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

Technology, Privacy, and eCommerce

CHEAT SHEET

- ***Spring cleaning.*** By prioritizing the most valuable data, in-house counsel can compartmentalize cybersecurity initiatives into smaller and more focused objectives.
- ***Checking your ethics.*** It is the ethical responsibility of in-house counsel to prevent data breaches through the consistent maintenance of electronically stored information (ESI).
- ***Protecting your valuables.*** Once you have defined which data to target, specific protections must be put in place, including the encryption of sensitive documents and ensuring the privacy of email servers.
- ***Achieving quick success.*** In-house counsel should work collaboratively to avoid wasted time and money, and think about the importance of the end-goal when attempting to make unnecessary shortcuts.

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 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 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 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 below), 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.

“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.

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 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.

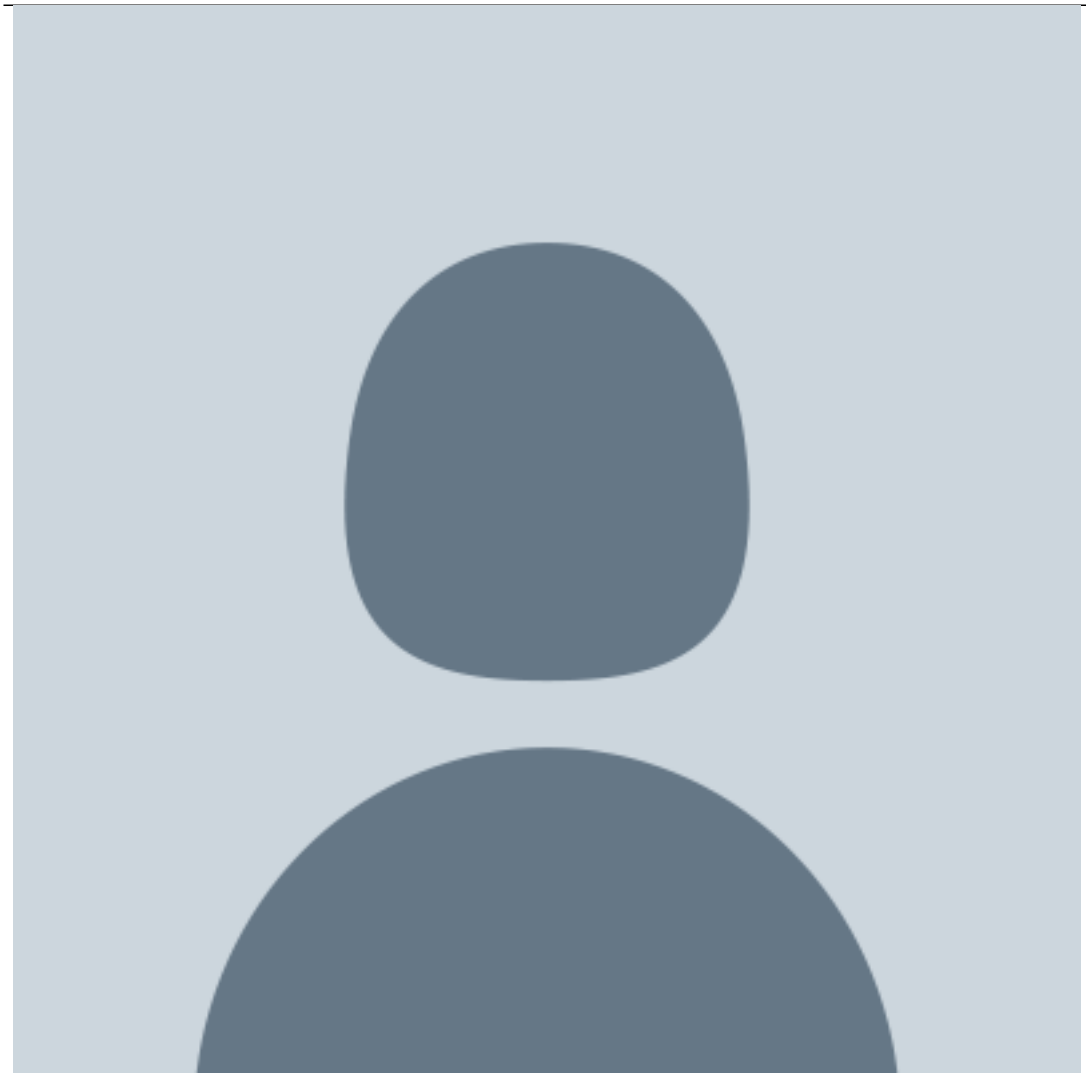
- **Don't forget about data privacy regulations.** "Beware of all of the international data privacy regulations and their amendments. You must understand that transferring data across borders is a very sensitive issue, even when the company has operations abroad."
- **Get outside help.** For those in 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.

Jennie McQuade



Chief Privacy Officer and Chief Legal Counsel

Swisslog Healthcare

Swisslog Healthcare is 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.

Jake Frazier

Senior Managing Director

FTI Consulting, based in Houston, TX

He heads the information governance and compliance practice in the technology segment. Frazier assists legal, records, IT, and information security departments identify, develop, evaluate, and implement in-house e-discovery and information governance processes, programs, and solutions.