Brought to you by the publishers of COMPLIANCE WEEK

INSIDE THIS PUBLICATION:

Data Governance 101: Getting Started

Compliance's Role in Data Privacy Controls

Is Your Data Governance Function Mature?

The Keys to Better Access Control Systems

Hurry-Up Offense on Employee Surveillance

Ideas for Compliance, Audit & Cyber-Security

From FTI Consulting: Identifying & Protecting the Corporate Crown Jewels

Keeping Your Corporate Data

Safe Under Lock & Key

An e-Book publication sponsored by FTI CONSULTING | TECHNOLOGY

COMPLIANCE WEEK

Compliance Week, published by Wilmington plc, is an information service on corporate governance, risk, and compliance that features a weekly electronic newsletter, a monthly print magazine, proprietary databases, industry-leading events, and a variety of interactive features and forums.

Founded in 2002, Compliance Week has become the go-to resource for public company risk, compliance, and audit executives; Compliance Week now reaches more than 60,000 financial, legal, audit, risk, and compliance executives.

FTI CONSULTING™ | TECHNOLOGY

FTI Technology helps clients manage the risk and complexity of e-discovery and information governance. Our complete range of offerings, from forensic data collection to managed document review services, provides unprecedented flexibility to address any discovery challenge with confidence. Clients rely on our software, services and expertise to address matters ranging from internal investigations to large-scale litigation with global e-discovery requirements.

Inside this e-Book:

Data Governance 101: Getting Started 4
Compliance's Role in Data Privacy Controls 6
Is Your Data Governance Function Mature? 7
From FTI Consulting: Identifying & Protecting the Corporate Crown Jewels 8
The Keys to Better Access Control Systems 20
Hurry-Up Offense on Employee Surveillance 22
Ideas for Compliance, Audit & Cyber-Security 24

Data Governance 101: Getting Started

Experts advise a cooperative effort among management, compliance, and legal is the best way to ensure an effective data governance system

By Joe Mont

Data fuels modern business, but ensuring the quality, usability, and profitability of all that information remains a struggle. And not only does the use of that data need to obey ever-expanding regulatory demands and privacy laws; it should also help alert a business when an employee, unit, or supplier poses a risk.

That's a pretty tall order, then, for good data governance.

"The only good data that is worth investing in is the information that creates greater velocity in the way you make business decisions," says Jeffrey Ritter, a technology consultant and lecturer at Georgetown University's Law Center. "There is tons of data being collected. What businesses need is more information that is trusted and immediately accessible."

The concept of data governance—establishing internal controls, protocols, and procedures to ensure that data assets are managed well—is nothing new. In fact, many describe the current iteration of these protocols as "data governance 2.0," a term that encompasses the explosion of Big Data and its associated analytics. The truth, experts say, is that companies of all sizes, in all sectors, have plenty of work to do.

> "There is tons of data being collected. What businesses need is more information that is trusted and immediately accessible."
>
> Jeffrey Ritter, Technology Consultant, Georgetown University

"Across the industry we are playing data defense," says Alan Paris, global head of financial services consulting for eClerx, a global technology company. "How do you transform that into data offense? How do you actually monetize data? How do you use the approach that you take to data, data management, and data governance to drive business? There is a lot of wood to chop there, and a lot of opportunity yet to be mined."

"With all of the competitive pressures that are on companies today, they can't afford not to know that the information is accurate," Ritter says. "They can't process fiction." Likewise, there must be assurances that the information can be used and analyzed without violating any regulatory obligations tied to the data. In privacy law, for example rules pertaining to personal information limit the use of that data. "That's important to the compliance community because their job is to align those rules of use to information assets," he says.

To understand what must go into a data governance initiative, think of it as an e-discovery program on steroids. The first objective is to make sure you know what data you have and that you can easily catalog and access it. Taking that inventory, however, cannot be offloaded to IT, since the business units are in the best position to know the data they need and the risks (regulatory or otherwise) that they face.

Collet

Protocols to govern data should be developed through a cooperative effort that includes management, compliance, and legal. "Traditionally the hardest problems to solve are the ones that are not solved in a single line of business or in a single workflow," says Harald Collet, global head of Bloomberg Vault. "You need a strong-willed and forceful leader, because there are a lot of obstacles to getting five or seven different parts of the company all on the same page."

"You need executive buy-in and support," says Rex Ahlstrom, chief strategy officer for BackOffice Associate. "How high up the food chain can you get? That will depend on a company. Maybe it's the VP running a division or the CIO, but somewhere along the line you need the buy-in."

Put to rest the notion you can just plug in a solution. "You can't just buy it," Ahlstrom says. "It needs to be a combination of the new processes you will have to implement, tying it into business value, and creating the right reporting structure so you can demonstrate a return and expand. You can't solve this with technology alone. You have to start with the right people, the right processes, and the right organizational structure."

Business owners "know what that data is used for and where it gets leveraged when they run those business processes," Ahlstrom adds. "If business is not a stakeholder and owns this, IT really has no idea where to go or what to do." He points to a Gartner statistic that shows how companies might bridge the gap between IT and the business: The research firm predicts that by 2017, 50 percent of companies will have a chief data officer.

Collet's advice for organizations is to avoid the temptation to "attempt data governance across the entire company." Instead, he says, you should narrow the scope of the implementation by focusing on the most regulated line of business.

Small Bites

Breaking the task into steps will also help navigate the complex world of data privacy laws. "You have to implement a data governance solution, but unfortunately you can't move the data into any kind of central place because of the data privacy rules in other countries," he says. "You can

end up in a stasis of not being able to do anything because of all the risks that operations, compliance, or legal teams see."

By prioritizing efforts within specific geographies that are less challenging, a data governance program can still gain momentum. "You need to set a strong business strategy so that instead of worrying about all the risks and unknowns, you make intelligent tradeoffs between a business strategy and the risks that are involved in deploying solutions in a certain way," Collet says.

"Certainly there is a strong cyber-security mandate now," Collet adds. "You have to get your house in order and know what data you have in order to protect it."

> "Getting your data act together is paramount to avoid steep fines, reputational risk, and embarrassment."
>
> Alan Paris, Global Head of Financial Services Consulting, eClerx

"Getting your data act together is paramount to avoid steep fines, reputational risk, and embarrassment," Paris says. "The stick is the regulatory fines you want to avoid by getting your data act together. Then, there is the carrot where you can actually run a more efficient and less capital-intensive, less costly business environment."

