FEATURE

Building Bridges With the Board—Innovation in Information Governance

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

https://bit.ly/2E5daDU

IT professionals and enterprise board members live in two very different worlds. Boards worry about strategic concerns such as revenue, share price and brand reputation, whereas IT staff are paid to deal with operational challenges such as those stemming from big data, cyberthreat actors and cloud usage. Bridging the gap between these strategic priorities and day-to-day concerns to initiate an organization's technological transformation can seem insurmountable.

In any enterprise transformational program, people, processes and technology are key ingredients to long-term success. Information governance (IG), which is an operational approach to managing the valuation, creation, storage, use, archival and deletion of data within an organization, is no exception. Proactive IG requires collaboration among legal, compliance, security and IT teams to take an incremental, measurable approach to deal with today's enterprise data challenges. Such cross-functional collaboration almost invariably requires an executive or board-level mandate. Often, however, absent fines, litigation and/or regulatory scrutiny, IG is not sponsored at the board or executive level. What can stakeholders in an IG program do to obtain the level of executive or board sponsorship necessary to ensure success?

In one recent client engagement, consultants helped legal counsel get a seat at the table and engage top enterprise leadership in establishing IG to mitigate risk around impending litigation. Conversely, consultants have also worked to help clients restart projects that have stalled due to competing demands within a cross-department project team.

T. Sean Kelly
Is a senior director within FTI Technology's Information Governance, Privacy and Security practice. He advises clients on all aspects of e-discovery and information governance, with a particular focus on developing and implementing legal-hold processes and technology and the legal impacts of migrating data to the cloud. He leverages more than a decade of experience in both legal technology and litigation support to advise clients on evolving technologies and the shifting landscape associated with cross-border transactions for global enterprises. Kelly previously worked for Johnson & Johnson, where he was responsible for e-discovery issues across business sectors, advising internal stakeholders and outside counsel on best practices in collection, forensic technology, document review and controlling cost.

Traversing the Gap

Failure to handle data properly often results in damaging data breaches, which have been estimated by the Ponemon Institute to cost US $3.62 million on average.[1] Beyond this and legal/compliance violations, breaches break trust and cause reputational damage. The key to obtaining C-level and/or board involvement in an IG initiative is to position its benefits as specifically addressing risk and brand reputation, rather than as operational improvements.

An organization's risk framework to prioritize its highest risk, such as regulatory/sanctions or reputational damage, can help an IG team evaluate which risk categories an IG program will impact, and make a cost-effective business case for it. Some of today's most pressing data risk scenarios include:

- **Big data**—Organizations have deployed numerous software systems—legacy and new—with data stored in many different places and ways. The Leading Edge Forum *Data rEvolution* study predicts that by 2020, 100,000 organizations will store one or more petabytes of data.[2] Organizations are managing rapidly evolving and heterogeneous data ecosystems spanning personal computers, mobile devices, social media

and a myriad of cloud-based collaboration tools, often with little insight into how information is created or managed. The proliferation of this dark data creates a level of disorganized complexity, causing confusion, security risk and increased costs for finding data when litigation, regulatory or investigatory mandates arise.

- **GDPR and privacy**—The European Union General Data Protection Regulation (GDPR) will impact many facets of business for multinational corporations. The GDPR requires organizations based in the European Union and those that retain personal data of EU citizens—including any information related to an individual, such as physical address, email address, Internet Protocol (IP) addresses, age, gender, global positioning system (GPS) location, health information, search queries and items purchased—to meet stringent data protection requirements. Many organizations that freely harvest and commercialize this information today will be required to bear the cost and risk of these requirements. Failure to comply can lead to fines of up to 4 percent of a company's global annual revenue or EU €20 million. Because the regulation is so expansive and new, just knowing where to begin is challenging.

  Included in the GDPR is an erasure, or right-to-be-forgotten provision, that gives EU citizens the option to require their PII to be erased from an organization's databases and other systems and made inaccessible to others seeking that information. Legal and IT teams must understand possible interpretations of this and other data-subject rights in the GDPR and be equipped to communicate the implications of noncompliance to the board.

- **Cybersecurity**—Data security is now an enterprisewide endeavor and a major concern for boards and top executives. Globally, there are dozens of laws that regulate how corporations manage cybersecurity and what they must do in the event of a data breach. Cybersecurity events seen over the past year demonstrate how extensive the damage of a global attack can be. Attacks and ransomware will continue to hit private and government networks around the globe, and threat actors will continue their increasingly sophisticated cyberaggression. As cybersecurity threats and regulations evolve, it is important for organizations to manage cyberrisk holistically, mapping out programs for addressing the unique challenges in each region where the organization does business. An IG program set up to protect valuable business information and the timely disposal of noncritical information contributes to the strong cybersecurity posture mandated by today's enterprise boards and executive leadership.

