MAYER·BROWN

ELECTRONIC DISCOVERY & INFORMATION GOVERNANCE

Tip of the Month

Implementing An Information Governance Program

Scenario

The IT department of a retail company implements email account volume limits in attempt to control growing data proliferation. In response, employees in the data analytics department begin using off-system cloud storage options to store their data. The cloud storage company announces that there has been a data breach exposing data stored in their cloud to hackers. Some of the company's stored information was included in the breach, including names, addresses and credit card information of customers. The massive breach severely damages the company's reputation among customers and shareholders and requires considerable resources to resolve.

The Problem: Data and Information Silos that Focus on Departmental, rather than Enterprise, Goals

Many organizations utilize multiple (four or more) records management systems. Departments like IT, HR, and Legal often have different record keeping policies and procedures based on department goals rather than organization-wide goals. This siloed approach can lead to higher costs and risks, security breaches, inefficiency and decreased compliance. Common examples of this silo approach include:

- Individual business departments making independent decisions about information technology tools, resulting in technology duplication and extra costs;
- An IT department imposing email account volume limits, leading users to save files on local drives or media, creating data security risks and difficulties in preserving emails for litigation;
- Personnel conducting business on their own laptops and smart phones without sufficient policies and controls to keep data secure and properly retain records;
- Records departments instituting a comprehensive data and email retention program, without regard to technological limitations or costs.

The Solution: Information Governance Policies and Procedures to Enforce Record Management, Privacy Standards, and Storage Optimization

"Information governance" (IG) is a set of multi-disciplinary structures, policies, procedures, processes and controls implemented to manage information at an enterprise level. IG supports an organization's current and future regulatory, legal, risk, environmental and operational requirements. It encompasses more than traditional records management by incorporating privacy

attributes, electronic discovery requirements, storage optimization and metadata management.

Although data generation and retention has expanded in recent years, few organizations have developed IG policies and procedures to keep up with it. With storage costs consuming nearly 20 percent of a typical IT budget, and enterprise data continuing to grow, the lack of a company-wide policy and commitment to IG may expose companies to unnecessary risks of data leaks, security breaches, litigation costs, loss of intellectual property and reputation damage.

Organizations can minimize these risks and costs and may gain business advantages by implementing an enterprise-wide IG program. An IG program's primary goal is typically to create and maintain processes and procedures that enable a coordinated, overall approach to decisions about information. When disagreements arise between stakeholders, the program should provide a decision-making method to resolve conflict. A focus on transparency, efficiency, integrity, accountability and compliance are keys to enabling the program to function effectively and withstand such conflicts.

Best Practices for IG Programs

Below are some suggested best practices for organizations considering implementing or maintaining an IG program:

Independence from other departments: Consider making the IG program and decision maker independent from any one department to encourage decision-making that prioritizes the entire organization's needs. Where possible, the decision maker should be provided with the requisite resources and authority to attempt to obtain organization-wide buy-in and compliance.

Stakeholder input: While the independence of the decision-making body and program is important, the interests of all stakeholders should be represented, including IT, legal, compliance, risk, audit, records and information management, operations and critical business units. An initial step in designing an effective IG program is to collect information from all key stakeholders about their current practices regarding records and information management, privacy and data security, and litigation preservation. Next, the organization should consider reconciling any differing practices with a goal to implement, if possible, one legally compliant, comprehensive program. Finally, a program that is regularly monitored can respond more quickly as the organization's objectives and its stakeholders' needs evolve.

Structure, direction, resources and accountability: If possible, an IG program should have structure, direction, resources and accountability. This can include direction provided to users through policies, contracts, protocols and training. Many organizations already have multiple policies governing information management, including computer use, information security, legal hold and electronic discovery. Consider reviewing such policies to eliminate conflicts and inconsistencies. Sufficient resources for an IG program can include appropriate personnel, technology and budget to support the program. Finally, accountability measures can include support from senior leadership, program objectives and regular compliance audits to evaluate if program expectations are met.

Using new technologies: Organizations can consider optimizing their IG programs through the use of emerging technologies. These technologies can make it easier to access information for e-discovery, compliance and open records laws, and increase business intelligence. For example, machine learning tools like predictive analytics can enable machines to learn what information may be relevant to an organization. Tools that auto-categorize content can help implement an IG policy by taking the burden (and risk of error) off the end user. These tools can eliminate the need for an end user to manually identify records, and can provide automatic identification,

classification, retrieval, archival and disposal capabilities for electronic business records. These emerging technologies may also function as an early warning system to predict and prevent wrongful or negligent conduct that might lead to data breach or loss. Each new technology has its merits and risks and should be considered individually for each organization.

Periodically reviewing and updating the IG program: Organizations and environments change, so the IG program should be revised to reflect these changes as soon as administratively possible. An organization should consider periodically reviewing and updating the program, analyzing whether its rules and risk controls remain appropriate as the organization faces changed circumstances and challenges.

Conclusion

Information Governance is more than records management, as it attempts to provide a coordinated, interdisciplinary approach to managing the information needs of an organization. Where possible, Information Governance should involve a top-down, overarching framework, informed by the information needs of a company's stakeholders, with a target of helping the organization to make decisions about information for the good of the overall organization and consistent with its strategic goals.

For inquiries related to this Tip of the Month, please contact Anthony J. Diana at adiana@mayerbrown.com, Kim A. Leffert at kleffert@mayerbrown.com or Dominique-Chantale Alepin at dalepin@mayerbrown.com.

Learn more about Mayer Brown's Electronic Discovery & Information Governance practice or contact Anthony J. Diana at adiana@mayerbrown.com, Eric B. Evans at eevans@mayerbrown, Michael E. Lackey at mlackey@mayerbrown.com or Edmund Sautter at esautter@mayerbrown.com.

Please visit us at www.mayerbrown.com.