robust monitoring capabilities will enable the IG sponsor to see when legal holds—or other policies—are not being acknowledged and escalate the issue to promote and enforce adoption of the processes.

Another important consideration is the existing data structure and overall IT infrastructure. For example, when an organization's data is all on shared drives, solutions must have the appropriate plug-ins to integrate with systems impacted. It is also important to consider how to automate deletion of data that is not subject to the established retention schedule, and strategically define when/how the organization stores its data. Having a set of clear goals at the forefront when evaluating technology will go a long way in ensuring that the team is asking the right questions during the purchasing process.

Tools that are offered as part of a broad suite of offerings typically do not have the sophistication to make sure nothing falls through the cracks. Best-in-class products that are purpose built for the one thing needed—such as legal hold or document and revision management—will be more successful in doing a thorough job and successfully integrating with existing systems.

A technology evaluation undertaken by a large manufacturing company serves as an example of one that was done really well. The company was liable for claims that otherwise could have been mitigated had the organization's data deletion

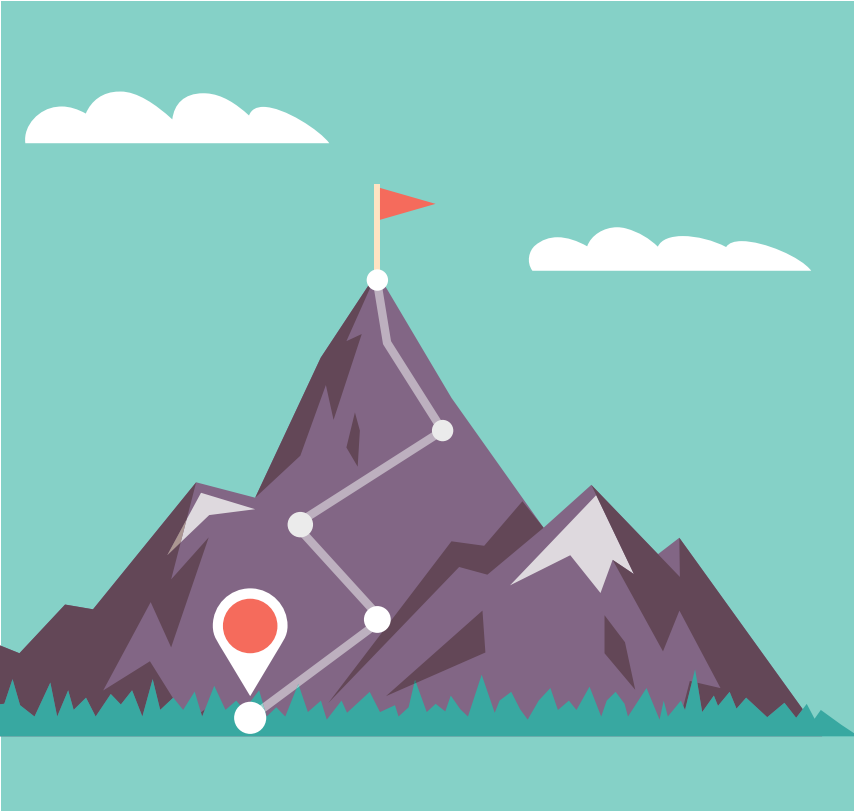
processes been executed. Essentially, the legal team was facing the burden to produce data that would have been defensibly disposed of had end-users complied with existing IG policies. By enforcing legal hold through a specific tool, and integrating it into their compliance and IT programs, the legal team was able to ensure that data could be defensibly and automatically deleted as soon as it was no longer subject to legal hold or any individual's retention schedule.

The ability to automate IG as much as possible, and track compliance across the company is absolutely critical in achieving ROI from the precious time and resources that are invested in building out these programs. Ultimately, it is up to the collaborative team of stakeholders to ensure that training and change management are addressed in a strategic and thorough way, and that technology solutions are selected based on the organization's unique and diverse needs. These important steps will promote IG wins and make it possible for the team to measure long-term adoption and success.

*T. Sean Kelly is a senior director within FTI Technology's information governance & compliance services practice.*



# Skills You Need To Climb the Mountain of Data Challenges



by Sonia Cheng

Sound information governance (IG) procedures are critical to broader legal, compliance and IT strategies. IG helps maintain compliance, reduce e-discovery costs, streamline large data volumes and bolster cybersecurity. Strategic and documented IG can also be helpful in defending data retention practices against motions for sanctions during litigation.

First, though, it is important to know what skills attorneys need to get these programs off the ground and how to bolster their abilities to ensure successful projects. Here are some of the skills needed to address data challenges:

**The initiative to secure collaboration across departments and among key stakeholders.** IG initiatives require approval and implementation from stakeholders across the organization; their success

depends on creating an inclusive team that reaches far beyond the legal and IT departments. Establishing appropriate policies and controls can be complicated by the requirements of various regulations, large data volumes, the number of individuals accessing records, new data types and the varied applications found within most organizations.

Any legal professional looking to work toward proactive IG must first have the initiative to secure buy-in across IT, information security, risk and business stakeholders and to foster a collaborative cross-department team that can work collectively on building IG goals and programs. Once stakeholders are on board, getting these programs off the ground becomes much more realistic. Involving the board and senior management is key to securing resources and funding.

**An understanding of security vulnerabilities and how to address them.** Figuring out where data breaches happen is critical to preventing them. Employee negligence, a mobile workforce and hacking are the top causes for breaches. One third of all known breaches come from loss of personal devices — and consider how much easier it is for a criminal to steal a device rather than penetrate an organization's network.

Counsel must be aware of the range of risks and work with other IG stakeholders within the organization to manage employees and ensure they understand their dynamic role in maintaining data security. An ongoing program that includes regular training and awareness campaigns is key to educating employees on current threats and how they can modify their behavior to reduce the possibility of a breach.

**The ability to manage change.** Change is difficult for many people, especially for attorneys rooted in traditional methods and resistant to adopting unknown technologies. Understanding how to effectively manage and enable change is essential for anyone looking to drive IG. Writing a data security policy is one thing, but the ability to translate security requirements into operations requires a holistic approach involving people, process and technology.

To do this, ensure that business executives are represented on the program's steering committee, and have metrics and accountability visible at the board level. Sometimes this requires engaging risk



and compliance stakeholders to ensure you have appropriate fail-safes to help reinforce change.

The widely accepted Kotter Eight-Step Change Model can help with managing data challenges. Some of its key tenets include creating urgency, communicating the vision, identifying and eliminating obstacles, setting short-term realistic goals that foster a sense of achievement among those involved and making changes permanent by solidifying adoption and addressing opposition head on.

**A sense of when to call in reinforcements.**

Outside experts can help guide IG efforts and identify weak points in the overall compliance structure, so know when to call on them. The IG professional must also evaluate these outside providers and be familiar with what to expect from them. The experts' findings not only inform stakeholders of needed improvements, they could also help sway reluctant executives to invest the needed time and money into these efforts.

Holding outside providers accountable to budget estimates, timelines, deliverables and security standards will go a long way toward ensuring initiatives meet internal benchmarks.

**A knowledge of sound budgeting practices.**

There is an ongoing industry-wide struggle to control e-discovery and other data-related costs. Knowing how to achieve budget predictability is a critical skill that can have a lasting effect on the success of any matter. As the industry matures, more lawyers are turning to master service agreements to negotiate alternative billing models and achieve greater budget predictability.

Another way to control budgets is to recognize the ways technology can affect the time and cost of a project. Sophisticated legal teams are using analytics and predictive coding to identify sensitive information for IG purposes or to uncover key facts for legal or regulatory matters. This helps reduce the time spent wading through large volumes of information, reducing overall costs.

**A solid grasp on technology capabilities and limitations.** Technology provides a variety of solutions to assist in getting data under control. When kicking off any initiative to address data security, remediation, preservation optimization or modernizing storage, the wise professional will become educated on the range

**The ability to translate security requirements into operations requires a holistic approach involving people, process and technology.**

and costs of technology solutions offered and emerging innovations disrupting the *status quo*. Without a clear picture of how technology plays into IG, lawyers will continue to struggle in addressing security challenges.

Counsel must also understand the limits of the technology being implemented and plan for how to navigate around those restrictions. Do not let perfect be the enemy of good. Take the time to prioritize requirements and implement solutions that address the biggest areas of risk.

**A global perspective.** Data breaches are a global problem, and your firm must stay current on the latest regulations wherever it has operations. The passage of the EU directive on the Security of Network and Information Systems (NIS) requires companies operating in critical sectors to satisfy wide-reaching incident reporting obligations. This, coupled with the General Data Protection Regulation (GDPR), which allows fines of €20m or four percent of global turnover, is a reminder to global organizations that they need to evaluate their obligations and take steps to be ready when regulations come into force.

**Skills To Climb the Mountain**

We continue to see that the rapid evolution across the legal industry is being met with flexibility, creativity and innovation. Legal teams are acting nimbly in a changing environment and are working diligently to stay in front of data disasters. The successes — and the failures — we read about in the headlines are shaping best practices for data security, IG and technology implementation. By building the skills and knowledge outlined above, practitioners will be better equipped to climb the mountain of never-ending data challenges. **P2P**



**SONIA CHENG**

As Senior Director at FTI Consulting, Sonia Cheng leads information governance initiatives for FTI's technology practice group, helping organizations deal with the challenges associated with exploding data volumes and complying with complex global regulations. Sonia has deep experience in transformation and change across related disciplines in e-discovery, records management, archiving and storage optimization. Contact her at [sonia.cheng@fticonsulting.com](mailto:sonia.cheng@fticonsulting.com).



This article was first published in ILTA's Winter 2016 issue of *Peer to Peer* titled "Professional Development: Sharpen Your Skills" and is reprinted here with permission. For more information about ILTA, visit [www.iltanet.org](http://www.iltanet.org).

# How to Safeguard the Crown Jewels in the Age of Information Security Threats

**By Jennie McQuade and Jake Frazier** Not all enterprise data is created equal, nor should it all have the same protections. Well-publicized data breaches, from customer credit card information to employee health records, highlight the increasing need for companies to better secure sensitive data. However, many organizations lack executive support for information governance, and others feel hampered due to their legal or regulatory profile.



In the last two years, data breaches have plagued organizations across every industry and in the public sector, including Ashley Madison, the IRS, BlueCross BlueShield, CVS, Experian, Army National Guard, Sony Pictures, and many more. As technology evolves and security risks rise, lawyers are confronted with an increasing challenge to satisfy their ethical duties of competence and confidentiality, making the issue of securing data and mitigating breaches increasingly severe.

This article will explore data breaches in detail, discussing how counsel can respond to these events, and outlining practical ways to implement a tiered approach to securing a company's crown jewels.