A data governance program needs to ensure data quality and reliability. "You have to fix the data at the source and you can drive accountability by creating scorecards and rating people for, essentially, their data citizenship," Paris says.

Some companies, Paris says, are considering whether to factor those goals into compensation. "So, if you are a bad actor and consistently providing poor, unclean, or spotty data to the rest of the organization, that's going to affect your paycheck," he says. "Managing compensation is a very good way to manage behavior and provide the proper incentives."

Just as company websites can mine a wealth of relevant customer data, social media can also be ripe with helpful information, including insight into customer behaviors and buying patterns. A company can assess its reputation, see whether marketing efforts resonate, and even pick up on inadvertent pricing and labeling issues. The challenge, as it is with other data streams, is separating good data from the bad, and that is easier said than done, given the sprawling nature of social media sites.

"Social is an interesting data source that presents interesting problems," Collet says. He suggests that it be viewed as a subset of the company's overall approach to collaboration data and use of services like Yammer, Salesforce Chatter, Bloomberg terminals, and other communication channels.

"Social media seems different, and can be very fragmented, but what you want to do from an enterprise data management perspective is not treat it as something that is very different," he says. "Treat it just as you would your e-mail system or an instant message sent inside the company. Then you can start getting consistency across the channels and a 360-degree view of the interactions." ■

BUYING INTO DATA GOVERNANCE

The following, from a blog post by Michele Goetz, an analyst at Forrester Research, details research by the firm into how vendors are adapting to the evolution of data governance.

- Vendors are still married to the legacy of data management owning and running with data governance focusing capabilities toward tactical data governance
- No single data governance tool manages across all five data governance pillars (MDM, data quality, ILM, metadata, security), although some vendors (IBM, Informatica, SAP) can with significant integration between products.
- Only two vendors (Trillium Software, SAP) provided data governance metrics that linked data conditions with actual business outcomes (regulatory risk, total cost of ownership, etc.)
- Only one vendor (Collibra) has an in market tool that provides a data governance 2.0 environment specifically for strategic data stewardship and operations.
- Significant product innovation is coming (from more application like tools to better user interfaces and reporting) that will lift data governance management out of IT and into the hands of the business.

What you should know when considering data governance tools:

- There is no single solution, but data quality, master data management and metadata management often are tightly connected to govern across.
- Identify tools that enforce best practices for the administrative aspects of data governance. Keep in mind the end user is the business and may not be a "data geek."
- Look carefully at what it takes to connect data conditions and processes to business outcomes as this effort may be a Business Intelligence on Data project.
- Understand the vendor roadmap. Choose those that have solid strategies and prototypes/early releases geared toward the strategy, process, and administrative aspects of governance, not just data management and data processing.

Source: Michele Goetz, Forrester Research.

Compliance's Role in Data Privacy Controls

By Joe Mont

Around the world, governments are responding to the massive trove of personal data companies and healthcare entities are amassing and a rash of data-security breaches with new, strict guidelines, regulations, and laws. In response, privacy and compliance programs are increasingly at an intersection.

Unfortunately, working together is often easier said than done, and the regulatory focus on data raises an abundance of questions. Should compliance oversee privacy, or must they be independent? What defines a healthy working relationship among those involved, including compliance, IT, marketing, and the board? A panel of privacy experts addressed these questions, and others, during a session at the 2014 Compliance Week Europe Conference in Brussels.

Build Bridges

A key to bringing compliance and privacy together lies in diplomacy, Jennifer Aikins-Appiah, regulatory compliance officer for CPA Management Services, said. When implementing a privacy program, even one with top-level sign off or executive sponsorship, departmental silos need to be broken down.

"There is no point implementing something that no one is going to buy into," she said. "Ultimately these are going to be the people who ensure compliance among their staff. They are going to be your gatekeepers."

Reaching out to middle management and IT and privacy corners of an organization, rather than issuing marching orders, is far more effective in getting buy-in and much-needed help, Aikins-Appiah said. However, compliance officers shouldn't fear standing their ground when the need arises. "Sometimes you do have to be a little confrontational," Aikins-Appiah said. "I don't mean put on your boxing gloves and wage world war within your organization; what I mean is to have open conversations. Some of the concerns may actually be justified and valid because the people you are talking to have more experience with the departments you are trying to reach and the things you are trying to implement. Their advice will help your policy go much further."

After a privacy program is implemented, a CCO should maintain his or her charm offensive," Aikins-Appiah said. "Don't become invisible," she said. "You have a privacy-by-design program you want everyone to abide by, but then go and sit at your desk all day where no one can see you? Put yourself out there. Try to engage not just with the managers but all levels of staff." This outreach will help give the CCO a better view of what is happening in these various entities. "You want to be on the forefront of any potential risks around data breaches," she added."You need to be on the ball."

Watch the Headlines

Being on the ball also requires knowing what is happening around the world, not just within company walls, Aikins-Appiah said. When Canada passed its new anti-spam law it had implications on marketing efforts, and those issues had to be dealt with immediately. Enforcement matters must also be keenly watched as they give a sense of governmental priorities and help set company risk weights.

Other developing trends include E.U.-wide privacy rules that, although delayed, could go into effect by 2017; the continuing U.S. crackdown on healthcare data breaches; and the growing concern over Big Data.

Multiple Hats, or One?

Should privacy and compliance be melded together? Uwe Fiedler, global privacy officer for Parexcel International, a pharmaceutical research company, sees value in keeping the various efforts within each function separate.

"It is helpful to have separation," he said, explaining that the role of both compliance and privacy officers is to report risks to the board and leave the matter in their hands. To ensure that the board takes matters such as privacy and breach notifications seriously, he suggests a firm recitation of all the executives and board members who have either lost their job or gone to jail for their negligence.

> "It's a lot of work, but you have to start somewhere. You have to put together a country-by-country, state-by-state matrix of all the breach rules, including how they define sensitive information."
>
> Jose Tabuena, Chief Compliance Officer, Next Health

"One of the issues is of size and scale," countered Jose Tabuena, chief compliance officer for Next Health (and a Compliance Week columnist). "At smaller, mid-size companies it is probably too much to have a chief in every area—chief information security officer, chief information governance officer, chief anti-trust officer. All of these to typically fall under the risk domain of compliance, which is the overarching framework. In most of my experience the chief compliance officer is also the chief privacy officer." At his company, a healthcare start-up, he serves as the compliance officer and has a privacy specialist who reports to him. That specialist and has more day-to-day responsibility for privacy issues.

