Five Steps In-house Counsel Should Take to

Mitigate Information Risk

H. Kirke Snyder, J.D., IGP

In-house counsel need to collaborate with key information governance stakeholders to help resolve their sometimes-conflicting information management goals and ensure that the IG program has the executive support and resources needed for the organization to achieve its core mission while preventing or mitigating risks.

Because of the risks associated with electronically stored information (ESI), organizations need a strategic information governance (IG) framework that addresses records and information management (RIM), data privacy and security, and e-discovery. If senior management fails to provide the framework, each department's perspectives will drive its data management goals. Their differing perspectives, though, can drive conflicting data management goals and can complicate or circumvent the organization's ability to govern its information effectively.

Perspectives That Produce Conflicting Goals

For example, the RIM perspective is driven by the records retention schedule, so one of its data management goals is to ensure that information is kept as long as – but no longer than – needed to meet legal/regulatory, fiscal, historical, and operational requirements. But, IT's perspective is driven by the need to manage storage costs, so it may establish e-mail account volume limitations that lead to e-mail records being disposed of before their retention requirements have been met, in conflict with RIM's goals.

The legal department perspective is driven by the need to avoid judicial sanctions for spoliation, so it may issue broad legal holds that cause information that is not relevant to litigation or regulatory actions to be retained longer than it should be, in conflict with both RIM and IT's goals.

Finally, business units, which are focused on data accessibility and convenience, may utilize third-party cloud data storage applications that put the organization's information outside of the organization's control, where it may not be secure and cannot be managed properly – in direct conflict with RIM, legal, and IT goals.

This is why effective IG requires senior management to collaborate with key stakeholders, hear all perspectives, gain an understanding of how the organization should best manage its information to achieve its core mission while preventing or mitigating risks, and to enlist executive support for appropriate people and financial resources.

The chief legal counsel has a critical role to play in this. Because the American Bar Association's Model Rule 1.1 requires lawyers to provide "competent" representation to clients – in this case their employing organization – in-house counsel can't afford to assume that IT and RIM personnel will get all the legal intricacies right, given the potential legal and financial risks of unmanaged information. The insights and practical advice offered below could help legal counsel save their organizations millions in fees and expenses.

Trends That Stem from Flawed IG

Flawed IG is causing three disturbing trends that carry significant legal and financial risk to corporate America, and in-house lawyers should not be sitting on the sidelines waiting for their number to be called.

Growing Number of Data Breaches

The first trend is the theft of ESI. Data breaches occur virtually every day (e.g., Sony, Target Corp., Home Depot, JPMorgan Chase), with significant reputational and financial costs for organizations. According to the 2015 "Cost of Data Breach Study: Global Analysis" conducted by Ponemon Institute and commissioned by IBM, the average cost of a data breach incident was $3.8 million.

Rising Cost of E-Discovery

The second trend is the rising cost of e-discovery, which directly affects an organization's law department budget. The 2012 report "Where the Money Goes: Understanding Litigant Expenditures for Producing Electronic Discovery" by the Rand Corporation found that U.S. corporations typically spend at least 70% of their litigation budgets on document review.

Exploding Volume of E-Records

Part of the reason document review takes so much of the budget is that it's common for lawyers to sift through documents and e-mail produced for discovery multiple times. But this cost could and should be much lower, as the vast majority of e-mail and documents collected, preserved, and reviewed is typically obsolete and should have been destroyed during the normal course of business in accordance with the organization's records retention schedule.

Even when organizations have a formal written records retention policy and retention schedules, they may not be fully implemented and are rarely audited, which may be due to lack of executive support for the RIM program to be sufficiently staffed or funded.

5 Steps That Will Mitigate Information Risk

While lawyers may hesitate to get involved in helping resolve the issue of ungoverned information because they don't feel trained or empowered to do so, they must roll up their sleeves and step in – pre-litigation discovery. Once a data breach has occurred or a legal hold of information that should have been destroyed is in place, in-house counsel will have to be involved, but at that point it's too late to save the organization from its poor housekeeping. Here are five actions they can take.

