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.

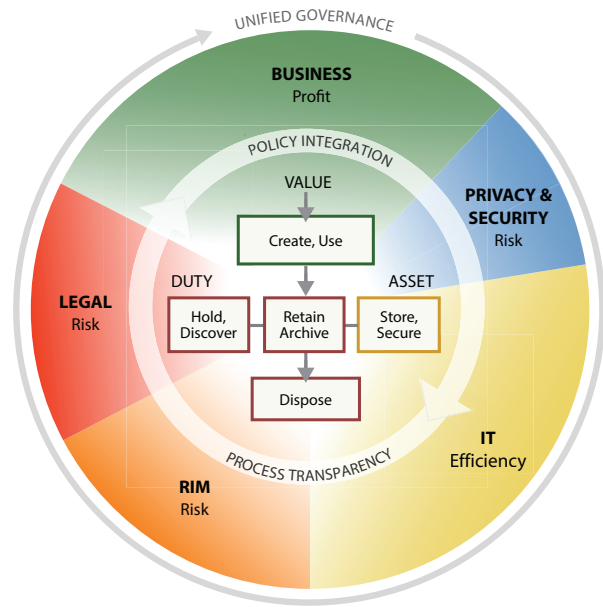
Similarly, every organization has a set of crown jewels—information that is critical, unique or irreplaceable. And much like at home, the most difficult part of protecting them is not actually the repository, it is determining what information qualifies for this type of protection, and finding it, and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

[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

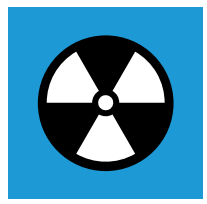
to be handled carefully, so that none of the metadata is altered. If no one at the organization knows what data exists and where it is, companies can easily find themselves with "dark data pools." This can include decades-old paper files or microfiche that are in storage.

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]

[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

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.

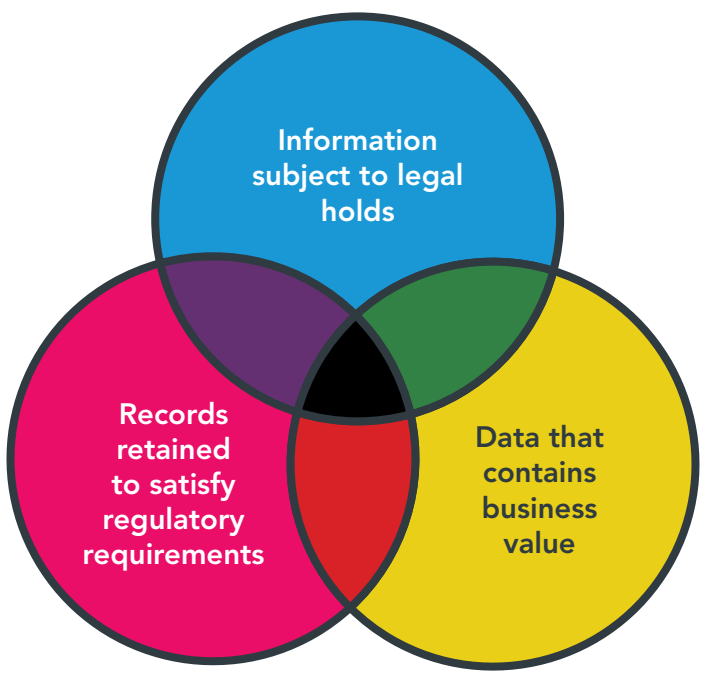
The same tools that help organizations identify their crown jewels can also help find documents that no longer have any value and should be deleted. Valuable information should be stored under lock and key, while the junk should be tossed out.

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.