Tabuena did concede, however, that in some industries the "privacy risk might be so large that you start having to put more resources in that area."

What's on the Horizon?

The need for compliance, privacy, and IT to work cooperatively will only become more pronounced in the months ahead.

At the conference, Sophie Nerbonne, deputy director for legal affairs and director of compliance at France's Commission Nationale de l'Informatique et des Libertés, dis-

Continued on Page 25

Is Your Data Governance Function Mature?

By Jaclyn Jaeger

Most companies still have lots of work to do to turn their information governance into "mature" programs, where they can extract value and insight from their troves of data while minimizing security and privacy risks. The good news is that progress is being made—albeit slowly.

That's according to the findings of a report from the Information Governance Initiative (IGI), a think tank dedicated to advancing information governance practices and technology; it polled 100,000 IG professionals on the subject. The report asked companies about their IG function maturity, what IG projects they're undertaking, the timeframe and costs involved in achieving those projects, and more.

Blair

"To date, very few organizations have taken a coordinated approach to how they manage and monetize their data," says Barclay Blair, IGI founder and executive director.

Overall, most companies rate the maturity of their IG programs as "nascent"—that is, they have some elements in place and are building the foundation, but many relevant information-related functions remain missing or underdeveloped. Others rated programs as "intermediate," meaning they are building the framework, according to the IGI report.

Robinson

"Many organizations are beginning to acknowledge the need for proactive IG functions, but most have been slow to develop and implement these functions in a sustainable and consistent fashion," says Eric Robinson, a solution architect for Kroll Ontrack.

In its simplest terms, information governance is a cross-disciplinary approach of governing and managing data across disparate systems and business functions. Historically, companies have struggled to manage risks across siloed risk management functions: cyber-security, records management, privacy, legal, and more. The goal is to have visibility into all those pockets of data at once.

Typically, information governance gets kick-started by a risk event—such as litigation or an investigation—when the company suddenly realizes it has no idea what data it has or where that data resides.

In addition to litigation and an investigation, the surge of cyber-attacks is also driving companies to ask probing questions about their data security and retention policies: What data do we keep? What data do we throw away? What data do we invest time and money managing? "Cyber-security is a huge driver for organizations to get their information house in order," Blair says.

CIGO Function

To put a formal structure around some of the answers to those questions, some companies—MasterCard, Aon, McKesson, and Autotrader.com, to name a few—have appointed information governance officers, tasked with coordinating the company's information governance program.

In the early stages of an IG program, many companies said the role of the chief information governance officer (new acronym time: CIGO) is to build a foundation of information governance. That requires someone with sufficient authority and leadership skills to see that the work gets done, according to the IGI report. As a company's information governance improves, CIGO's role is to develop the framework of an information governance program and then maintain and improve on the IG program as it develops and matures.

According to the IG report, CIGO has three primary tasks:

» Information leadership. At most organizations, nobody "owns" the information problem. CIGO fills this leadership gap by taking on accountability for the governance of information in all forms across an organization.

» Inter-departmental coordination. Information-related

Continued on Page 25

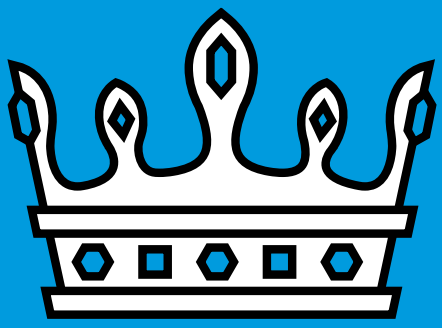
UPCOMING IG PROJECTS

How many projects do practitioners have planned in the coming year? See below.

Projects	Practitioners
Updating policies and procedures	69%
Scanning paper documents	50%
Data consolidation and cleanup	47%
Migration of unstructured information from one system to another	46%
Defensible deletion	42%
Decommissioning an archive or system	40%
Implementation of a new corporate governance framework for IG	37%
Data loss prevention	31%
Implementing legal hold tracking	30%
User rights audit and analysis	22%
Big Data analytics	15%
Creating a new senior role for IG and filling that role	9%
Other	5%
Monetizing data	5%
We aren't doing any IG projects currently/don't plan to.	6%

Source: Information Governance Initiative.

CGOC
THE COUNCIL



Identifying & Protecting the Corporate Crown Jewels

By Jake Frazier, Senior Managing Director, FTI Technology

FTI™ CONSULTING | TECHNOLOGY

Anyone 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.

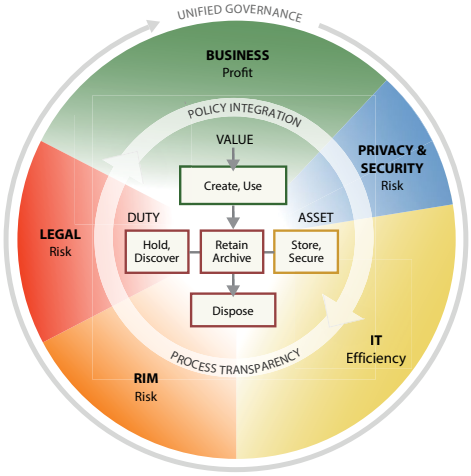
Similarly, every organization has a set of crown jewels—information that is critical, unique or irreplaceable. And much like at home, the most difficult part of protecting them is not actually the repository, it is determining what information qualifies for this type of protection, and finding it, and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

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 / edrm.net

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.[1]

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

[1] "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

needs 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.

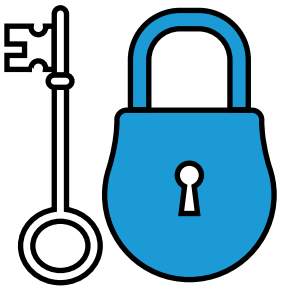
Many organizations are confronting a relatively new problem, as their store of emails begins to stretch out for years and even decades. This can include emails sent and received by people who left the organization a long time ago. If these old emails contain keywords that have been identified as part 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.[2]

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.