The recent *Advice from Counsel* (AFC) study, which examines practices within Fortune 1000 legal departments, found that 76 percent of respondents have information governance programs — dedicated staff and budget — and that data security is the number one driver for these programs. Similarly, an article in *Bloomberg Businessweek* cited insider threats, both intentional and accidental, as the biggest concern for more than 70 percent of information security managers. However, the initiatives cited in the AFC study ranged across 30 different focus areas, including data security, efficient records retention, data analytics, and data optimization for litigation needs, underscoring the challenge organizations often face with information governance. How can in-house counsel implement programs that are continually improving and holistically addressing all major data challenges, while simultaneously resulting in tangible benefits?

In looking at information governance for data security specifically, AFC study respondents identified four key areas:

- Securing sensitive personally identifiable information (PII) for clients/customers, patients

and employees, and fulfilling the responsibility for protecting the sensitive information of customers and employees;

- Securing sensitive company IP;
- Creating a tiered security network to protect against cyber security threats; and,
- Developing protocols and systems to ensure secure access to the network by partners and other approved third parties.

The parsing of “data security” into these buckets can help organizations take a large challenge — protecting the organization's data from internal and external threats — and channeling it into initiatives that are smaller, more focused, and easier to accomplish. Protecting customers' credit card information, for example, may require different technology and processes than authenticating the identity of employees trying to access the company's intellectual property.

Depending on the industry and its regulations, a company's crown jewels can include customer credit card records, salesforce client lists, proprietary IP, and employee or patient health information. Whatever a company considers its most valuable or sensitive data, the steps for securing that data through information governance are the same.

### Origins of security leaks

Understanding the root of most data breaches is critical to prevention. Employee negligence, a mobile

workforce, and hacking are the three causes for most breaches. Below is an overview of each of these areas, which is the first step in helping counsel understand exactly where security events originate.

#### Employee negligence

According to the *Ponemon Global Cost of Data Breach* study, breaches attributable to employee negligence rose by 72.7 percent between 2012 and 2013. The ACC Foundation's *The State of Cybersecurity Report: An In-house Perspective* found that in 2015, employee error was the leading cause for data breaches. This type of breach happens when employees accidentally download malware, fall victim to hacker schemes, or inadvertently email confidential information to the wrong contact, among other actions. It's important for counsel to be aware of this risk, and work with other information governance (IG) stakeholders within the organization to manage employees and ensure they understand their role in maintaining data security.

The 2010 breach of employee log-in credentials and other data at *Business Wire* serves as a prime example of employee negligence resulting in compromised security. In this case, a Ukrainian hacker penetrated *Business Wire* and other newswire companies using a tactic known as spear phishing. The hacker sent emails to employees that appeared to be legitimate. When employees clicked on the email, however, hackers then gained access to the entire company's



**Jennie McQuade** is the chief privacy officer and chief legal counsel for Swisslog Healthcare, a member of KUKA Group, a global supplier of intelligent automation solutions. The view expressed in this article are of the author's and not necessarily of Swisslog or KUKA Group.  
[jennie.mcquade@swisslog.com](mailto:jennie.mcquade@swisslog.com)



**Jake Frazier** is a senior managing director of FTI Consulting, based in Houston, TX. He heads the information governance and compliance practice in the technology segment, and helps identify, develop, evaluate, and implement in-house e-discovery and information governance processes, programs, and solutions. [jake.frazier@fticonsulting.com](mailto:jake.frazier@fticonsulting.com)

systems. There are many similar examples, which highlight how thorough employee education and training can make a notable impact on data breach prevention. Companies that fail to educate employees on potential dangers and safety best practices will remain at risk for future breaches.

### Mobile

One third of all known data breaches come from loss of personal devices, which is particularly troubling, as this medium simply requires a criminal to steal the device, rather than penetrate the entire company's network like with other methods. The increase in BYOD (Bring Your Own Device) workplaces is further complicating the risks of a data breach by mobile device, and will continue to be a dynamic problem for IT and legal departments.

In 2010, Educational Credit Management Corp., a nonprofit guarantor of student loans, experienced a breach of this nature when a portable media device containing sensitive data was stolen. The breach compromised PII such as names, addresses, and social security numbers for more than three million people, and was estimated to impact up to five percent of all federal student loan borrowers.

### Hacking

Cyber criminals, disgruntled employees, and corporate spies are all potential perpetrators of hacking. As noted in the BusinessWire example above, hackers will use tactics including spear phishing email attacks and website defacements to expose employee naïveté; or use malware and other tactics to break into corporate databases. Insider data theft and external data migration are common methods used by rogue employees or spies with inside access.

One of the most recent examples of hacking is the devastating Anthem, Inc. breach, involving the loss of personal information for approximately 80 million people last year. Hackers

compromised names, birthdates, medical IDs, Social Security numbers, employment information, and more for former and current customers and employees. This ultimately resulted in far-reaching consequences for the company and for the tens of millions of US consumers. This is the largest healthcare breach in history, and beyond the extensive cost and reputational damage to Anthem and its brands, the company faces regulatory discipline.

Hilton Worldwide also confirmed a data breach in late 2015, resulting from hackers gaining access into its point-of-sale systems, and installing malware that enabled the theft of customer names, credit card numbers, and security codes. The full scale and impact of this breach is still unconfirmed, but it serves as yet another example of the various ways cyber criminals can infiltrate corporate data, and why it is so critical to proactively identify and secure high risk data.

### Ethical obligation

Another key point for counsel is the matter of ethical obligation, specifically pertaining to what level of duty counsel has in both preventing and communicating data breaches. Federal and state laws require companies, including law firms, which are depositories of information, to implement reasonable security protections to safeguard personal data. In connection with these laws, companies must report breaches related to personal data. Currently, 47 states have "breach notice" laws, which generally require notice to all affected parties and relevant agencies within a certain time period.

For example, in New York, reporting is required as soon as possible, unless notice would impede law enforcement investigations. Fines up to US\$10,000 per instance of failed notification can result if reporting is not carried out in a timely and thorough manner. While the laws are clear that companies must

**While the law indicates that any reasonable anticipation of a breach must be reported to those affected, security teams can only investigate a fraction — about four percent — of these events each day, leaving a great deal of uncertainty.**

report suspected breaches to those impacted, a lot of gray area remains around the guidelines for disclosure. In some industries, customer contracts that require notification within a certain period of time are becoming increasingly common.

Most large corporations have, at a minimum, some level of security monitoring and notifications in place. According to a 2014 article in *Security Week*, these company devices are generating an average of 10,000 security events per day, with the most active generating 150,000 events per day. With tens or hundreds of thousands of potential breaches daily, there is no reasonable way for a company to disclose or even investigate each event. While the law indicates that any reasonable anticipation of a breach must be reported to those affected, security teams can only investigate a fraction — about four percent — of these events each day, leaving a great deal of uncertainty.

Last year, TalkTalk disclosed a breach that resulted from a distributed denial-of-service (DDoS) attack, impacting millions of its customers. While TalkTalk commendably took fast and decisive action in communicating the breach — to the extent of publicly stating that potentially all of its customers were affected — the subsequent investigation determined that only a fraction of those were actually impacted. This keenly highlights the complexity of breach investigations



## “Quick wins”

- Form a working committee across teams — security, legal, and IT — to get the conversation started;
- Develop short-term and long-term data security goals that can include:
  - To-do lists and timelines;
  - Creation of a Governance Committee to begin policy development;
  - Interviewing employees to map how data comes in and where it is stored;
  - Determining which department will lead the information governance initiative; and,
  - Deciding an information governance budget.
- Leverage existing security mechanisms and passwords to better protect devices;
- Develop formal policies to manage data; and,
- Include data security best practices in employee training programs, including for the pre-hiring and on-boarding process.

and the need to be thoughtful in determining when and how to disclose security events to the public.

Beyond duty to disclose, counsel is also obliged to consider the ethical obligation to maintain a level of technical savvy. In the *Play Visions v. Dollar Stores, Inc.* case, sanctions were ordered as a result of counsel’s failure to appropriately search for electronic records in a timely fashion as well as failing to guide the client’s production of discovery responses. Because counsel did not take an active role during the e-discovery process, they were ruled to have failed to meet the ethical obligation to competently represent the client.

ABA Model Rule 1.1 states “a lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.” In dealing with data breaches, it’s critical for counsel to understand the following:

- Data sources and retention practices: The lawyer needs to be able to identify and describe sources of electronically stored information (ESI), as well as understand the retention policies and practices that

impact on the availability of ESI for production;

- Impact of their choices: Counsel must know how their handling of ESI will impact the completeness and accuracy of their responses to discovery requests; and,
- Accuracy of facts: It’s key to have clear and accurate representation of the facts that are being shared with opposing counsel and the court.

### Finding and securing crown jewels

In information governance, counsel is almost always focused on litigation hold and managing e-discovery budgets. Legal teams want to support and implement information governance, but are unsure of how those initiatives map back to the legal team’s responsibilities and needs. Conversely, the CISO and CIO have growing budgets and an inherent focus on securing data and leading large, company-wide transformational initiatives that have long-term ROI. But these groups — and others — share a common interest when it comes to protecting the company’s most valuable data.

Generally, three key groups within companies should participate in identifying which data counts as a crown jewel: the legal department, the

records management group, and the businesspeople. Each group should be given access to the underlying database where the records are kept, as well as its own interface into the data. For example, the legal group interface can help manage legal holds, while the records management interface assists in tracking what information must be retained for which length of time as part of the company’s document retention policies.

Crown jewels can be separated into several categories: data that must be preserved for legal or regulatory obligation (i.e., legal holds); valuable data assets (IP or customer lists); and data that must be protected (customer PII, employee information). Once the crown jewels have been defined and located, processes can be developed to keep the data safe. When considering steps for securing critical information, organizations should look for solutions that protect against threats like hackers, but also safeguard data from those inside the organization.

By working closely with the stakeholders across the company, and with the CIO/CISO, legal teams can put protections in place and collaborate on programs that bolster e-discovery efforts, ensure fulfillment of legal obligations to secure data, and make it easier to mitigate increasing security risks. Some important steps to take in partnership with these stakeholders include:

- Establishing a sophisticated, central repository for the crown jewels, including granular security including authentication, access tiers, and controlled permissions;
- Supporting sufficient storage and backup for the crown jewels database;
- Enabling tracking for which employees are placing information in that repository and accessing data stored there;
- Ensuring email servers are private;
- Encryption of sensitive documents;

- Implementing Secure Socket Layer (SSL) protocol, which manages authentication and encrypted communication between users in a network;
- Using security information and event management (SIEM) tools to analyze security activity in real-time;
- Password protecting devices and keeping passwords protected and separate from encrypted documents;
- Employing remote access to wipe and locate lost or stolen devices;
- Controlling use of public cloud providers such as Dropbox and provide easy ways for employees to securely access these providers without hindering functionality; and,
- Training employees on policies, procedures and safeguards to ensure widespread adoption and enforcement of programs.

Some of the same techniques that help organizations identify their crown jewels can also help find documents that no longer have any value and should be deleted. Valuable information should be stored under lock and key, while the junk should be tossed out.