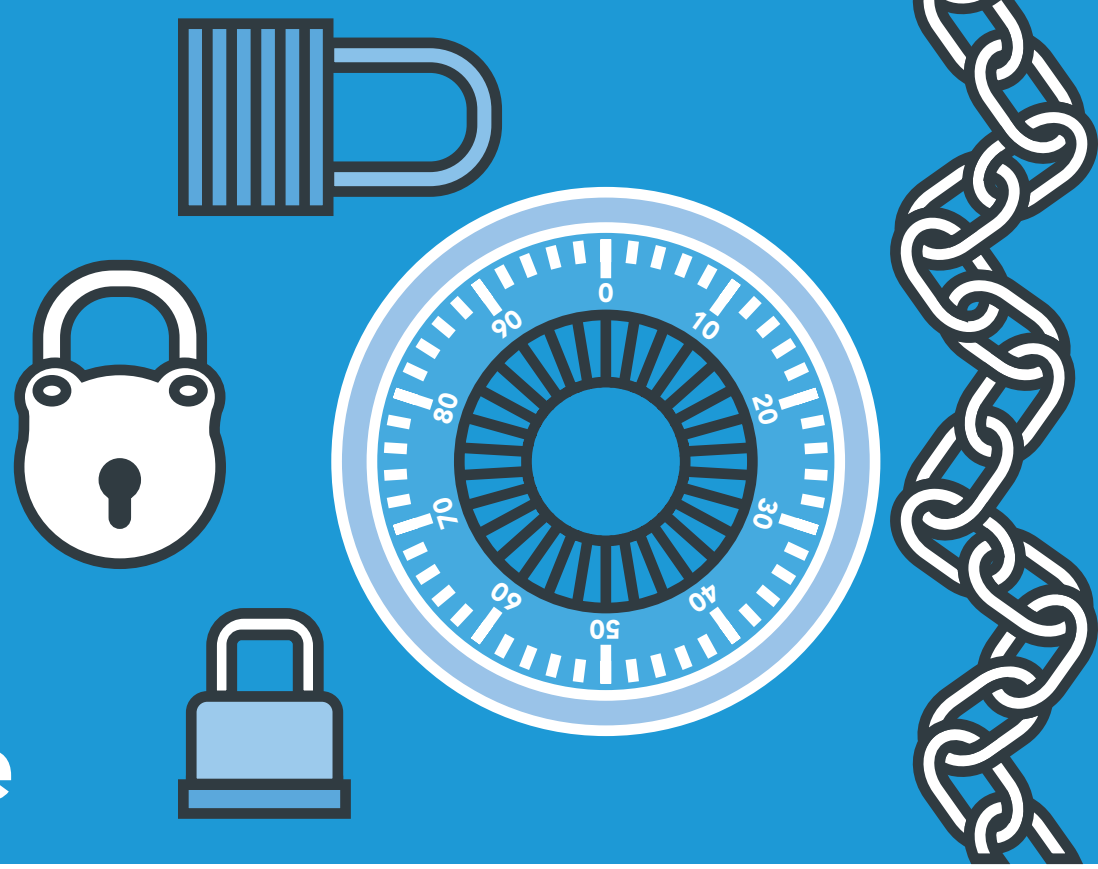
Generally, three different groups within companies should identify the information: the legal department, the records management group and the businesspeople. But it's not necessary to form another committee and bring representatives from each group together to review every potential piece of data. Instead,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

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.

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.



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.