> "IMPLEMENTATION OF CLOUD SERVICES INTRODUCES A VARIETY OF IG-RELATED RISK FACTORS RELATED TO EMAIL ARCHIVING, DATA PRESERVATION, CROSS-BORDER REGULATIONS, DATA SECURITY AND E-DISCOVERY PROCESSES."

- **Legal hold, e-discovery and compliance**—Legal hold is another area where poor execution can lead to significant financial and legal risk, but which can be addressed by proactive IG. This process requires close monitoring to ensure its defensibility and to guard against possible spoliation charges in litigation, which can come with steep penalties. It can be difficult for organizations to scope the correct individuals who need to be under legal hold and limit preservation to only those individuals. Legal teams are critical

Enjoying this article?

- Read *Innovation in Information Governance—Getting Started with Data Governance Using COBIT® 5. www.isaca.org/data-governance-COBIT-5*
- Learn more about, discuss and collaborate on governance of enterprise IT in the Knowledge Center. *www.isaca.org/governance-of-enterprise-it*

to informing leadership which regulations are applicable to the organization's specific industry and regions of operations. Managing e-discovery burden and cost continues to be a pain point for many large organizations. A strong IG program can significantly reduce e-discovery and legal-hold cost and risk by reducing the amount of data subject to discovery and by making the process for finding, preserving and producing relevant data more efficient and less subject to manual error.

- **Digital transformation**—Many organizations are undertaking digital transformation efforts involving migrating data to the cloud. Microsoft Office 365 alone has more than one million monthly commercial users, and Microsoft indicates adoption is growing rapidly.[3] Implementation of cloud services introduces a variety of IG-related risk factors related to email archiving, data preservation, cross-border regulations, data security and e-discovery processes. The movement of critical enterprise data to the cloud raises security and data protection concerns, and studies have shown the incidence of advanced email threats rising for organizations of all sizes.[4] For all these reasons, cloud migration and other digital transformation efforts aimed at business process optimization and improving cost efficiency should be viewed as critical initiatives.

One Step at a Time

IG is often thought about in the context of IT efficiency, data security and regulatory compliance. While it is true that these are the most critical drivers for executing data and information governance programs, the equally important factor of brand reputation deeply resonates with an organization's board and C-suite. Projects may be driven by a variety of internal sponsors, all bringing varying needs and goals to the table. The chief financial officer (CFO) or finance department may be looking to reduce year-over-year spending by remediating data and increasing storage efficiency. The IT department cares most about mitigating the costs of big data and ensuring that the organization does not suffer from network overload. The legal team is focused on e-discovery, ensuring legal-hold compliance and fulfillment of regulatory requirements. Understanding and leveraging these various drivers can help gain executive sponsorship for the project and make it easier to bring a group of stakeholders together to tackle the implementation.

With cross-functional support, stakeholders can demonstrate how specific IG initiatives can directly reduce reputational and other key risk and gain support from the board. Projects that can help ensure safe and responsible handling of sensitive data, strong compliance and business process efficiency include:

> "WITH CROSS-FUNCTIONAL SUPPORT, STAKEHOLDERS CAN DEMONSTRATE HOW SPECIFIC IG INITIATIVES CAN DIRECTLY REDUCE REPUTATIONAL AND OTHER KEY RISK AND GAIN SUPPORT FROM THE BOARD."

- **Eliminating legacy data and adjusting policy**—Remediate legacy storage by refreshing backups, disposing of redundant backup tapes and establishing an enforceable archiving policy. To remediate legacy back-up tapes, legal and compliance teams must collaborate with IT to take inventory of and address any regulatory and legal-hold obligations on the data. This process can also be a forcing function to standardize legal-hold policies, potentially saving significant long-term storage and e-discovery costs.
- **Bringing unstructured data under control**—Most organizations store unstructured data that include confidential data or PII that may be subject to privacy laws. Taking the time to scan file shares for sensitive data, identify critical information, and get it under lock and key can help mitigate the risk of loss of intellectual property and trade secrets, and the operational and reputation risk involved with managing a data breach.
- **Modernizing message archiving**—Email archives are one of the most undermaintained systems within an organization, and most archives are built on aged technology that desperately needs to be

updated or evaluated for defensible disposition. New archiving technology can provide built-in IG controls and a much better experience for running searches and extracting data for e-discovery or other reasons, as well as for end-user management of email. Features include preset retention policies and the ability to identify sensitive information that is being sent outside the organization so it can be stopped before it leaves the network. An archive modernization initiative provides a good opportunity to show value with IG.