1. Role Play a Rule 30(b)(6) Deposition

Rule 30(b)(6) of the Federal Rules of Civil Procedure (FRCP) and the corresponding state rules require an organization faced with e-discovery to designate officers, directors, managing agents, or other persons to testify under oath as to matters known or reasonably available to the organization (e.g., information management and document retention). These 30(b)(6) depositions can be a nightmare for the unprepared.

Don't wait for the onset of litigation; identify the individuals who will be designated to testify for a deposition and play the role of a plaintiff lawyer by asking typical Rule 30(b)(6) questions about document management systems, information management policies and procedures, and the data deletion process. This exercise will help prepare the "deposed" individuals and reveal a more accurate picture of any RIM vulnerabilities.

Counsel may find that many record types are not destroyed according to policy and schedule, and that multiple copies of "records" are stored in the basement, offsite, on the shared network, in the e-mail application, within SharePoint sites, and on third-party cloud systems.

2. Challenge IT to Create a Data Map

Under the FRCP, parties must cooperate to reveal everything about their ESI, including location, type, source, and format. In addition, litigators must come to the FRCP Rule 26 "Meet and Confer" with an understanding of the nature, variety, and kinds of electronic storage media involved; how to retrieve data; the types of electronic data; the format in which the electronic data is stored; and the expense of collecting and preserving the data. In effect, these requirements are tantamount to requiring the parties to produce a data map of their potentially relevant information.

Without specialized technology, an IT department can exhaust significant resources creating a data map for a single litigation. The map must consider listing the core records from important production systems and applica-

tions, along with data stored in the cloud, data from the computers of individual employees, data from applications that are no longer in use, and even the contents of CD-ROMs and backup tapes.

Don't wait for litigation to prompt learning about the ability of IT and RIM to create a litigation data map. As with the mock 30(b)(6) depositions, give the IT department a date range, a list of key employees, a description of topics and key words, a specific deadline, and an evaluation of its work product. This preparation is not "busy work." It will save the organization 10 times the investment.

To cost-effectively manage its data assets (both proactively and in response to a legal action), the organization must have the technology to easily identify, copy, move, protect, and destroy ESI throughout the enterprise.

3. Convince Senior Management of Resource Needs

Armed with insights acquired from the mock Rule 30(b)(6) deposition and the data map exercise, counsel can begin convincing senior management that a legally defensible RIM program is not optional. Senior management must understand that the improved RIM program may require new computer hardware, software, and training. Specialized technology tools will help lock down records in a safe place and identify files with personal data for encryption or destruction.

Too often, the RIM and IT departments lack the budget to acquire the very tools that could save the organization millions by mitigating the likelihood of a data breach or litigation e-discovery. To cost-effectively manage its data assets (both proactively and in response to a legal action), the organization must have the technology to easily identify, copy, move, protect, and destroy ESI throughout the enterprise.

One such tool is *storage resource management* software that "crawls" the storage objects to collect and store information about those objects in an informational database. The database could be searchable by metadata only (e.g., file type, creation date, size) or by the metadata and the full text of every stored file within the enterprise.

Such applications typically come from vendors selling information security, litigation e-discovery, or network storage management applications. These applications can:

- Identify documents with personal information for deletion or encryption
- Identify documents or e-mail with key words or concepts
- Determine the age of the documents or e-mail (by the date created, received, or last edited)
- Act upon a group of selected files (e.g., copy, move, delete)
- Discover the department (or employee within the department) that created or owns the data
- Identify duplicate or near-duplicate documents and move the final record copy to a secure location

Enterprise records management software provides manual or systematic storage and retrieval of documents and e-mail with record value. It makes records widely available at any location as a searchable repository for shared knowledge, compliance, and litigation support. Such a central records repository for the important documents will allow IT to apply an automatic document deletion schedule to non-record (transitory) data stored on shared servers and e-mail. The records repository application will protect records from accidental deletion or modification and allow file-level audits, encryption, user access, and version control.

4. Revise the Records Retention Policy and Schedule

Many "for profit" business organizations in the United States have a records policy and retention schedule that are not enforced or audited. Many of the policies and schedules were written before the explosion of e-discovery, e-records, and e-mail. The modern records policy and retention schedule must be updated with an emphasis on identifying and storing electronic records. Consider modifications in the following areas.