### Achieving quick wins

Nearly a quarter of advice from counsel respondents said that the initial challenge with information governance is deciding where to begin. To avoid this “analysis paralysis,” it may help to bring in a third party that can manage the project, achieve some quick wins (see sidebar), and build momentum for an information governance program without significant cost.

Through these quick wins, survey respondents with dedicated information governance programs have realized the tangible cost benefits and achieved an ROI through reducing storage costs, reducing the amount of data to review

as part of the e-discovery process, and reducing the risk of data breaches. As a result, in-house counsel can further protect the company’s reputation.

### Global considerations

Earlier this year, the European Union revealed that the new EU-US Privacy Shield agreement was forthcoming as a replacement for the former international Safe Harbor Privacy Principles adopted by the United States and members of the European Union. The Privacy Shield will outline and enforce rules for how protected data residing in Europe is transferred and treated across US borders, and aims to bring some consistency in ensuring privacy through international data sharing. Aside from the vast implications for cross-border e-discovery and investigations, the Privacy Shield will also affect how multinational organizations approach information governance.

The aforementioned steps for securing crown jewels include actions, such as scanning file shares and email, and migrating data to a central repository. However, corporations with global email systems are not able to take that approach given the varying data protection regulations across Europe (i.e., Privacy Shield), Asia, etc. Instead, counsel can implement a zone approach that isolates IG programs by region.

While an organization may run scanning tools on data residing in North America, that approach would potentially violate data protection laws in Europe or other strictly regulated areas, such as China. The steps for identifying crown jewels in international jurisdictions can be modified and tailored to comply with data protection requirements in each zone, ensuring consistent and adequate protection of the crown jewels company wide.

### Peer insights

In addition to the steps above, respondents in the AFC study mentioned

## The steps for identifying crown jewels in international jurisdictions can be modified and tailored to comply with data protection requirements in each zone, ensuring consistent and adequate protection of the crown jewels company wide.

earlier in the article provided their insights for broader information governance success. These include:

- Secure executive buy-in. “A program of this kind takes time and money so you need someone at the top level of management who “gets it.” It’s important to remind senior managers of their fiduciary duty to protect sensitive data.
- Develop cross-functional teams. To avoid duplication and wasted time or money, “you need to get everyone talking to one another about what they’re doing and what needs to get done.”
- Secure your sensitive data. “Invest in people that know how to protect data and how to use it effectively. Generating data is not very good unless you are ready to use it and can protect it.” This also includes ensuring that systems are up-to-date and back-up tapes are remediated in a timely and defensible manner.
- Don’t forget about data privacy regulations. “Beware of all of the international data privacy regulations and their amendments. You must understand that transferring data across borders is a very sensitive issue, even when the company has operations abroad.”
- Get outside help. For those in highly regulated industries, this was a recurring theme. “Work with professionals. Hire outside counsel



and others who have been there before. Make sure they understand your business to ensure that what they give you is not off-the-shelf, but suited to your business. It is basic common sense for anyone who is in a highly regulated environment. Each company's facts and circumstances are different so take the time to work with someone who knows you."

- Think about your end-user. "Give people tools so they are not taking shortcuts that bypass your protocols. Make it easy to access information so that people are not enticed into making poor judgments about the protection of information where you could have a breach."
- Don't let perfect be the enemy of good. Several study respondents discussed how to create realistic benchmarks that deliver results and focus on business requirements, even if they don't solve every challenge. One professional suggested, "To develop a complete map of what you have and where it is can be extremely time-consuming. We have incrementally become more aware of information that isn't governed as much as we thought because it exists in silos around the company in a way we didn't appreciate at the outset.

I view e-discovery as a targeted question you are answering and do as well as you can in satisfaction of all legal requirements. The information governance leaders are looking at it from a 'big picture' standpoint. They answer the broad question, but my obligation as in-house counsel is to focus on the narrow question. Working together, we try to draw some conclusions."

### Conclusion

Once crown jewels are properly addressed, it is critical to maintain protocol and ensure flexibility to address emerging factors. Existing systems may need updating on a regular basis, and older systems may not meet today's requirements. It should be noted that while the process to implement an information governance program often starts with the legal department, the long-term ownership may be a better fit for another department, depending on the company.

Companies that do not have the technical or policy expertise to properly and cost-effectively manage all of these steps are not alone, and can rely on third party experts to advise the implementation of new solutions and programs. This is where companies can begin to see tangible results, and experience how information governance can reduce costs and risk in the real world. **ACC**

---

#### ACC EXTRAS ON... Cybersecurity

##### **ACC Docket**

A Crash Course in Data-Security Regulation and Litigation (Sept. 2015). [www.accdoCKET.com/articles/resource.cfm?show=1408874](http://www.accdoCKET.com/articles/resource.cfm?show=1408874)

Cybersecurity — Emerging Trends and Regulatory Guidance (May 2015). [www.accdoCKET.com/articles/resource.cfm?show=1398885](http://www.accdoCKET.com/articles/resource.cfm?show=1398885)

Cybersecurity: How to Prepare for and Respond to Cyber Attacks (March 2014). [www.accdoCKET.com/articles/resource.cfm?show=1360853](http://www.accdoCKET.com/articles/resource.cfm?show=1360853)

##### **QuickCounsel**

Cybersecurity Failures and Resulting Liability Issues (April 2016). [www.acc.com/legalresources/quickcounsel/cybersecurity.cfm](http://www.acc.com/legalresources/quickcounsel/cybersecurity.cfm)

##### **Top Ten**

Top Ten Tech Tips for Corporate Lawyers (May 2016). [www.acc.com/legalresources/publications/top10-tech-tips-for-corporate-lawyers.cfm](http://www.acc.com/legalresources/publications/top10-tech-tips-for-corporate-lawyers.cfm)

Cyber Insurance Policies: Top 10 Questions Your Business Should Ask When Considering a Policy (Nov. 2015). [www.acc.com/legalresources/publications/top10-cyber-insurance-policies-top-10-questions.cfm](http://www.acc.com/legalresources/publications/top10-cyber-insurance-policies-top-10-questions.cfm)

ACC HAS MORE MATERIAL ON THIS SUBJECT ON OUR WEBSITE. VISIT [WWW.ACC.COM](http://WWW.ACC.COM), WHERE YOU CAN BROWSE OUR RESOURCES BY PRACTICE AREA OR SEARCH BY KEYWORD.

# Preparing For the Breach: A Look Into Essential Cyber IG Practices

By Ricci Dipshan

It's a situation every attorney dreads: You are sitting at your computer on what seems like a normal day, when suddenly the screen goes blank, replaced by a notice that your files are being held ransom or your most valuable data has been stolen out of your system.

In the immediate aftershock, myriad questions can run through your mind. But none is perhaps more important, more pressing, than—what's next?

The answer, explains Jake Frazier, senior managing director at FTI Consulting, depends largely on what has come before.

"Pretty much what I see is that the work you do before the breach is most everything you can rely on once the breach happens. Once the breach happens, it's really difficult to maneuver," explains Frazier.

Preparing for the question of "what's next?" ahead of time can at first seem like common sense, but it is too easy to underestimate the complexities and handicaps posed by an actual breach.



"We do these what we call table-top exercises, where basically we'll come in and it's like a war game simulation," Frazier says. "And we'll say we just learned the system has been comprised or this ransomware is happening, trying to encrypt things, so what do we do?"

Often when we work with clients who maybe have underestimated the difficulty of what would happen. They might say, 'OK, first I'm going to email so and so,' and we say 'No,

you can't email, email's offline—now what?' And then we just get blank stares and people immediately say, 'OK, we don't know what to do.'

The problem, Frazier explains, is that as cyberthreats have evolved, information governance programs have stayed the same.

"What information security historically has done was focus on the fortress approach—how do we put walls up to keep people out. So that would be proxies, firewalls,

encryption security event information management systems, etc.,” he says. “But as we’ve seen for the most part, that is not sufficient, people will get in one way or another, so the problem is once they get in through a backdoor or over the fortress wall, then they can just run amok.”

## Triage and Mirage

But this can only happen if data is out in the open for cyberattacks to exploit. Paramount to any data breach preparation is the golden rule of any information governance program: knowing where sensitive data resides. Yet this, of course, is much easier said than done.

“The key to a good IG policy,” explains Farid Vij, lead information governance specialist at ZL Technologies, “is having a complete understanding of your data at all times so that you can be in a proactive position during a data breach, which is the biggest challenge for enterprises today. There’s simply too much data.”

Thankfully, however, data breach preparedness doesn’t require an all-or-nothing approach.

“This isn’t about creating a basic data map; today, we have to get down to the content level of the document to identify things like personally identifiable information, personal health information, and payment card information.”

What this comes down to is extracting the most sensitive information among the daily network traffic and regularly created or obtained files, and placing

them in repositories with security provisions and data backup options.

“That’s definitely one of our most popular engagements right now,” Frazier says. He adds that in previous client engagements, “we were looking at the transactional data that had to do with account setup, and account numbers, things like that,” in which to create “a tiered approach where critical, private data goes off to other repositories that are much more secure, and your transactional data stays behind.”

While these repositories can have the usual layers of security such as “requiring stronger passwords and dual factor authentication,” Frazier notes that they can also provide “data masking.”

This entails scrambling data to create invalid credit card or Social Security numbers. These work as decoys to cyberattackers, while allowing developers to build and test apps using the information as well.

## Careful Sharing

Equally as important and valuable in data breach preparedness is controlling user access rights to these repositories.

“The key challenge with these breaches is often figuring out what data has actually been compromised and ironically, most organizations don’t know where to start,” says Vij. “Take Sony, for example. The majority of the risk and cost associated with the cyberattack was not the data that was directly hacked, but all the data

that the hackers got access to as a result of securing passwords and confidential information.”

But as Terrence Coan, senior director in the Law Firm Advisory practice at HBR Consulting explains, when it comes to delegating file access, the legal industry is ahead of the game.

“Law firms are obviously very organized around client and matter, so there’s an implied hierarchy; if I know who is authorized to access a client matter, then when I file documents into the system by that client and matter, the system applies the appropriate security to the matter team or to those who have reason or right to know.

Yet like any company in 21st century, law firms are also at the mercy of file shares, which while increasing employee efficiency and collaboration, potentially leave valuable data unsecured and accessible to all.

Frazier calls file shares “one of the least secure areas in a network, because it doesn’t have really rigid permissions. There are a lot of permission profiles on file shares that we see called ‘everyone,’ which means anyone who is in the network can just navigate to the file shares and have access.”

He adds that such areas have been used as “dumping grounds,” where in a recent engagement with a client, Frazier and his team found “a few petabytes of data.” Such fileshares, he notes, can include “HR records, compensation statements, customer records, and permission forms to set



up direct deposits with routing numbers and account numbers, and all kinds of really risky data.”