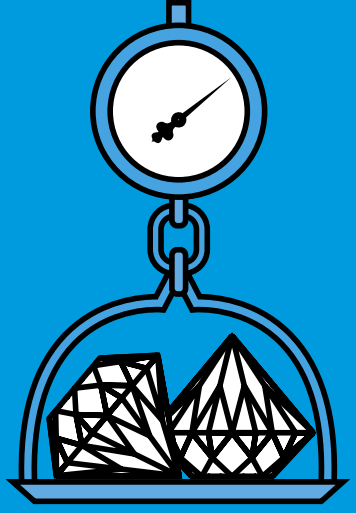
The same tools that help organizations identify their crown jewels can also help find documents that no longer have any value and should be deleted. Valuable information should be stored under lock and key, while the junk should be tossed out.

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



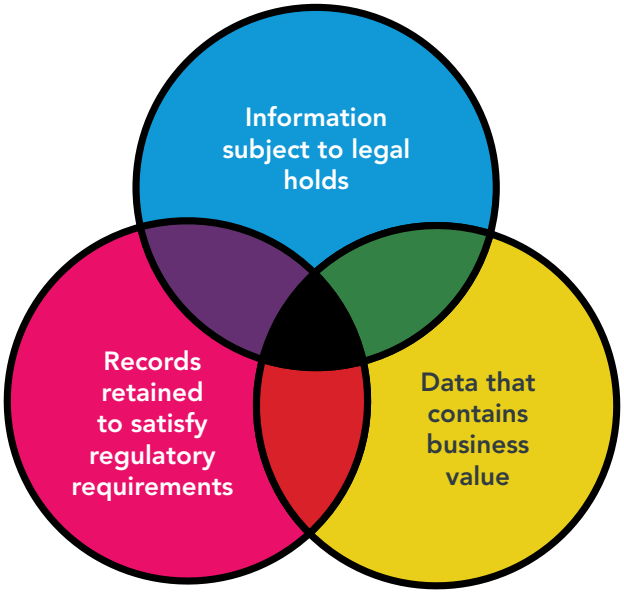
[2] "The Best Way to Use Data to Cut Costs? Delete It" CIO Insight, August 17, 2015. http://www.cioinsight.com/it-strategy/big-data/slideshows/the-best-way-to-use-data-to-cut-costs-delete-it.html

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.



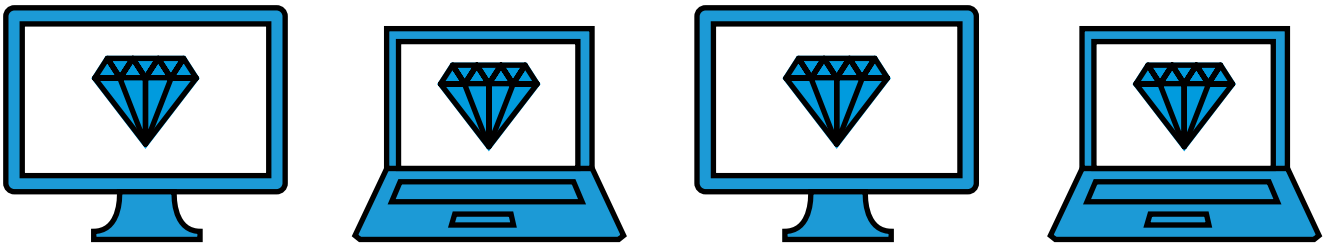
Generally, three different groups within companies should identify the information: the legal department, the records management group and the businesspeople. But it's not necessary to form another committee and bring representatives from each group together to review every potential piece of data. Instead, 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.

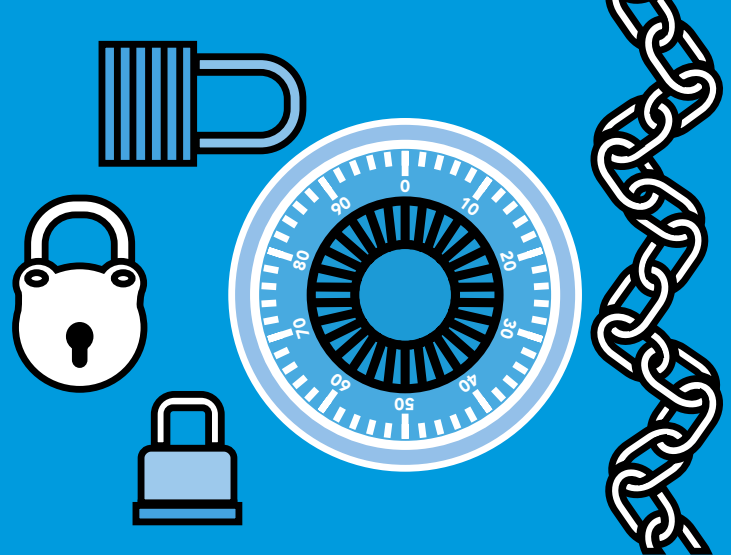
One thing to keep in mind: important information is often kept together. Just as you may have all your jewelry in a single drawer at home, your customer lists may all be in the same electronic file on a drive shared by the marketing department.

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.

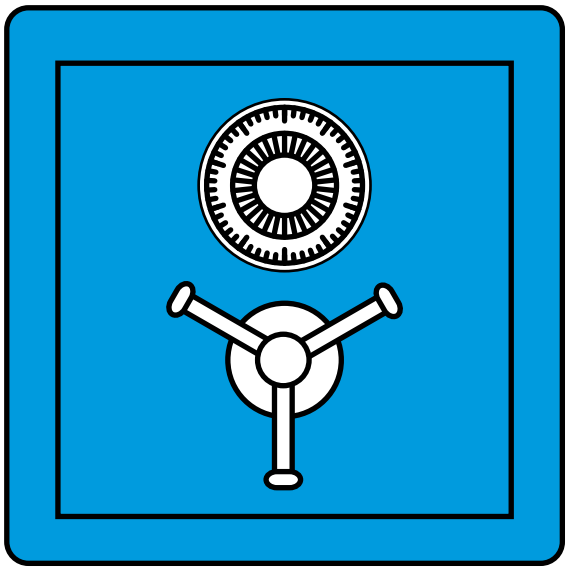
When considering the process for securing critical information, organizations should look for tools that protect against threats like hackers, but they also need to figure out how to safeguard data from those inside the organization.