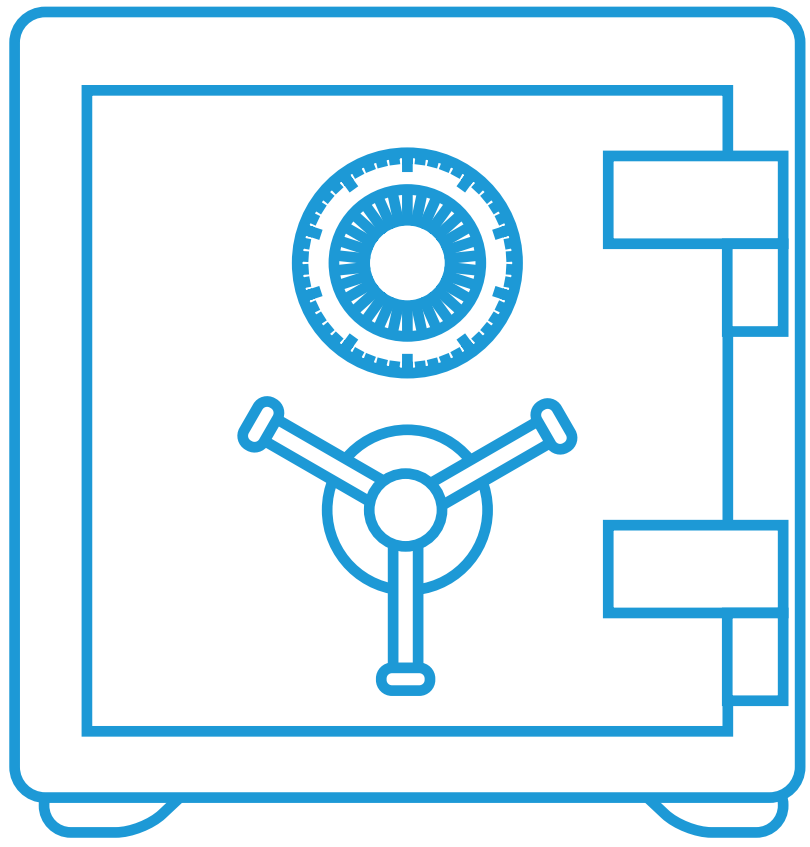
When considering the process for securing critical information, organizations should look for tools that protect against threats like hackers, but they also need to figure out how to safeguard data from those inside the organization.

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.



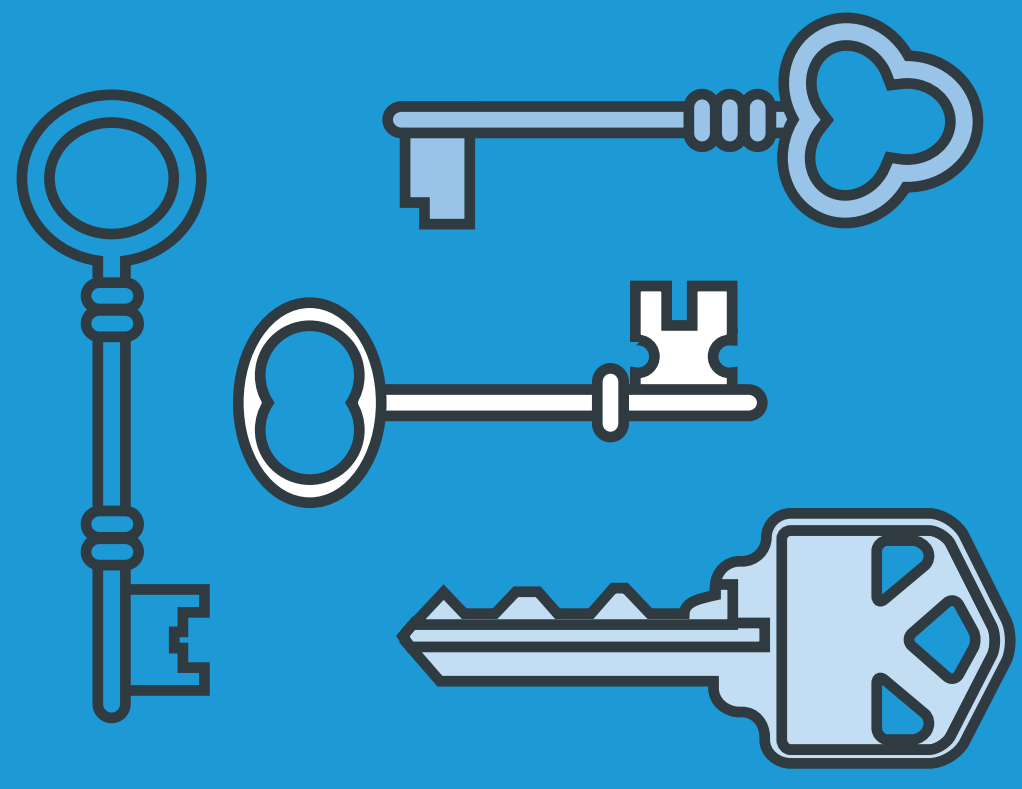
Creating Repeatable Processes Across Locations

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 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.