But like a potentially unsecure database, Coan says, file shares can be an easy fix. “We may lock those down and prevent people from filing to those locations going forward. While we may not delete the materials currently filed there immediately, we tell users that these locations are not an appropriate place to file materials, and if they do file materials on a network file share, we are going to purge them automatically within a defined period of time.”

## Of Man or Machine?

While breach preparedness seems simple in theory, execution may be a whole other story.

“On almost every engagement, I’m asked by the clients, do you believe in a human approach where users are going to classify the data and put it in the right spot, or do you believe in a more automated scanning approach? And my answer is always yes — both,” Frazier says. “So it’s always a belt and suspenders approach that works best.”

Using scanning and AI technology even on computers not connected to the network, he adds, can allow companies to find, move or lock down critical files.

“But in the end,” says Coan, “it often comes down to users having to interact with the data to have context to what the data is saying. If they have personal experience with it, they can then make an informed decision where it goes.”

Admittedly, it can be difficult to trust employees — after all, the rise of shadow IT, fileshares, and poor digital hygiene have made insider threats more probable than external breaches.

But employees will always remain central to breach preparedness and must be kept up to speed through constant training, Coan advises.

“It’s always more going to be a situation that they don’t train enough. And that’s because they can’t or don’t get the budget to do the necessary training and education. ... There has to be ongoing and routine training, there needs to be training for new employees who are brought into the organization, and there has to be refresher training of the entire employee population on some periodic basis. For example, every year or every couple of years, just to remind people about why this is important, why we are doing it and what we are expecting people to do.”

And more important, Fraizer notes, training works: “We find ultimately that through education and awareness, people do get better about how or when they use shadow IT such as cloud storage, or that they are more rigorous around defining who can access it and making sure that there are controls to minimize unrestricted access by somebody who shouldn’t have it.”

When developing a data breach preparedness plan, he adds, companies must also be careful not to set employees up for failure by encouraging them towards shadow IT or other risky tech behavior.

“In a breach, when systems start getting shut down, knowledge workers have pressure to get their jobs done. If all of a sudden emails are not working because there’s a breach, it’s not unlikely that you’ll see users using Yahoo, Gmail, Dropbox, Google Drive and really anything they can get their hands on to continue to do their job.”

Companies, Frazier says, need to let “users know if there’s a breach, don’t go using other systems, and your manager will take into account any lost time due to this breach — an escape valve, so that the day-to-day pressure is alleviated a little bit while the breach remediation is happening.”




**ADVICE**<sup>TM</sup>  
FROM COUNSEL

# Tackling Data Security Risks

**Data breaches. Employee fraud. Regulatory change.**

These headline-grabbing business challenges are keeping many legal, information security, IT and compliance departments up at night. Organizations are challenged to support the modern workplace environment – mobile phones, remote employees, cloud collaboration sites, social media, IM platforms and chatrooms – while keeping this data secure and easily retrievable for legal or regulatory needs. How can organizations create an information governance framework that protects data while staying adaptive to the rapidly evolving business landscape (*GDPR, Brexit, Privacy Shield, etc.*)?





**W**e asked this question of 33 information security, risk, legal, IT and compliance executives, most of whom work at Fortune 1000 companies with responsibilities that include anti-fraud, data privacy, regulatory compliance, information governance and other risk management activities.

## Seven key themes emerged:

1.

# Start with a Data Assessment.

For many, the process of beginning an information governance program can be daunting. *Where do you begin? Who should be involved? How do you ensure the right executive buy-in? How do you keep momentum going?*

To help answer these questions and focus the project, a third of respondents recommended conducting a data assessment at the outset.

## Advice:

---

A

“Conduct a baseline assessment without any assumptions and understand the company’s culture.”

B

“Start with an assessment and determine what is already being managed; since you cannot boil the ocean, you need to figure out where to start and where you need to go.”

C

“That risk assessment should drive where you need to focus your efforts.”

## Benefit:

Have a clear roadmap that will help you prioritize projects.



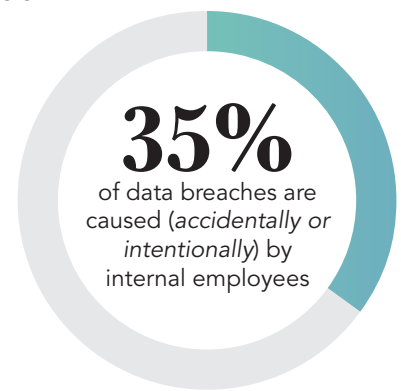


2.

# Engage Internal and External Experts.

Because of the risks involved, data security is now an enterprise-wide endeavor, and not just the concern of IT or information security teams. External data breach threats are rapidly evolving, and recent research from Forrester indicates that 35% of data breaches are caused (accidentally or intentionally) by internal employees.

To help offset this, most respondents recommended recruiting expert analysis to “determine where your weaknesses and gaps are” since “it’s hard to do that internally.” Or, as another respondent said, “Seek out external expertise because the field is too complex for any one individual to manage and the risks are too high.”



## Advice:

A

“If it is just you on an island, you will not succeed; tap into industry analysts and thought leaders for guidance since you cannot do it alone.”

B

“Hire someone with a good deep knowledge of technical implementation and crafting policy.”

C

“You need to ask someone and figure out what others are doing; engage a full cross-section of business personnel beyond senior leadership.”

## Benefit:

Subject matter experts can ensure your program is up-to-date, and internal leaders can aid in company adoption of best practices.

3.

# Prioritize Data Remediation.

Across the board, respondents expressed frustration at runaway data volumes, with over 90% saying they do not know how much data they are managing. Keeping redundant, outdated or trivial (ROT) information can make it harder to find and protect the truly sensitive information under the company's care.

Respondents recommend creating or updating an organizational data map, especially as part of a data assessment, and using data remediation to regularly cull out unimportant information.



## Advice:

A

“Data has a lifecycle and represents a huge liability today. At the end of its useful life, a company needs to purge it to promote an environment of data minimization.”

B

“The most important data held in Salesforce is not that substantial, but shared folders are filled with significantly more data. The key data is not that substantial.”

## Benefit:

Less data means lower storage costs and the ability to focus on protecting sensitive information.



4.

# Prepare for the General Data Protection Regulation (GDPR).

The impending GDPR regulation, set to go into effect in May of 2018, is top of mind for respondents with employees, customers or partners within Europe. The European data privacy law will harmonize European data privacy laws to ensure that data transferred from Europe to the US is appropriately handled and that personally identifiable information (PII) remains secure.

Respondents recommended conducting an analysis of the law to understand how this will impact current processes and systems.

## Advice:

---

A

“The company is developing a cross-functional task force to evaluate the different options supported by an external law firm.”

B

“The company will focus on alternatives, including implementing the model clauses, which will be part of an overall third party risk strategy.”

## Benefit:

Understanding and acting in compliance with GDPR from the outset of implementation can help your company avoid costly fines and reputational risk.



# 5.

## Use your Migration to Microsoft Office 365 as an Opportunity.

According to a recent Gartner survey, 54% of organizations will move to Office 365 in the next 1-3 years. The migration from one archive to another provides an opportunity for an organization to take stock of its email and data management practices and potentially update policies and remediate data for greater efficiency and security.

From legal holds to data retention and security policies, respondents in the process of migrating to Microsoft Office 365 shared how the procedure provides an opportunity to make additional process and policy improvements.



### Advice:

- (A) “Office 365 has new encryption technology to protect data better. The use of cloud-based storage for employees facilitates sharing, but opens up a new set of compliance standards and requirements.”
- (B) “The company implemented a 90-day e-mail retention program along with Office 365 so if you do not manage your e-mail within 90 days, it is automatically deleted.”
- (C) “Cloud e-mail in general has created information governance concerns, including expanded individual storage, which has created concerns about over retention resulting in litigation challenges, but there is better ability to search and manage the data, which is an advantage. The cloud system has inherent vulnerabilities, but Microsoft is a trusted partner.”

### Benefit:

Take advantage of a company-wide migration to remediate old data and update important policies and processes.

# 6.

## Right-Size Your Solutions.

Some organizations have faced major data breaches, regulatory investigations or large-scale litigation that warrants a complete audit and update of existing processes and technology. Other organizations may not have the same pressures, budget or appetite to make anything other than small changes to key processes.

Respondents repeatedly stressed the importance of fine-tuning any information governance and data security program to the particular needs of the organization.

### Advice:

---

A

“Know your audience and make sure the program is culturally adapted to the organization.”

B

“Knowing the population of people you serve personally, figuring out how to make compliance a value-added part of their activities, and fully understanding the businesses that you support is key.”

C

“The biggest thing is to engage the business and make sure that what you are doing is right-sized for the organization and that you have the resources to achieve success.”

### Benefit:

Information governance and data security have a greater chance of success if the program is fine-tuned to the needs and culture of the organization.



# 7.

## Data Security is a Multi-Faceted Challenge and Requires a Multi-Faceted Approach.

Given the complexities within the corporate data environment, there isn't a silver bullet technology, process or executive that can solve the immense problem of keeping data secure.

That said, respondents recommended a broad range of actions to ensure that an organization's people, processes and technology are all working in alignment to address various internal and external threats.

### Advice:

---

- A** "Encrypt data so that personally identifiable information is stored in a protected environment and access is limited to those with positions that require such access."
- B** "Some competitors pay 'friendly hackers' to test their systems."
- C** "Figure out how to get employees taking more training and determine how to make the training message more effective."
- D** "The ability to be prepared to take the necessary steps to protect customers when the data breach happens is as important as prevention; there is just as much liability created by a poor reaction as by the fact that it happened in the first place."
- E** "Encourage a clean desk policy so that information is secured at the end of the day and personal information is not left publicly available in breach of a client's security request."