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.

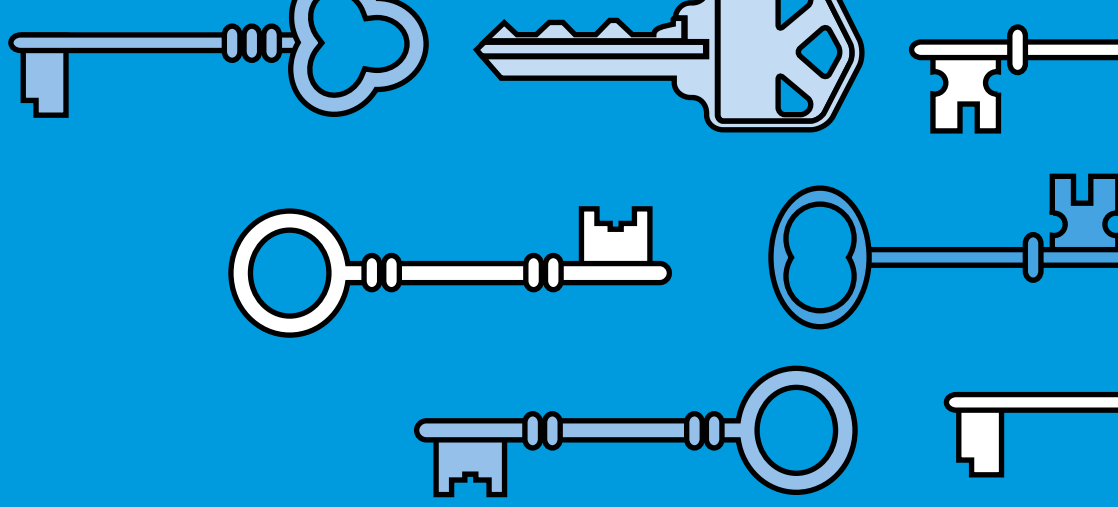


Creating Repeatable Processes Across Locations

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 a 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 is the chair of the CGOC. 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.

The Keys to Better Access Control Systems

A common mistake, says one cyber-risk professional, is to believe you can design a control for every type of system breach

By Edith Orenstein

Access controls used to be easy: just lock the door, filing cabinet, or safe. Anyone who wanted to break in needed to steal the key and pick the lock, or force his way in.

Those days are gone. And anyone trying to recreate a control environment akin to the simplicity that existed before the Internet is deluding himself.

"In today's open world, it's very easy to attack people and systems," says Andrew Morrison, principal in Deloitte's cyber-risk practice. "The Internet created the ability to share information, and trying to lock it down is kind of at odds with its goal."

A common fallacy, Morrison says, is to believe you can design a control for every type of hack. Cyber-controls are less like securing an office or filing cabinet, he says, and more like protecting against a flood: water is all around, searching for the path of least resistance. He cites three areas worth a compliance or audit executive's attention:

- Designing preventative controls to keep your data as secure as possible;
- Knowing what "normal" looks like in your systems, and be vigilant against anomalies;
- Building a system resilient enough to restore operations quickly after an attack happens.

Morrison recommends cyber-drills, where companies run through an attack that tests how someone can get in, how to detect, and how to respond—"just as you would operate for an earthquake at corporate headquarters."

One of the biggest problems in practice, Morrison says, is underweighting internal threats versus external threats. "There's been a lot of focus around keeping the bad guys from coming in, but it's almost been done at the expense of understanding and monitoring who is in the organization already," he says. "The failure in all these breaches typically comes down to a human with compromised credentials, or working in collusion with others."

A Balancing Act

Granted, the concept of access controls has been floating around the compliance and audit community—and in guidance such as the COSO framework for internal control, among others—for decades. What's changed, says Johnny Lee, forensic, investigative, and dispute services practice leader at Grant Thornton, is a shift away from individual access to network access.

And while best practices to protect network access might be clear, companies sometimes decide their budgets don't allow for best practice anyway. The result is the need for a balancing act in responding to risk, and judgment comes into play.

Lee

"Unless we have a discussion about the specific residual risks we allow to survive, such as how long a time period between reviews for breaches," Lee cautions, "if someone wreaks havoc on your network, that may become the balancing act between risk and performance."

Each model for access control (say, decentralized or single sign-on to IT systems), has its own challenges and monitoring issues, Lee says. First, is the sheer volume of access logs to review. Second, context is crucial.

"If you see an access that in isolation seems sinister or inappropriate, and you don't have the benefit of [knowing] that user's access to other systems, you might spend a lot of time chasing false positives," Lee says. The auditor needs to understand how systems interact with each other.

> "In today's open world, it's very easy to attack people and systems. The internet created the ability to share information, and trying to lock it down is kind of at odds with its goal."
>
> Andrew Morrison, Principal - Cyber-Risk Practice, Deloitte

Lee also warns about another risk not always disclosed to auditors that he politely calls the "care and feeding of server logging," which can be so resource-intensive that IT departments neglect it.

The problem is symbolic of many in IT controls. Users call the IT department to complain about system performance ("Why does it take four minutes to log onto e-mail?" Lee quips), so IT workers disable logging rather than let it slow down server efficiency.

An IT security no-no? Absolutely, but it happens. Lee encourages regular and candid discussions among internal audit, IT, and compliance to identify those problems with IT infrastructure and management. He also recommends that IT audits avoid a "gotcha" approach, which will probably cause the IT department to stop returning your calls.

Another common mistake, Lee says, is to assume that the control is the log itself—the control is the review of the log, and everyone involved should understand exactly what the log captures (name, date, time, device used, and so forth).

One of the biggest problems, says Lee, is revoking access rights that are no longer proper; such as when someone leaves the company, or moves to a different position or department. The more senior the executive, the more rights and access he or she likely had. That makes revoking rights all the more urgent, as well as periodic reviews of who has access to what.

> "If you see an access that in isolation seems sinister or inappropriate, and you don't have the benefit of knowing that user's access to other systems, you might spend a lot of time chasing false positives."
>
> Johnny Lee, Forensic, Investigative, and Dispute Services Leader, Grant Thornton

Understanding Business Is Key

Brian Barnier, a risk adviser with ISACA and principal at Value Bridge Advisers, says access control is like a "chain of fitness," with steps ranging from a control being used as intended to a control passing robust stress tests. If one of the links fails, the access control gate can be disabled.