Format. Based on the sheer volume of e-mail, documents, and other ESI being generated every day, the organization's policy must state that records will be maintained in electronic format only. The organization won't eliminate hard copy *documents*, but it will eliminate hard copy *records*. In the end, this key policy will also lower the cost of identifying, collecting, and reviewing materials related to e-discovery.

Storage Location. One of the greatest challenges will be to distinguish records from non-records if both are stored in the same application, drive, or folder. The new policy should specify that the official "record copy" of a document or e-mail will be stored within a centralized record repository application, not in Outlook or on a shared network drive.

Ownership. The new policy should specify who identifies the records. The legal department will know if a

particular document type should be saved only relative to its regulatory requirement. RIM won't know which of the various near-duplicates of a document is the official record copy. Only the business unit has the subject matter expertise to manage its own records. Therefore, the new policy should state that each business unit is responsible for its own records.

Legal should assist business unit leaders by providing a spreadsheet of minimum statutory and regulatory retention requirements for their own department's record categories. Each business unit leader should identify an experienced team member to help the organization's records manager finalize the department's records retention schedule.

Mandatory Audit. The last but most critical component to add to the new records retention policy is an audit imperative. The legal standard that will be used to judge the defensibility of the RIM program is "reasonableness." It is not reasonable to issue a legal hold notice and not follow up on it. The audit (or compliance) department will propose an audit schedule and methodology to ensure that records and non-record information are being maintained in accordance with the department's retention schedule. Ultimately, the audit process will document that the organization's RIM program is legally defensible.

In addition to revising the retention policy, the legal department must re-think the logistics of the retention schedule. Most schedules are confusing because they have too many "retention buckets." A schedule that counts on users to classify a document or e-mail based on a spreadsheet of hundreds of document types is doomed. The answer is to simplify the classification process.

For example, some documents and e-mail are important enough to be saved forever. With little training, users can typically identify this type of document. Most e-mail and documents can be deleted within a few months. With just one more bucket – say, one that specifies a 10-year retention – the simplified retention schedule would be easier to understand and easier to audit. Each department must train its own users with the retention rules and exceptions.

5. Modify Vendor Storage Contracts

Many organizations are utilizing a third-party file hosting service with cloud storage for file synchronization and data sharing. Cloud storage can be cost effective during the normal course of business, but it can create nightmares for RIM and the e-discovery process.

The legal department can directly reduce the risk by reviewing proposed or existing cloud contracts for red flags and asking a few pointed questions to identify the contracts for terms and conditions that need to be negotiated or renegotiated, such as the following:

- The right to use data and metadata
- Ownership of data and copyrights
- Physical location of stored data
- Changing of terms or assignments without consent

The legal standard that will be used to judge the defensibility of the RIM program is "reasonableness." It is not reasonable to issue a legal hold notice and not follow up on it.

- Notification of subpoenas
- Responsibility for e-discovery costs
- Destruction and auto-delete procedures
- Compliance and audit rights
- Data portability
- Procedures for security, business continuity, and disaster recovery

Counsel should ask about the nature of the data being stored in the cloud and the philosophy concerning its storage management. For example, ask if the documents are to be managed as *records* or are they considered *transitory data*, with the final record version to be transferred and managed within the in-house records repository application. Ask who will identify and preserve records as well as turn off any auto-delete function in case of a legal hold.

Involvement That Bucks the Trends

Organizations greatly benefit when inside counsel take an IG leadership role. First, by using common-sense litigation preparedness exercises to gain valuable insights into the strengths and weaknesses of the current IG processes and protocols, counsel will not only satisfy ABA Model Rule 1.1 that requires lawyers to provide "competent" representation, the organization will emerge with a data map and staff members that are prepared to be deposed about the RIM program.

Second, by advocating to the organization's executive leadership the importance of funding the required resources for IG, litigation e-discovery costs can be reduced or avoided because the volume of stored data will be diminished. **END**

H. Kirke Snyder, J.D., IGP, can be contacted at kirkesnyder@gmail.com. *See his bio on page 47.*