### Benefit:

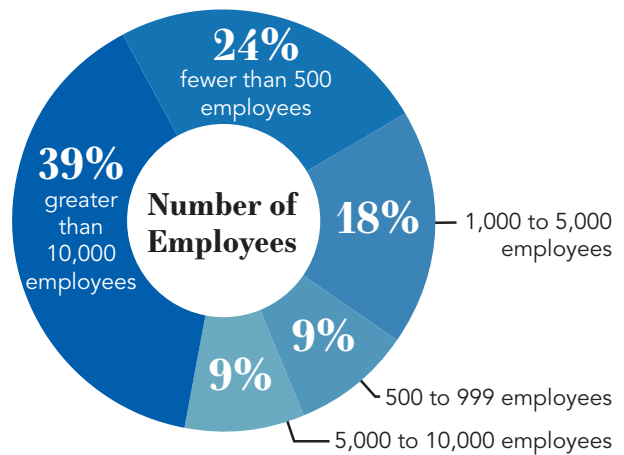
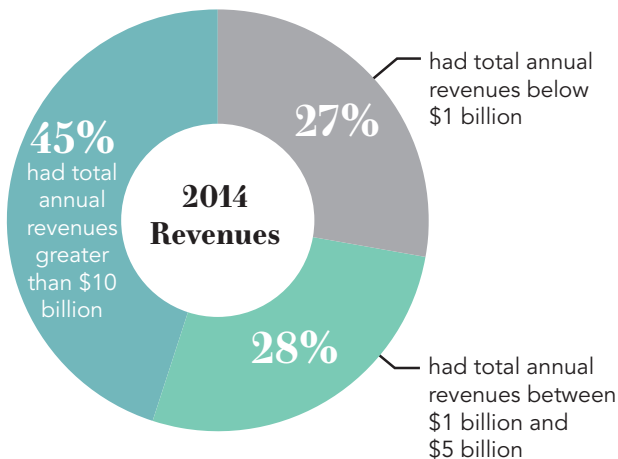
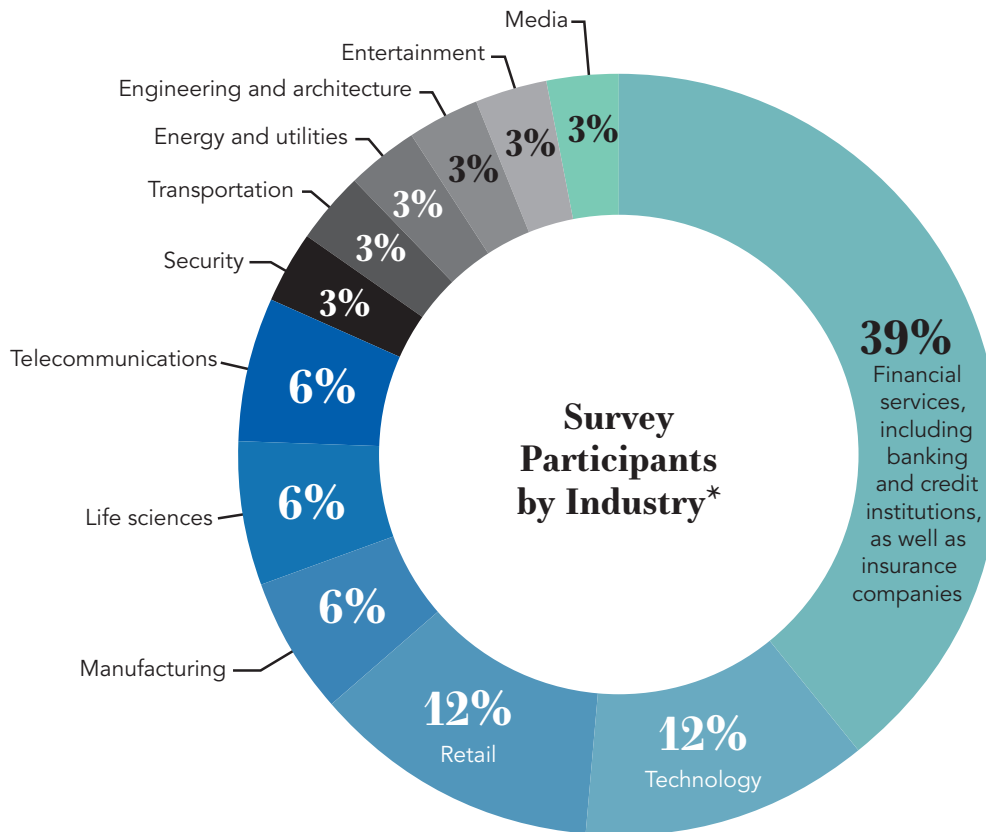
The adage "hackers only need to get it right once, whereas organizations have to get it right every time" is true, but implementing the right programs can help ensure better security. This includes regular employee trainings, using outside third parties to test your system, creating a tiered architecture to better secure sensitive information, and developing a data breach response plan.



# Appendix

FTI Technology partnered with Ari Kaplan Advisors to conduct the study by interviewing 33 in-house compliance leaders. Most participants were from Fortune 1000 corporations and all spoke by telephone, under condition of anonymity, during November and December of 2015.

Of this year's participants, 100 percent develop and implement compliance policies and processes, while 78 percent select, implement, or manage information governance software and service providers.



## About Advice from Counsel

Through in-person events, virtual meetings, webcasts, surveys and reports, Advice from Counsel helps e-discovery leaders share ideas and advice with peers in an open and collaborative forum. Begun in 2008 as an annual survey and report on top e-discovery trends, Advice from Counsel has evolved into an interactive community of e-discovery professionals working to strengthen the people, process and technology at the core of e-discovery. Advice from Counsel is sponsored by FTI Technology.



## FTI Technology solves data-related business challenges, with expertise in legal and regulatory matters.

As data grows in size and complexity, we help organizations better govern, secure, find, analyze and rapidly make sense of information. Innovative technology, expert services and tenacious problem-solving provide our global clients with defensible and repeatable solutions. Organizations rely on us to root out fraud, maintain regulatory compliance, reduce legal and IT costs, protect sensitive materials, quickly find facts and harness organizational data to create business value. For more information, please visit [www.ftitechnology.com](http://www.ftitechnology.com).

### For more information:

[ftitechsales@fticonsulting.com](mailto:ftitechsales@fticonsulting.com)

[www.ftitechnology.com](http://www.ftitechnology.com)

North America: +1 (866) 454 3905

Europe: +44 (0) 20 3727 1000

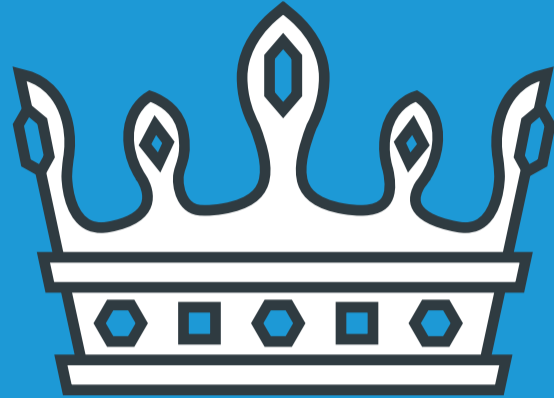
Australia: +61 (2) 9235 9300

Hong Kong: +852 3768 4500

Shanghai: +86 21 5108 8002

Tokyo: +81 3 5369 3939





# Identifying & Protecting the Corporate Crown Jewels

*By Jake Frazier, Senior Managing Director, FTI Technology*



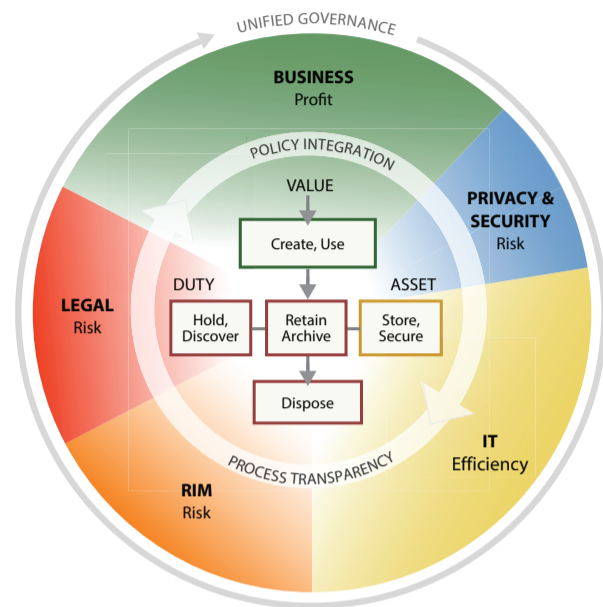
**A**nyone who owns a home understands they need a way to safely protect their family's "crown jewels," such as key documents, jewelry and irreplaceable photos, from theft, loss and catastrophe. Solving this problem is typically simple: buy a safe. Somewhat more complicated is the process of finding and determining what to put in the safe. Should the title to the car go in there? What about passports? If I wear my Rolex once a week, is it worth bothering to keep in the safe the rest of the time? And those photos of my grandparents are in a box in the attic somewhere; I really should find them and put them in the safe.

Similarly, every organization has a set of crown jewels—information that is critical, unique or irreplaceable. And much like at home, the most difficult part of protecting them is not actually the repository, it is determining what information qualifies for this type of protection, and finding it, and moving it to a safer place.

This is in part because no single person or department can define what constitutes the crown jewels. That requires a multidisciplinary,

### Information Governance Reference Model (IGRM)

Linking duty + value to information asset = efficient, effective management



**Duty:** Legal obligation for specific information

**Value:** Utility or business purpose of specific information

**Asset:** Specific container of information

Information Governance Reference Model / © 2012 / v3.0 / edm.net

cross-functional approach. It must encompass information that would be devastating to have stolen, but may also include data that needs to be exempt from disposition and can't be destroyed, such as executive emails under legal hold.

When identifying and protecting crown jewels, organizations must involve many stakeholders, determine the processes for keeping the data safe and create procedures for removing information that has lost its value. With the right tools and technologies, companies can keep their crown jewels from being lost or stolen.

# Categorizing Critical Information

Data cannot be simply locked up and shut away. If that happens, it becomes useless. Think about heirloom jewelry. It was meant to be worn, but if it is kept inaccessibly in a safe deposit box at a bank downtown, it cannot be. Similarly, paintings may be extremely valuable, but storing them in a fireproof warehouse makes them less enjoyable.

At the same time, it is critical to determine what type of information requires protecting. For example, much like flammable household products, some information may not be considered crown jewels, but can quickly cause tremendous damage in the wrong hands. Sony Pictures Entertainment learned this lesson when it was hacked last year and lost control of the Social Security numbers of workers who had long since left the company.<sup>1</sup>

Crown jewels can be divided into several categories and can exist in multiple locations and different formats:



## Information that may not be destroyed

Some information may need to be carefully maintained, not because it has intrinsic value but due to legal holds, regulatory requirements and other reasons.

This type of information can exist in many places within organizations, such as a file share, on an employee's mobile device or on a hard drive. It must be protected from inadvertent destruction.

Some of these files may be old or exist in legacy formats. When moved to a secure location, this type of data needs

<sup>1</sup> "Sony Pictures Reaches Settlement in Hacking Lawsuit," Los Angeles Times, September 2, 2015. <http://www.latimes.com/entertainment/envelope/cotown/la-et-ct-sony-hack-studio-reaches-agreement-to-settle-with-plaintiffs-20150902-story.html>

to be handled carefully, so that none of the metadata is altered. If no one at the organization knows what data exists and where it is, companies can easily find themselves with “dark data pools.” This can include decades-old paper files or microfiche that are in storage.



## Items of actual value

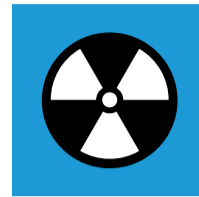
Like real precious jewels, some corporate information is truly valuable. This can include customer lists, formulas, intellectual property, schematics, pricing templates and other types of information that provide competitive and strategic advantage. As in the Sony case, it can also include master copies of intellectual property (e.g. films not yet released).