As discussed in Barnier's ISACA Now blog post Why Didn't the Dog Bark?, another cause of control failure is when "the auditor or compliance person fails to bark because all looks well—because he or she does not understand the chain of fitness and other assumptions. There is a false sense of security."

"If they don't understand how the business works, all bets are off," Barnier adds. "You can build a tool, but the tool can fail, and if you just add new tools, you can be replacing one failure with another failure."

Barnier, who authored ISACA's Operational Risk Handbook for Financial Companies, has reviewed FBI files on financial crimes and sees a classic security problem: someone with knowledge of front-, middle-, and back-office operations is able to cover up his tracks. That is an instance where certain access should have been turned off and more segregation of duties should have been in place within the organization.

Morrison adds that behavioral considerations are critical in determining what access, even when properly authenticated, is appropriate. For example, a doctor reviewing files of patients he is treating would be normal; looking at sequential patient files would not. "Typical controls don't do that type of behavior monitoring, which is becoming more and more important," Morrison says. Controls would include pattern analysis and behavioral analysis, and running correlations.

"Are hackers going to get better? Yes," Barnier says. In applying longstanding literature infused with new knowledge, it appears that effective access controls rely heavily on communication and education. ■

CONTROL CHAIN OF FITNESS

Below Brian Barnier of ISACA outlines nine steps companies should implement toward better access controls:

1. The control is used as intended
2. The control is maintained as implemented
3. The control is implemented as designed
4. The control is designed from the appropriate template
5. The control is appropriate for the process class and problem
6. The control is located properly in the process flow
7. The control is based on the location of useful warning signs
8. The control is based on robust, real-world "What if?" scenario analysis
9. The control is based on scenario analysis conducted properly based on a thorough "know the business" understanding of environment and capabilities

Though still challenging, these assumptions are easier to meet when applied to retrospective financial reporting, when those reporting systems are stable and a threshold of materiality (percent of revenue or income) can be applied. These assumptions are more difficult to meet when a prospective view is needed of a dynamic, operational world, where a tiny issue can turn into a huge problem.

The second cause for controls churn and confusion is when the auditor or compliance person fails to bark because all looks well—because he or she does not understand the chain of fitness and other assumptions. There is a false sense of security.

Why do some auditors miss these problems? In speaking at ISACA programs around the world, show-of-hands surveys reveal that it has much to do with the time a person began working in audit. In particular, whether a person's work experience begins before the Sarbanes–Oxley Act of 2002, when IT audit began focusing on a narrow financial reporting notion of "IT General Controls" (ITGC).

The modern, skilled IT pro has a clear operational view of a control as something that senses and responds, whether dumb like a light switch or intelligent like server load balancing.

ISACA's COBIT 5 offers help in the shift from "controls" (too often understood mostly as ITGC) to business-objective-oriented management practices. More broadly, consider ISACA's tagline: "Trust in, and value from, information systems." Value creation in Val IT (now incorporated in COBIT 5) is well beyond controls that struggle just to protect value.

I suggest taking action—host a "Cut Controls Churn and Confusion Day" at your chapter or for your team at work. Invite a panel of people with managerial accounting, operational process improvement and IT process improvement experience to discuss why improved oversight, management practice and core business process are more effective than controls for any operational situation.

Source: Brian Barnier, Risk Advisor, ISACA.

Hurry-Up Offense on Employee Surveillance

Reeling from the financial crisis and the LIBOR scandal, JPMorgan among financial services firms to improve sales & trading practices

By Jaclyn Jaeger

Employee surveillance is one of the most sensitive—and yet, rapidly evolving—areas of compliance for financial services firms today. Initially a response to regulatory pressure, surveillance obligations are now becoming an integral part of a robust internal control system.

That does not mean those obligations are easy to fulfill.

Monitoring employee activities to detect and prevent illegal conduct—fraudulent trading, benchmark rate manipulation, or any other offense—is not a new concept per se, especially for large financial institutions. Both the Securities and Exchange Commission and the Financial Industry Regulatory Authority, for example, have long required banks to monitor their employees' personal trades. Traditionally, however, the data generated by such surveillance activities has been done in a manual, cumbersome, and often siloed fashion. That approach left significant gaps in oversight.

Taking harsh lessons learned from the financial crisis, and still reeling from the billions of dollars in fines resulting from the LIBOR scandal, financial services firms now want ways to monitor employee activity actively, rather than responding to regulatory demands. "They're no longer just complying with regulations," says Jake Frazier, senior managing director at FTI Consulting. "They want to take it to the next level."

JPMorgan's Corporate & Investment Bank (CIB), for example, said it launched a comprehensive review last year to analyze and make improvements to its sales and trading practices and related communications. "We recognized that enhancing market conduct would require using multiple preventive and detective levers in a coordinated way," the bank stated in a report to shareholders. That review considered various means to:

- Establish information barriers;
- Conduct communications and transaction surveillance;
- Adopt policies;
- Implement training; and
- Incorporate enhanced supervision, compensation, and disclosure practices.

JPMORGAN SALES, TRADING PROCESSES

Below is an excerpt from JPMorgan's "How We Do Business" report, describing its revised sales and trading practices.

We recognized that enhancing market conduct would require using multiple preventive and detective levers in a coordinated way. For example, the review took into consideration various means to establish information barriers; conduct communications and transaction surveillance; adopt policies; implement training; and incorporate enhanced supervision, compensation and disclosure practices.

In the first phase of the review, the business enhanced information barriers by implementing new policies around electronic chat and launched an effort to increase and improve communications guidelines and surveillance of chat and email. In the second phase, we are carrying out a review of information flows in the markets businesses, further refining electronic chat guidelines, continuing enhancement of surveillance and prioritizing other issues for review.

