LJN LAW JOURNAL NEWSLETTERS

Cybersecurity LAW & STRATEGY®

An ALM Publication

October 2016

Data Breach Prevention and Information Governance Go Hand-In-Hand

Information governance has a wide range of varying definitions, depending on whom you ask. Some consider it to be an amorphous collection of policies that are difficult to translate into the real world. Others view it as a holistic strategy document, or a series of discrete, tactical projects that implement best practices in data security or storage optimization.

By Jake Frazier

Information governance (IG) has a wide range of varying definitions, depending on whom you ask. Some consider it to be an amorphous collection of policies that are difficult to translate into the real world. Others view it as a holistic strategy document, or a series of discrete, tactical projects that implement best practices in data security or storage optimization.

Organizations struggle with the notion of information governance for a variety of reasons. Some lack the executive support necessary to get programs off the ground, while others feel hampered from executing on small, tactical projects due to their legal or regulatory profile. Equally confusing is the purpose of IG 'whether it is intended to reduce storage costs, improve e-discovery or impact corporate risk and security.

When executed well, IG can accomplish all of these things and more. But one of its most meaningful results is the differentiation of data types and stronger security protocols around a corporation's most sensitive data. Because not all enterprise data is created equal, different data requires differing levels of protection. As we've learned from the long list of publicized data breaches, there is an increasing need for companies to get smarter about locating, organizing and securing their truly sensitive data.

For the vast majority of organizations, progress on this front is gradual. This was illustrated in a recent study of in-house lawyers, examining the health and success of IG programs within Fortune 1000 corporations, which found that most are in the early stages of IG adoption. In the study, data security was the top recurring theme across responses when participants were asked about IG drivers within their organization. And while 76% of respondents confirmed they have IG programs within their organization, there were more than 30 areas of focus listed.

Regarding data security efforts, many corporate teams agree that initiatives can be parsed into four key areas: 1) securing sensitive personally identifiable information for clients, patients and employees; 2) securing sensitive company intellectual property; 3) creating a tiered security network to protect against security breaches; and 4) developing protocols and systems to ensure secure access to the network for partners and other approved third parties. Addressing each of these buckets with focused projects helps protect the organization's data from internal and external threats and makes it easier to tackle the seemingly insurmountable task of arming the company against a data breach.

Common Roadblocks

It is first helpful to understand the top challenges teams face when working toward IG programs.

Work Styles and New Technology

For many companies, the main challenge is that employees are working and collaborating in new ways that are enabled by the proliferation of cloud-based applications. In the study mentioned above, nearly a third of respondents indicated this as a roadblock, and cited that the wide variety of collaborative tools and mobile devices combined with the lack of employee awareness to sensitive information has made the prospect of controlling where data is shared increasingly complicated. Employee conduct comes into play with this issue, and the lack of control points to the need for processes and training that would help prevent employees from making poor information management decisions.

Jake Frazier is a senior managing director at FTI Consulting, based in Houston. A member of our Board of Editors, he heads the information governance and compliance practice'in the technology segment. 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. Frazier is a founding member of the Electronic Discovery Reference Model and is also a member of the Sedona Conference.

Identifying a Starting Point

Organizational structure is often mentioned as a barrier because various parts of a company are responsible for different elements of information governance. Because IG involvement ranges from legal and IT to risk, records management and security, corporations find it daunting to prioritize which areas need attention first. If the scope of the project is too huge, it can and will fall under the weight of itself.

Big Data

There are countless software systems 'both legacy and new' and many needs for information stored in many different places and ways, making cohesive IG difficult. Further, organizations are trying to manage rapidly evolving data ecosystems that span personal computers, mobile devices, social media and myriad cloud-based collaboration tools. Legacy data is difficult to store and retrieve, but may still be relevant for existing legal hold or other uses. This, combined with increasing data volumes and BYOD (bring your own device) work environments, produces a level of disorganized complexity that causes confusion and security risk.

Human and Financial Capital

In the study mentioned above, 25% of respondents noted lack of resources as a key challenge for IG. For some, it was a matter of mere headcount to get the job done. Many worried about the fact that IG is an initiative that should include collaboration across teams within various functions, from IT and records management to legal and the lines of business. This fact, combined with difficulty in securing buy-in from key stakeholders, can hinder an IG initiative from the start. For the handful of companies with resources solely dedicated to IG, the average number of staff is four, and budgets ranged from $200,000 to $20 million among the companies that were able to quantify their IG spend. Most companies do have at least one in-house person handling IG, but these roles typically span a range of other areas as well.

Tips for Success and Added Benefits

Overcoming the challenges outlined above is realistic, and many corporations are seeing success. Following the key principle of "don't let perfect be the enemy of good," will guide teams toward a step-by-step approach that focuses on the basics. By basing programs on key business requirements, projects will be more likely to come to completion and have tangible results. Additional tips for successfully getting IG off the ground include:

- **Secure executive buy-in.** With a champion at the top level, teams will be able to secure approval for the time and money required to implement the project.
- **Bring in the experts.** Particularly for companies in highly regulated industries, it is important to work with professionals that understand IG and the many legal and regulatory factors that apply. Outside counsel and other third-party providers that have experience with these issues will ensure that solutions are tailored to the corporation's unique needs.
- **Develop cross-functional teams.** Making sure key stakeholders from across departments are on the same page will go a long way in avoiding duplicated efforts and wasted resources.
- **Empower the end users.** As much as data usage must be governed and restricted, it is important to provide employees with tools that make it easy for them to comply with company policies. Without this, many people will take shortcuts that bypass protocols and ultimately make poor judgment that can expose sensitive information.
- **Beware of international factors.** Multi-national corporations need to be highly aware of data privacy regulations and their impact to moving data across borders. This is a very sensitive issue, and is best addressed when IG programs are customized and executed individually for each jurisdiction. [Editor's Note: As an example, *see*, "China's Second Draft Cybersecurity Law's Expanded Data Localization Requirement," in this issue.]
- **Look at the big picture.** Without allowing a project to become overwhelmingly large or complex, it is important for IG teams to take a step back and look at the big picture. Projects must have focused goals and outcomes, but they should all play into a holistic strategy that addresses broad company needs.

Ultimately, IG programs can help corporations identify their most at-risk datasets, reduce them compliantly and add security protocols to protect against a data breach. The benefits of these efforts are far reaching, although can be difficult to quantify. Beyond avoidance of severe financial implications brought on by a data breach, corporations that get it right achieve reputational savings and keep their brand image intact. Additionally, IG initiatives often involve internal education and awareness, which helps employees understand the company's security responsibilities and goals, and their role in maintaining sound IG.

While many describe their IG programs as nascent, with broad policies still in the works, focused, tactical projects are offering benefits. Among these are reduced storage costs resulting from maintaining data deletion practices and improved e-discovery processes. Streamlined legal hold and information collection and reduced data sets are common outcomes of IG work, and can significantly improve e-discovery efficiency.

Conclusion

In total, information governance is still a relatively new concept, and while it poses a number of challenges 'spanning technology, processes and culture' it is providing early adopters with some key advantages. By understanding the basic mechanics, corporations can better outline programs that make sense given their needs and regulatory profiles. With the risks of today, and the commonality of cyber attacks, security should be at the heart of all IG projects. Identifying and mitigating sensitive data repositories are only effective if a company is then ready to do what it takes to protect that key information.

—❖—