## Information that can be risky or dangerous in the wrong hands

Some information must be kept private, regardless of its actual value. Employee records are a good example of this, as are documents developed for regulators and documents that carry attorney-client privilege, or the Social Security numbers of the prior Sony employees. These documents are likely much more valuable

to outsiders than the company itself, and therefore must be protected carefully.



## Information that can be risky or dangerous to keep in any hands

Some information can cause significant reputational risk if it isn't protected. Other information can be very costly, particularly if it becomes potentially responsive in litigation. This was also a factor in the Sony hack.

Many organizations are confronting a relatively new problem, as their store of emails begins to stretch out for years and even decades. This can include emails sent and received by people who left the organization a long time ago. If these old emails contain keywords that have been identified as part of an e-discovery collection, those emails will end up in the document populations that must be reviewed. No one who is currently employed by the company may be familiar with the people or issues that have triggered the review. The document reviewers may not be able to determine if the emails are responsive, so they may need to produce them. Then the legal team has to answer questions about the emails. This can be enormously time-consuming and costly. It may also require companies to turn over meaningful documents to adversaries.<sup>2</sup>

<sup>2</sup> “The Best Way to Use Data to Cut Costs? Delete It” CIO Insight, August 17, 2015.  
<http://www.cioinsight.com/it-strategy/big-data/slideshows/the-best-way-to-use-data-to-cut-costs-delete-it.html>



By hanging on to information that is of no use, companies may also misallocate information that is very valuable. It's like buying an expensive sports car, and not being able to park it in the garage because of old furniture stored there.

The same tools that help organizations identify their crown jewels can also help find documents that no longer have any value and should be deleted. Valuable information should be stored under lock and key, while the junk should be tossed out.

---

**Valuable information  
should be stored  
under lock and key,  
while the junk should  
be tossed out.**

---





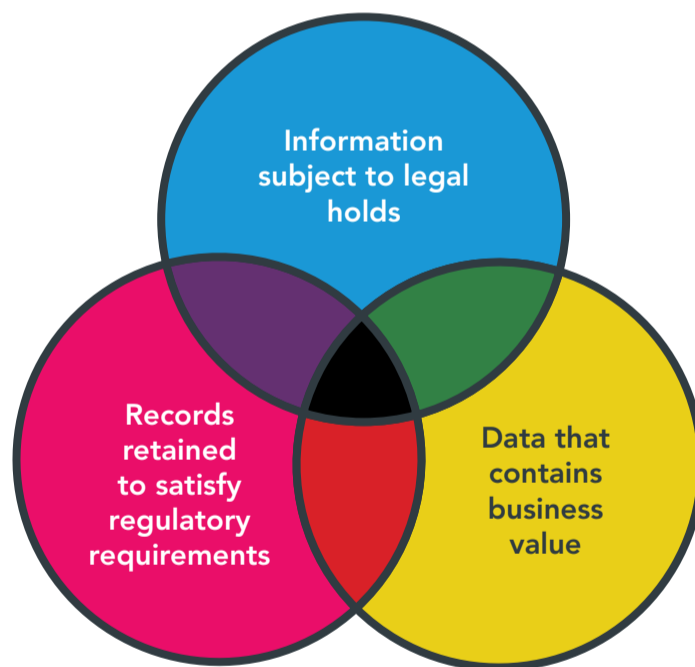
# Identifying the Crown Jewels

Deciding what qualifies as a crown jewel or one of the other important data types can be challenging, even after defining what all the types are. For purposes of simplicity, in this paper we will group all of the various types of important data under the crown jewels moniker. When grouping data it is tempting to rely on the information technology department, but this is often not the best group to make this determination. (They will protect the information, but someone else needs to define what is important and worth protecting.)

When figuring out who should identify the information that needs protecting, it can help to think of a Venn diagram. Crown jewels can be found in three types

of groups that can overlap: information subject to legal holds; records that must be retained to satisfy regulatory requirements; and data that contains business value.

Crown jewels can reside in any of these three circles. The rest is information that can be deleted according to the schedule of the company's records management program.



Generally, three different groups within companies

should identify the information: the legal department, the records management group and the businesspeople. But it's not necessary to form another committee and bring representatives from each group together to review every potential piece of data. Instead, each group should be given access to the underlying database where

the records are kept, with each group having its own interface into the data. For example, the legal group's interface can help it manage legal holds while records management's interface assists it in tracking what information must be retained for which length of time as part of the company's document retention policies.

One thing to keep in mind: important information is often kept together. Just as

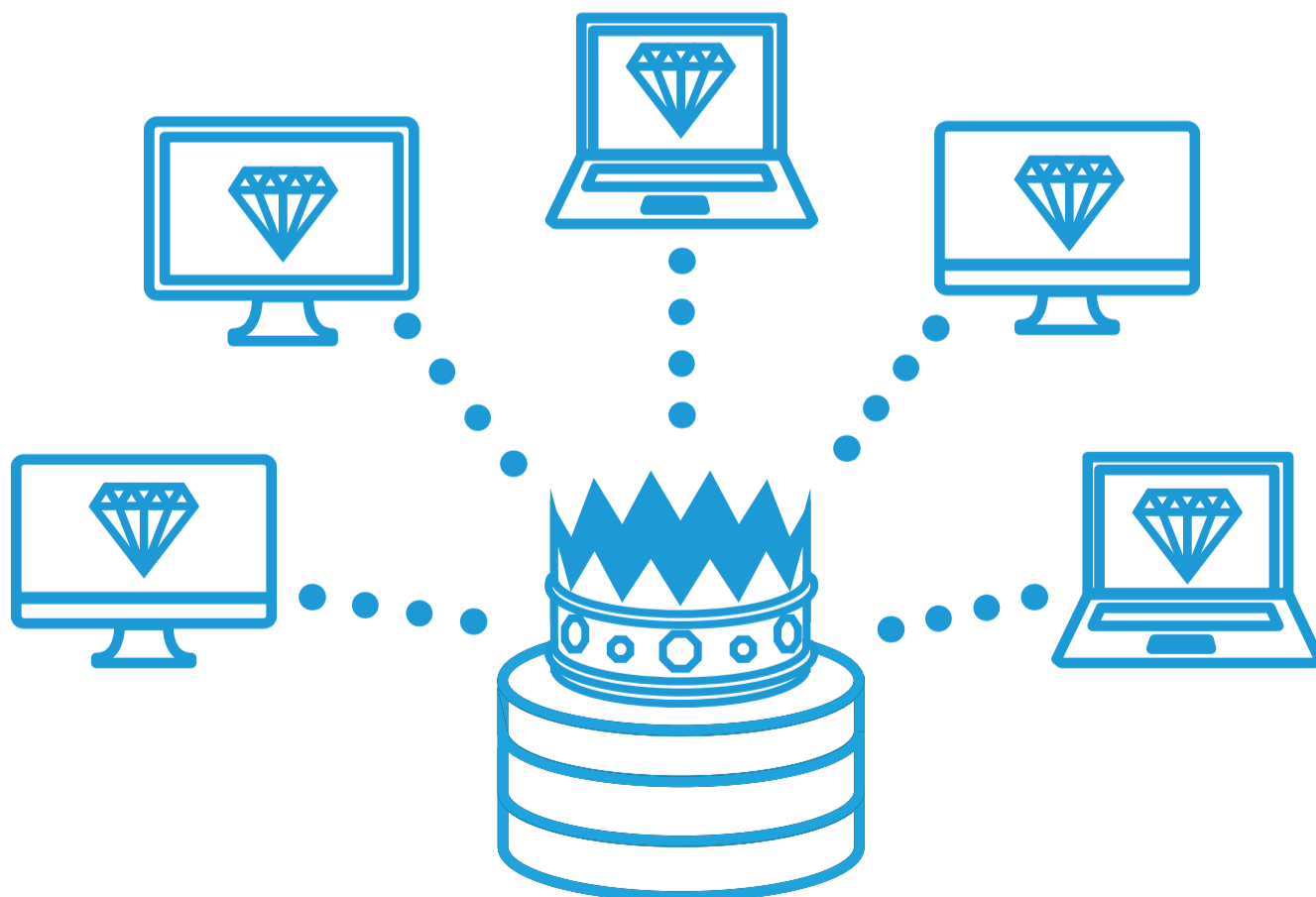
you may have all your jewelry in a single drawer at home, your customer lists may all be in the same electronic file on a

drive shared by the marketing department.

From a strategic value point of view, the businesspeople should decide how long information should be retained, based on the last

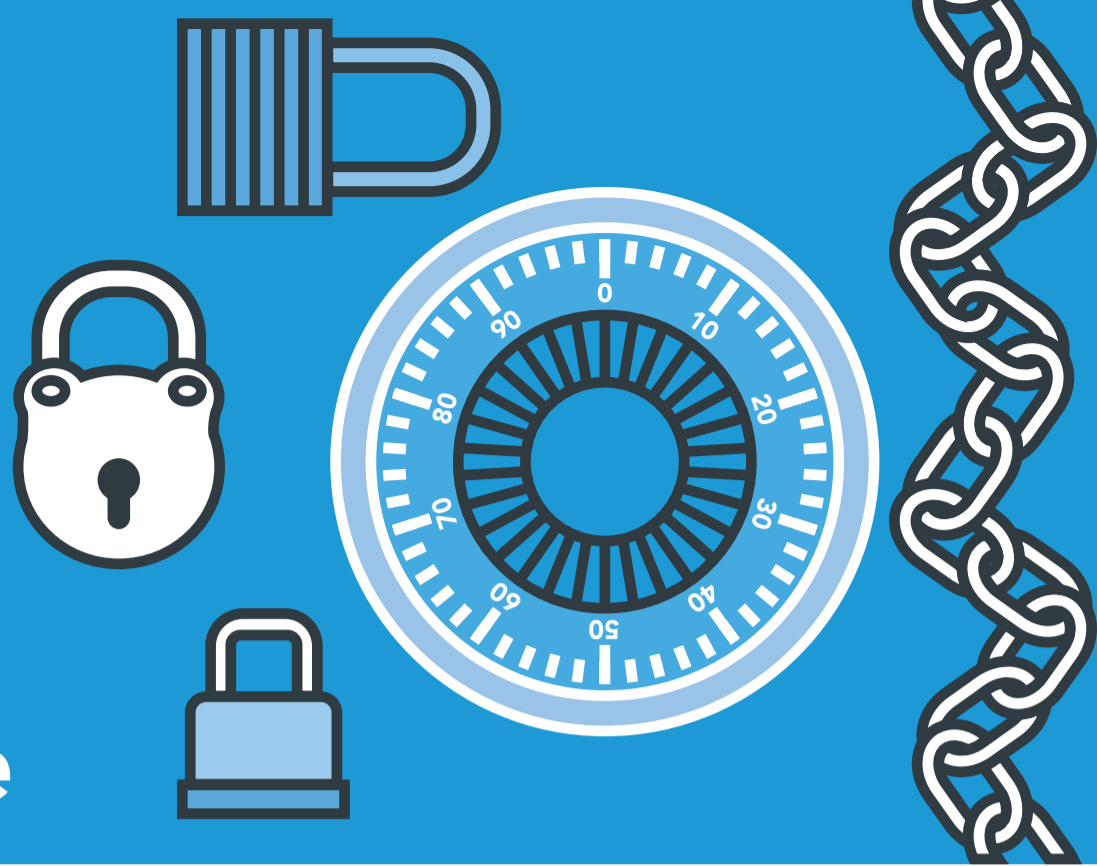
date it was accessed. In other words, if people are looking at the information, it has value and should be retained.