The project seeks to identify certain per se prohibited communications and set forth principles governing permitted communications—including information to be shared on a need-to-know basis and only for legitimate business purposes, such as trade execution or clarification of operational details. Our efforts over the past year include:

- **Establishing a Steering Committee to develop a global governance framework.** The committee is charged with setting policy and standards and creating an operating model to support a global communications surveillance program. The committee also is integrating current pilot projects and identifying technology options that support enhancements and a target-state vision
- **Expanding current electronic surveillance.** The CIB has added Compliance surveillance employees globally through the second and third quarters of 2014
- **Moving to a more sophisticated predictive technology for surveillance** by participating in a pilot assessment expected to be completed by mid-2015
- **Continuing to engage in discussions with existing vendors** around current and future availability of enhanced tools to monitor chat room participation

Additionally, in December 2013, the CIB implemented a policy that prohibits staff from participating in electronic chats or instant messaging groups with two or more other banks/dealers. The prohibition applies to communications with third-party trading desks that are competitors or market-makers, as well as brokers or inter-dealer brokers.

Source: JPMorgan.

"In the first phase of the review, the business enhanced information barriers by implementing new policies around electronic chat and launched an effort to increase and improve communications guidelines and surveillance of chat and e-mail," JPMorgan said. "In the second phase, we are carrying out a review of information flows in the markets businesses, further refining electronic chat guidelines, continuing enhancement of surveillance, and prioritizing other issues for review."

JPMorgan added that the project "seeks to identify certain per se prohibited communications and set forth principles governing permitted communications, including information to be shared on a need-to-know basis and only for legitimate business purposes, such as trade execution or clarification of operational details."

Financial services firms are realizing they can "better protect their employees and their brand by having more clearly defined policies and exceptions to those policies," says Scott Rister, vice president of compliance solutions at Charles Schwab. For example, some firms historically have allowed employees to maintain personal investment accounts anywhere they wanted, as long as the firm could get a paper statement at least quarterly. Now they're refining those policies, requiring employees to use broker-dealers who provide an electronic data feed, so that the firm has better access to real-time information—usually next day—and can analyze it in a more efficient manner, he says.

> "Financial services firms are realizing they can better protect their employees and their brand by having more clearly defined policies and exceptions to those policies."
>
> Scott Rister, VP of Compliance Solutions, Charles Schwab

Another approach that many banks have developed as part of their surveillance programs is a "hub and spoke type of model," Frazier says. Under that model, a compliance committee, or even a group of compliance liaisons, serve as the central hub, disseminating relevant information down to the business units, he says.

JPMorgan, for example, established a steering committee, tasked with developing a global governance framework. "The committee is charged with setting policy and standards and creating an operating model to support a global communications surveillance program," the bank said.

Advanced Analytics

As the industry has evolved, and as technology has evolved, financial services firms now also have the ability to gain greater insight into potential illegal conduct across various business units, and at speeds once inconceivable. Although regulations still drive most employee surveillance activities, "most financial institutions are much more proactive in how they monitor, meaning they are looking to leverage technology to get more timely access to information and better identify potential issues," Rister says.

Newer surveillance technologies, for example, employ analytics that use not just structured data—such as trading activity—but also unstructured data generated by e-mails, text messages, phone conversations, and social media. The goal of marrying together structured and unstructured data is "to find patterns that wouldn't otherwise pop up for an investigator or an auditor if they were looking exclusively at one of those two silos," says Joram Borenstein, vice president of marketing at NICE Actimize.

Many banks today also are implementing audio communication surveillance capabilities, which employ a real-time phonetic index of telephone conversations, much in the same way that a keyword search can analyze electronic communications. "For example, if a broker says on the phone, 'I guarantee you five times your money back on this investment,' then the phonetic indexing will catch that," Frazier says. Historically, such information may not have been captured until an investigation ensued, he says.

Companies now can also overlay this data with information from other departments such as HR records and financial records. The overall intent is to look at employees' personal behaviors in the context of their IT behaviors, to see whether there is a heightened risk, or a shift in behavior, that suggests something needs to be investigated, says Greg Henderson, government healthcare director in the security intelligence global practice of SAS. If an employee suddenly is taking a lot of vacations and traveling to suspect foreign destinations during a time when his IT activity is also suspect, those factors together might be a red flag to the company that the person needs to be investigated further.

With today's advances in technology, even small firms are now able to implement a system that meets their needs, as more vendors offer monitor capabilities that can be scaled to the size of the firm. "That's definitely made it easier for firms of all sizes to conduct surveillance in a more cost-effective and expedient manner," says Amy Lynch, founder of FrontLine Compliance, a financial services consulting firm.

For financial services firms still developing their employee surveillance and monitoring activities, Borenstein says compliance officers shouldn't simply rely on whatever regulatory framework they're required to comply with—whether that's Dodd-Frank, the Sarbanes-Oxley Act, or any other regulation. "They shouldn't take a check-the-box approach," he says. Instead, they should satisfy those regulations as a minimum standard, and then take a step back and ask where else their institution might have risks that the regulatory framework might not completely cover. ■

Ideas for Compliance, Audit & Cyber-Security

CW Editor Matt Kelly offers some advice: Worry more about how information is governed; define roles for how cyber-security is managed; study the SOX, cyber-security bond

By Matt Kelly

Nobody can get enough guidance about cyber-security these days, and the New England Chief Audit Executives group is no exception. I attended the group's winter meeting here in Boston, and that's all we talked about for two solid hours. These folks had good ideas galore about managing cyber-security risk, so let me recap the most important ones here.

First, worry more about the process of how information is governed at your business than about the tools you use to protect it. The discussion started with a panel of audit and IT executives, and every one of them agreed on this point. Tools address one specific risk, and they may do that quite well—but they may also be useless for every other risk. And if your process for governing information is sloppy overall, those other risks will hit you eventually. The tools you have won't do you much good then.

I always favor analogies from the real world, so try this one: at some point in life you might suffer a heart attack. You can go through life equipped with tools to reduce that risk, such as a defibrillator, and it will indeed help when the time comes. Or you can improve your process of being healthy: eating right and exercising. Neither one of those procedures will assure that you never have a heart attack—but they will help you immensely in staying alive should a heart attack come to pass.


Kelly

Good tools without good process is the equivalent of carrying around a defibrillator while you overdose on salty foods and sit on the couch all day. Does that sound like a good strategy for preventing heart attacks to you?

Second, define the roles for managing cyber-security risk at your business. Nobody at the CAE group specifically mentioned the Three Lines of Defense model, but that's my default for any conversation about who oversees what part of a risk. In that case, the internal auditors have things a bit easy: you're in the third line as usual, testing the security procedures and controls like you would any other.