- **Using cloud migration as an opportunity**—Migration to cloud systems provides an opportunity for an organization to take stock of its email and data management practices and potentially update policies and remediate data for greater efficiency and security. Cloud solutions do introduce new IG concerns, including expanded individual storage and retention challenges, but there is also better ability to search and manage the data and significantly reduce storage costs.
- **Moving beyond first-generation e-discovery**—With the broad awareness most organizations and law firms have today around e-discovery, a surprising number of them are still using first-generation tools for search and retrieval. There are a handful of organizations on the forefront of emerging technology, but most still use basic bulk collection from email archives as their primary process for e-discovery. Further, most first-generation tools have trouble with e-discovery from other unstructured data sources such as SharePoint and cloud-based repositories. Collaborative platforms often contain information critical to a case, and the scope of e-discovery has gone well beyond email and traditional electronically stored information (ESI), frequently calling for desktop, file share, and other structured and unstructured data sources. Updating e-discovery processes and technology can enable the legal team to deal with matters that are on their desks today and provide tools to build toward stronger IG.
- **Leveraging analytics/machine learning**—Advanced technology has emerged that can accelerate IG remediation and support in investigations and litigation. Legal and IT teams are just scratching the surface for advanced analytics and machine learning tools that can be applied to advance IG initiatives. These technologies can be useful in taking large amounts of data and classifying them in an efficient way, reducing manual effort and cost.

Measuring Success

For a long time, boards have overlooked the inherent risk living within the organization's data. The combination of new privacy laws and the increasingly aggressive nature of cyberthreat actors is changing all that. Top enterprise leadership must start paying attention to these issues to maintain baseline security and compliance. Proactive IG can be an important component to effectively address these challenges and provide other tangible and sustainable benefits.

"IG ENABLES TEAMS TO MORE EFFICIENTLY CONDUCT A DETAILED ANALYSIS OF SECURITY WEAKNESSES AND GAPS, AND PROACTIVELY MONITOR LOCATIONS WHERE CRITICAL DATA ARE LOCATED AND LOSS IS LIKELY TO OCCUR."

There is a significant reduction in cost and an increase in efficiency of e-discovery processes when an organization's data have been properly organized and remediated as part of an IG program. With disorganized, unmanaged enterprise data environments, e-discovery teams have difficulty viewing and managing data across dozens of different file servers, Skype, email, Dropbox and other data sources. Remediated data environments also make it easier to search and identify PII and other sensitive data such as credit card information and government identification numbers, helping to meet privacy obligations and take necessary remediation steps such as securing, encrypting and/or deleting sensitive data. IG enables teams to more efficiently conduct a detailed analysis of security weaknesses and gaps, and proactively

monitor locations where critical data are located and loss is likely to occur. This makes it possible to put protections in place, as well as reconcile remediation with steps to preserve data required for compliance or legal-hold purposes.

While data issues can be overwhelming, teams must remember that they do not need (nor should they try) to boil the ocean. Instead, data remediation projects can be prioritized by those that address the highest-risk areas or provide a quick-win to give momentum. One way to help prioritize might be to break down IG goals into categories:

- Protecting the sensitive information of customers and employees
- Securing sensitive company intellectual property
- Arming against cybersecurity threats
- Developing protocols and systems to ensure secure access to the network by partners and approved third parties

These or similar subcategories within a broader IG program can help take a large challenge and channel it into initiatives that are more focused, easier to accomplish and supported by the board.

Endnotes

1 IBM, "Cost of Data Breach Study," June 2017, *https://www.ibm.com/security/data-breach*
2 Koff, W.; P. Gustafson; "Data rEvolution," The Leading Edge Forum, USA, 2011, *http://assets1.csc.com/innovation/downloads/LEF_2011Data_rEvolution.pdf*
3 Bright, P.; "Microsoft 1Q18: Office 365 is Booming, Azure Continues to Climb," *Ars Technica*, 26 October 2017, *https://arstechnica.com/information-technology/2017/10/microsoft-1q18-office-365-is-booming-azure-continues-to-climb/*
4 Neely, L.; "Exploits at the Endpoint: SANS 2016 Threat Landscape Survey," SANS Institute InfoSec Reading Room, September 2016, *https://www.sans.org/reading-room/whitepapers/analyst/exploits-endpoint-2016-threat-landscape-survey-37157*