**Each group should be given access to the underlying database where the records are kept, with each group having its own interface into the data.**





# Keeping Information Safe



Once legal, records management and the businesspeople have determined what and where their crown jewels are, it's time to develop the processes to keep that data safe. In parallel with tracking which employees are placing information in the central repository, it's important to begin training.

When creating the repository for the crown jewels, organizations may be tempted to think of it similar to a home security system. Companies generally focus on designing systems to keep out external threats. However, homes are at a much higher risk from internal threats, such as housekeepers and other employees. When considering the process for securing critical information, organizations should look for tools that protect against threats like hackers, but they also need to figure out how to safeguard data from those inside the organization. These internal threats often come from those who aren't deliberately malicious, but

who hoard valuable data and never release it into the company's systems. Without a central repository to store the crown jewels, important information may exist that no one has visibility into or can find.

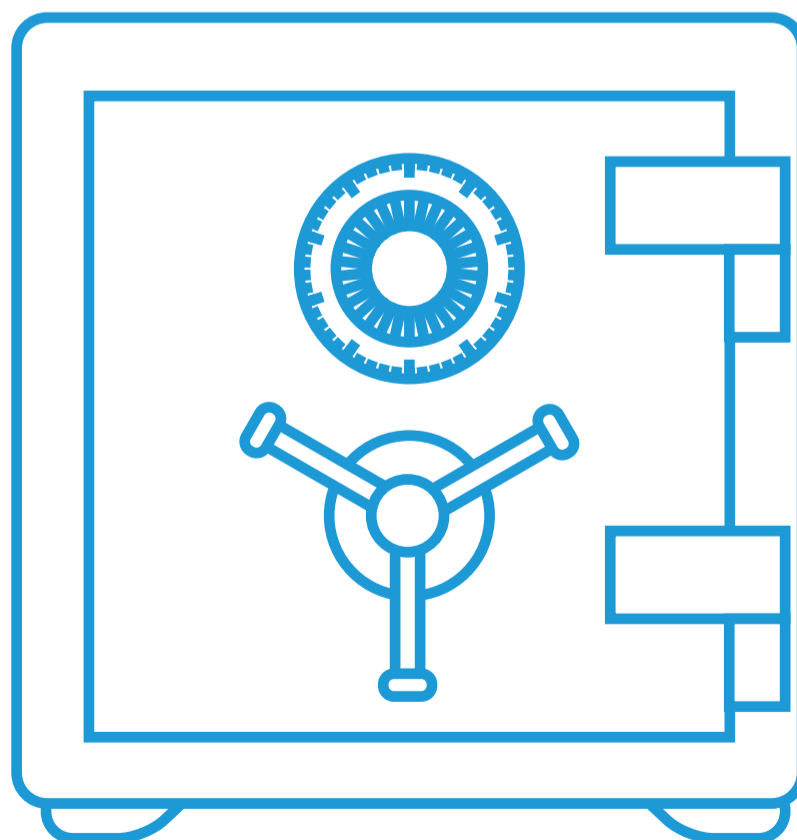
**When considering the process for securing critical information, organizations should look for tools that protect against threats like hackers, but they also need to figure out how to safeguard data from those inside the organization.**

And such a repository must be much more sophisticated than a simple file share, which any one can access and copy or delete files anytime. Rather, the central repository should have more granular security such as authentication labels, different access tiers and permissions in order to better control access. It also requires more sophisticated storage and back up protocols than a standard file share.

Creating an audit and reporting trail is extremely important. When someone identifies information as a crown jewel, it should automatically trigger a set of steps to identify and preserve that information. Companies should also institute and maintain a hierarchy of important data, since not all valuable information is equally valuable. For example, information that falls under a legal hold should have the highest priority.

From a change management standpoint, companies probably should not attempt all of this at once, as employees will become overwhelmed, systems may fail and momentum will be lost. The first step should be to report on which information is worth keeping, and then identify where the information resides. Before deleting the data, it should be moved to a secret place as a fallback, in case there are issues when the new system is being instituted.

Once procedures are in place, the company should regularly review and tweak them when necessary. More efficient processes may be identified, new regulations regularly emerge and legal holds could close, allowing data to be deleted. However, the technology itself should be extremely flexible, with no limits to data that can be classified as crown jewels.





# Creating Repeatable Processes Across Locations

All of this is challenging enough when companies only have one office or location. With multiple locations, the process becomes much more complicated. The terabytes and petabytes of data that companies today produce make it even harder to develop processes that are consistent and repeatable.

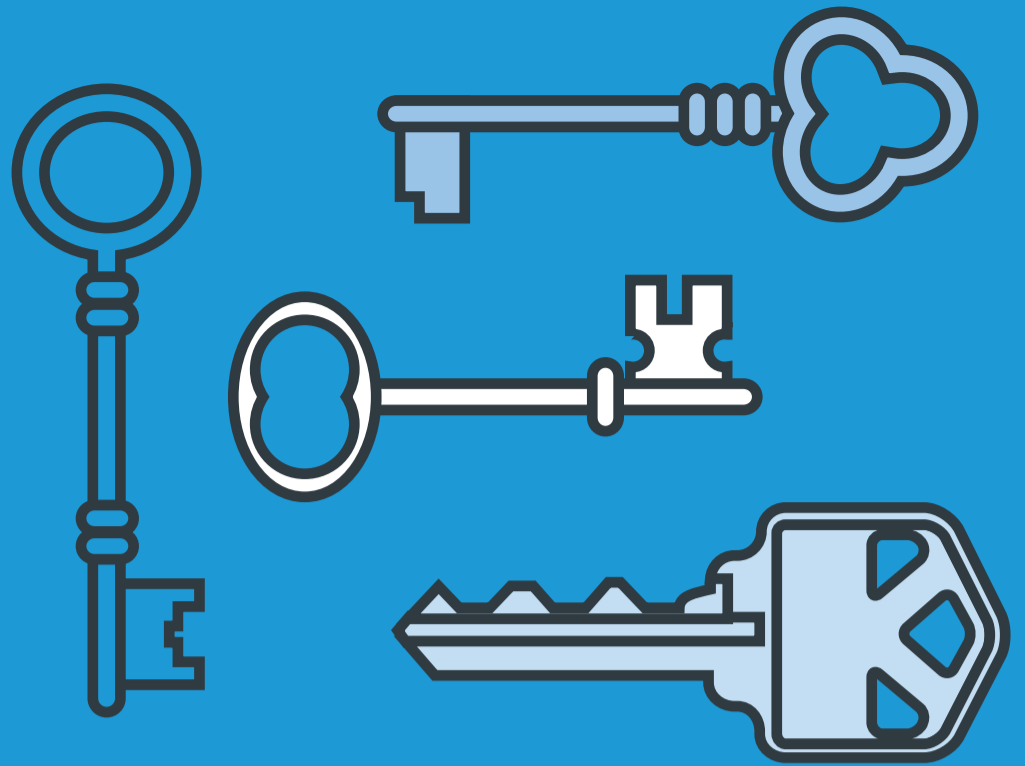
This is where technology comes in. Companies should consider factors such as using indexing rather than crawlers to find crown jewels. With e-discovery collection tools such as crawlers, the technology goes to files, opens them up, reviews them and then moves on. If someone at the company needs to revisit the file, the entire process has to begin all over again. Indexing presents a much smarter approach. With indexing technology, the system opens, scrapes and maintains information in an index, with a pointer to the file. (This is how Google works.) If updates are made to some files the next day, the system

knows when to skip files and when to review them. Indexing technology looks for additions, deletions and changes to files, and reindexes them every day. This enables a continuous process and keeps rules static until needed. That results in a much smaller expense.

**The terabytes and petabytes of data that companies today produce make it even harder to develop processes that are consistent and repeatable.**



# Locking the Safe



Once information is identified and located, it is critical to secure it in the correct repository and otherwise continue to protect it. This includes ensuring repositories are built on WORM (write once, read many) storage, properly migrating data from legacy archives to cloud applications, having—and adhering to—a policy for archiving emerging data types, keeping messaging policies updated and developing a cloud strategy. The fact that companies may not have the technical or policy expertise to properly and cost-effectively manage all of these steps does not make them less important and there are third parties that can easily step in to help meet those challenges.

This is where the rubber meets the road and companies can see tangible results. It's also one of the ways that information governance can be used to reduce cost and risk in real-world environments, by identifying and safeguarding the

company jewels. If companies aren't doing this already, they need to start before their most valuable possession are stolen or lost. And if they need help, they must find it.

---

**The fact that companies may not have the technical or policy expertise to properly and cost-effectively manage all of these steps does not make them less important.**

---

# About the Author

## **Jake Frazier**

Jake Frazier is a Senior Managing Director at FTI Consulting and is based in Houston. Mr. Frazier heads the Information Governance & Compliance practice in the Technology segment. Mr. Frazier assists legal, records, information technology, and information security departments identify, develop, evaluate and implement in-house electronic discovery and information governance processes, programs and solutions. These solutions are designed to produce the largest return on investment while simultaneously reducing risk.

# Why Data Deletion Makes Sense (and Dollars)





# Conventional wisdom says the cost of storing data is declining. Conventional wisdom is right ... and wrong.

**T**he price of disks has been dropping for years. According to Gartner, the **cost of disk storage per terabyte has been falling, too.**

Additionally, distributed computing, virtual machines and on-demand storage capacity that can be ramped up or down according to a business' needs all have combined to lower the total cost of ownership ("TCO") for storage. This has led many business executives to believe that the TCO for data storage will continue to decline ad infinitum, allowing them to collect all the data they would like to use to improve performance and drive top-line revenues.

All this would be true if not for several inconvenient truths.

Market research firm IDC estimates that the amount of all digital data created and consumed in 2012 was 2,837 exabytes. (One exabyte equals a million terabytes.) And that number is forecast to double every two years, reaching 40,000 exabytes by 2020.

Meanwhile, ICT Analytics reports that the amount of data being stored is **increasing, on average, 45 percent annually.** In fact, storage is the fastest growing cost within the enterprise data center.

But, one asks, what about the cloud? Doesn't cloud computing permit businesses to outsource storage to providers at a fraction of the cost of a proprietary data center?