The first and second lines of defense get more complicated. Clearly IT (or the IT security function, if you have a separate one) belongs in the second line. Compliance does too. But each one supports the business units bravely holding down the first line of defense in different ways. My first point above, to worry more about process than tools, still holds true—but you do need both tools and process to have effective cyber-security: IT supporting the tools to fight cyber-security risks, compliance supporting the processes.

I like to think of effective cyber-security defense as this: for business units to follow effective processes there in the first line, compliance needs to do its job in the second line defining what those processes are. They might be policies to have third parties certify their data security, or procedures for swift disclosure of a data breach. But the business units can't follow a good process unless compliance does its job spelling out the policies and procedures that govern that process.

The third point I heard, and perhaps the most heartening one, was that Corporate America has faced a mess of poor controls and poor understanding of risk before—and we solved the problem. We've been here before with Sarbanes-Oxley compliance.

Numerous times I heard speakers worry about weak processes and then breezily add, "unless it's a SOX process, because our SOX processes are generally strong," or "If it's a SOX-related control usually we're confident it works."

> Good tools without good process is the equivalent of carrying around a defibrillator while you overdose on salty foods and sit on the couch all day. Does that sound like a good strategy for preventing heart attacks to you?

Study those parallels between SOX compliance and cyber-security, because they are deep and vital. A huge amount of cyber-security risk hinges on access: ensuring that only authorized users get access to certain types of data. That is the same worry compliance and internal auditors have about access control to financial information—and you've been testing your access controls for financial data for the better part of a decade. Drop the word 'financial' from my last sentence, and you have your marching orders for cyber-security risk. I'm not saying that goal is easy to achieve, but that's the goal.

You can even make an intellectual leap from SOX compliance back to the importance of a strong process. When you read through the 17 guiding principles of the updated COSO framework—the framework we're all using for SOX compliance—those principles are all about strengthening your process. Everyone might be using the framework right now for internal control over financial reporting, but COSO intended the framework to be a roadmap for internal control over other risks too, cyber-security included.

So as scary as cyber-security might be right now, it can be conquered. If the compliance and audit community tamed Sarbanes-Oxley, you're in prime fighting shape for this threat too. ■

Compliance's Role in Data Privacy Controls

Continued from Page 6

cussed the state of privacy protection measures in France and throughout Europe. CNIL is an independent regulatory body that oversees the application of privacy law to the collection, storage, and use of personal data. It is comprised of 17 members from various government entities in France, including four from its parliament.

In January 2014, CNIL issued a ruling that Google's privacy policy did not comply with French data protection laws and issued a fine of €150,000. More recently, CNIL was behind a September "cookie sweep," a series of not-so-surprise company audits to assess compliance with French and European Union rules requiring websites to obtain user consent before installing cookies, those tiny bits of data that get popped onto your hard drive every time you visit certain websites. Users must also have the ability to know how cookies are used and to opt-out of the data collection.

Nerbonne updated the audience on the status of long-delayed EU-wide personal data protection legislation. Negotiations will soon restart on a new law that would consolidate the data protection regulations of individual EU member nations. An ongoing point of contention among business leaders is that the new law may demand breach notifications within 24 hours of an infiltration, without any safe harbor for data encryption.

Other measures likely to be included in the legislation are the right to portability of personal information, the "right to be forgotten," requiring a project- and product-based Privacy Impact Assessment; and fines €100 million or 5 percent of global turnover for companies that transmits personal data outside the EU without a customer's permission. "A lot of work has been done and there are just a few points to clarify," Nerbonne said. "We are still hoping that by the end of the first part of next year it will be done and then it will take two years to put the new regulation into application."

"The challenge with the U.S. Health Insurance Portability and Accountability Act and other standards are that, on one hand, they are flexible and agnostic in terms of technology," Tabuena said. "On the downside: They are flexible. They don't really give you a lot of specifics on what it means to be secure and what is a reasonable control. That is where I am going to need to rely on the IT and information security experts to help me out."

Their assistance, and the help of the legal department, can help map out what threats exist and the priority status that should be placed on them. "It's a lot of work, but you have to start somewhere," Tabuena said. "You have to put together a country-by-country, state-by-state matrix of all the breach rules, including how they define sensitive information." ■

Is Your Data Governance Function Mature?

Continued from Page 7

functions often operate in isolation. Information governance needs a leader who can coordinate, call the shots, and drive governance across all information facets in an organization.

» Balancing risk and value. Information is a business asset, creating both risks and value. The CIGO must find the right balance between the risk and value.

Current IG Projects

The IGI report also said many companies have multiple information governance projects underway. Sixty-nine percent identified updating policies and procedures as one project they are undertaking, followed by scanning paper documents (50 percent), and data consolidation and clean-up (47 percent) as their second- and third- most common projects.

Other common projects include the migration of unstructured information from one system to another (46 percent); defensible deletion (42 percent); and decommissioning an archive or system (40 percent).

"Data mapping is a foundational element in the information governance process," Robinson says. "It is necessary to start with a base understanding of what and where data exists." Only after that happens can you start to leverage all that day, either for regulatory requirements or for business intelligence purposes.

On a practical level, Robinson says, some IG projects might entail:

» Identifying critical assets that require a higher level of protection from cyber-risk;

» Identifying information that may have been compromised in a breach; and

» Identifying redundant, trivial, and obsolete information, and disposing of that data to reduce e-discovery costs, supporting more effective management of information.

Getting an IG project off the ground can take a significant amount of time. According to the IGI report, the plurality (35 percent) of practitioners said it takes longer than a year to get an information governance project started. Another 22 percent said it takes at least a year, while 16 percent said six months. Only 10 percent said three months or less.

The average number of information governance projects that companies are taking on vary greatly by size. Companies that have 10,000 or more employees are working on an average of seven information governance projects at once, spending an average of $777,000. On the lowest end, companies with up to 1,000 employees are undertaking up to four projects at once, spending an average of $186,000. ■

Magic wand not required.

Too many information governance projects begin with unreal expectations and end in disappointment.
FTI Technology provides practical information governance with tangible benefits, including reduced risk and cost.

Reality-based information governance.
Learn more at www.ftitechnology.com

FTI™ CONSULTING | TECHNOLOGY