Yes it does for some types of data. But it gets complicated for critical data. Data privacy laws vary by industry, by

country and even sometimes from state to state. The cloud storage providers' business model typically assumes they can move data freely from jurisdiction to jurisdiction — optimizing server capacity and availability and, thereby, controlling their own costs. Adding jurisdiction-specific requirements to a hosting contract often can increase the cost significantly.

In practice, with the rapid acceleration of the volume of data generated (all those exabytes produced by the proliferation of sensors, tablets and smartphones) and the concomitant increase in the data that businesses are storing, the total cost of data storage is not (despite conventional wisdom) declining. How could it? Walmart, for example, **handles more than a million customer transactions each hour and imports those transactions into a database estimated to contain more than 2.5 petabytes of data.**

Do the math.

If a hypothetical company stores one petabyte of data this year, it will store 1.45 petabytes next year.

If the cost to store data drops 15 percent a year (or even 30 percent at the high end) while volume grows 40 percent, it's easy to see that the conventional wisdom that the total cost of storage is declining *is wrong*. And this simple calculation does not include ancillary storage costs such as staffing; data backup; and confirmation that the data collected are accurate, useful and clean.

This growth in storage and its management is placing a growing burden

on all businesses — a hidden tax that is ever increasing. However, this is a tax that businesses can do something about. They can delete a significant percentage of their expensive-to-store data.

Unfortunately, while everybody is storing more data, very few are deleting any. Call it data hoarding.

## Data Hoarding: Sense and Nonsense

Not all data that businesses collect are useful. Indeed, as the enterprise's haystack of data climbs ever higher, businesses often do not know what data they possess. Much of the information may be — and frequently is — junk, and data analysts waste time working with this junk, finding spurious patterns within it, thus hindering the company's decision-making capabilities while incurring needless costs.

Why do businesses collect and store more data than they are able to process and use? One reason is Big Data hype and the vague belief that more is better — that somewhere in that ever-growing haystack is a golden needle that will produce new insight and generate additional revenues. This, however, is not a business strategy; it is a business wish.

Another reason businesses store data is fear of the possible legal consequences that may arise from deleting information. U.S. Securities and Exchange Commission regulations, for instance, demand that brokers and dealers **retain all client account information for six years and copies of all reports requested or required by**

**regulators for three years.** Regulations such as these encourage data hoarding, as many businesses believe that in the current rigorous regulatory environment, it is safer to keep everything and delete nothing. There is, in effect, no obvious incentive to delete, and underpreserving creates risk if data later are deemed critical or discoverable. Recognizing this growing problem, and the potentially unreasonable persistence of data, some European states have proactive deletion policies, especially in cases such as employee performance reviews and disciplinary actions. **According to the European Union Advisory Board on Data Protection and Privacy,** “The annual assessment of a worker contains information regarding a concrete date and a given contact. After some years, there is no reason in principle to store the information regarding such evaluations. Therefore, the retention period should be limited to two or three years maximum after the evaluation.”

In litigation, U.S. courts instruct juries to place a negative inference on the absence of relevant data such as emails, thereby encouraging businesses to store everything in the event there ever is a request to produce information in the discovery phase of a lawsuit or trial. However, that court mandate applies only if there was a duty to preserve the data in the first place. Unfortunately, that duty rarely is defined before a case is brought, and overpreserving, and failing to remediate backup materials, results in additional costs when there is a request to produce, as attorneys or e-discovery providers must spend time reviewing a greater quantity of material.

The hours add up.

**A 2012 RAND study found the cost to review one gigabyte of data was \$18,000.** Of course, improvements in e-discovery and predictive coding technologies can reduce those costs, but, again, as volume increases, those savings can be devoured.

Volume is key and creates its own risks. For one thing, if more data are stored, there, obviously, is a greater amount

of data to lose. Recent high-profile data breaches at various retail and entertainment companies have made public enormous troves of data.

Breaches are expensive. **According to a recent Ponemon Institute study,** the average total cost to an organization of a data breach in 2014 was \$5.85 million.

That’s real money.

And today, even smaller companies are collecting — and storing — an ever higher volume of data as smartphones make data more available to businesses. Almost all retail sectors are seeing **enormous growth in smartphone purchase conversion.** According to Cisco’s Visual Networking Index forecast, **global information processing traffic will grow at a compound annual growth rate of 20+ percent from 2013 to 2018, with over half of that coming from non-personal computer devices.** All this collected data attract hackers and other criminals, as personal credit information (which either can be used or sold) becomes more available and accessible.

Businesses can attempt to secure their data — as they should — but recent history indicates there’s no guarantee they can do so successfully. The simplest solution to the risk and expense of collecting and storing too much data is deleting the data not needed.

## Getting Rid of Junk Data Requires Information Governance

Storing data that businesses don’t have to keep ends up absorbing capital that otherwise could be deployed on operations or investments or return on capital. If a business chooses to reduce spending by cutting budget or laying off workers, in effect, it has (perhaps unknowingly) chosen data — much of which may be junk — over working capital and productive employees. It, therefore, is important to understand that junk data — and the attendant tax

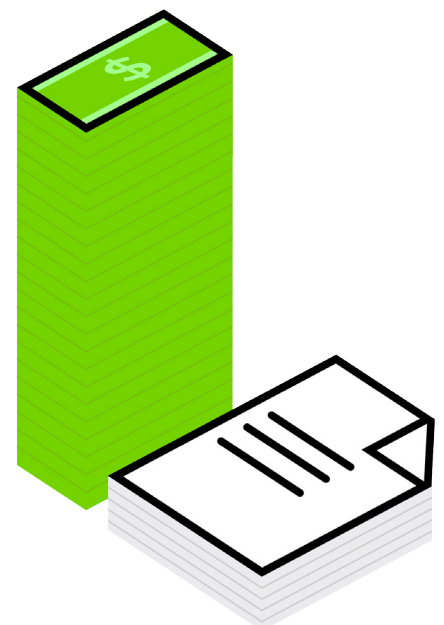
they levy on a company’s resources — are not an information technology (“IT”) problem; they are a business problem.

To attack the junk data issue, businesses must take a holistic view of the challenge, working across functions. That includes the chief information officer and the chief financial officer, as well as the company’s Legal, Compliance and Security departments. Working together, the company can determine what data it needs to store and what data it can delete. The return on investment (“ROI”) of deletion will become visible to the business as it begins to understand the extent of the resources needed to secure that data.

This is known as information governance. Good information governance requires creating a map of information assets across the business units, including cloud applications. This is the first step toward accurately classifying and categorizing data and allows a comprehensive assessment of which assets should be retained and which can be deleted.

Developing defensible statistical sampling protocols can help businesses reduce large amounts of stored media. Indexing and machine analysis of backup media can pinpoint what data should be preserved and what can be deleted.

Trying to delete large quantities of data manually is difficult and expensive; it is a



process that begs to be automated. This means establishing machine rules that mandate the deletion of unnecessary and vulnerable duplicates. These are created when multiple copies of documents or files are downloaded to often-insecure devices or when individuals email files to themselves. It has been estimated that in a number of companies, duplicated files represent 20 percent to 40 percent of the data. Reducing duplication is a good thing. It improves operational efficiency, as duplicate data drive up data volume while slowing processing times and hampering business agility. Deleting duplicate data also decreases legal review costs as attorneys no longer have to examine repetitious documents. Good information governance is an investment with an immediate and long-term ROI.

For example, in 2014, multinational metals and mining company Rio Tinto, which was generating a rapidly growing volume of data, identified approximately 40 percent of its stored data as junk or, in the words of its head of global business services, “eligible for defensible destruction.”

Acknowledging that Rio Tinto, like most large companies, is not good at “hitting the delete key,” the executive said the company saw “a strong ongoing business case” for lowering storage costs “while strengthening our overall information governance across Rio Tinto.”

It has been estimated that Rio Tinto immediately saved \$8 million simply by eliminating 35 percent of the file shares in its network.

In another instance, a top-tier financial institution was able to get rid of useless log files (records of requests to servers saved to hard drives, including those created during system installations) that were stored in the depths of its IT system and provided no value whatsoever. Working with FTI Consulting, the bank was able to delete hundreds of useless terabytes of data. At a cost to store of \$3.20 a terabyte, the company saved over \$600,000 in the first year and more than \$3 million over five years.

Another financial institution was sending thousands of backup tapes every month to an information management services company. Although the cost of storing tapes isn't large, the software that makes the tapes must be licensed from a software provider — a recurring and perpetual expense. Reducing the number of tapes and licenses translated to impressive savings for the firm.

## Of Course, No One Said It Would be Easy

In many businesses, data storage is considered an IT issue, and if IT tells a business unit leader that it wants to delete the unit's data, there's generally pushback. After all, the data belong to the business unit, not to IT, and maybe, just maybe, the information is valuable.

Even when an enterprise recognizes that it has a data retention problem, business-level views do not always align. The issue is that each business function considers data differently. Various functions have unique needs, requirements and targets,

and these factors often discourage deletion. It necessitates someone with appropriate perspective and seniority to see across the business' fiefdoms and work with Legal, Compliance, Security, IT and the business units to implement an information governance plan and begin deleting junk data. This is why, in the long run, information governance efforts have to be led from the top.

## No End to the Data Deluge

As smartphone adoption and use increase, the digital universe will continue to grow. Right now, digital's size beggars the imagination. In a few years, it will defy it. Unless businesses begin deleting data they don't have to have access to at the moment, they will jeopardize the technological, financial and operational resources available to collect, process and analyze the torrent of incoming data they will need later on. This may place them at a future competitive disadvantage while increasing the financial and legal risks currently being faced.

Deleting data is not really about saving money; it is about not wasting money and spending it, instead, on initiatives and innovations that drive revenues.

Deleting data, and the information governance processes that enable enterprises to do so safely and securely, is just good — and logical — business. ■

### Jake Frazier

Senior Managing Director  
Technology  
Information Governance & Compliance  
FTI Consulting  
[jake.frazier@fticonsulting.com](mailto:jake.frazier@fticonsulting.com)

For more information and an online version of this article, visit [ftijournal.com](http://ftijournal.com).





[www.ftitechnology.com](http://www.ftitechnology.com)  
[ftitechsales@fticonsulting.com](mailto:ftitechsales@fticonsulting.com)

North America +1 (866) 454 3905  
Europe +44 (0) 3727 1000

Australia +61 (2) 9235 9300  
Hong Kong +852 3768 4584

CRITICAL THINKING  
AT THE CRITICAL TIME™

#### About FTI Consulting

FTI Consulting, Inc. is a global business advisory firm dedicated to helping organizations protect and enhance enterprise value in an increasingly complex legal, regulatory and economic environment. FTI Consulting professionals, who are located in all major business centers throughout the world, work closely with clients to anticipate, illuminate and overcome complex business challenges in areas such as investigations, litigation, mergers and acquisitions, regulatory issues, reputation management and restructuring.

[www.fticonsulting.com](http://www.fticonsulting.com)