HUSCH BLACKWELL

May 2010

THE INFORMATION GOVERNANCE "C" CHANGE

Peter Sloan

Swamped by overflowing data and buffeted by e-discovery costs and information security requirements, companies are now compelled to make information management a priority of the first order. To regain control over their information assets and exposures, companies must harness convergence, connections, collaboration, and commitment... the "C" change for compliant information management.

OVERVIEW

Companies are awash in an ocean of data. E-mail servers are overflowing, troves of legacy data and documents are accumulating, rogue IT is proliferating, and social media and other Web 2.0 usage is seeping into the workplace. These same companies are also experiencing a sea change in their information compliance environment. E-discovery costs and exposures continue to mount, while courts' expectations are escalating for compliant preservation, collection, and production of ESI. And new laws and regulations are expanding the reach of information privacy and security requirements to a broader range of entities and business operations.

There is a ray of sunshine in this stormy weather — more than ever before, companies are now compelled to recognize that they are in the information business, and that managing their information is a business and compliance priority of the first order. Information must, and indeed can, be managed in a way that confronts the exposures above and also creates business efficiency and value.

But to regain control over their information assets and exposures, companies must harness convergence, connections, collaboration, and commitment... the "C" change for compliant information management.

CONVERGENCE

For some time now, various company functions have separately experienced their own data and informationrelated challenges. IT functions have struggled with the accumulation of e-mail and other unstructured data; addressed management excitement about "going paperless" or other trends; and battled the spread of rogue IT usage. More recently, IT functions are wrestling with the logistics involved with cloud computing, SharePoint and other collaborative browser-based environments, and enterprise content management initiatives. Often, IT feels compelled to proceed without clarity on applicable legal requirements. IT is also pulled into preservation and collection activities for litigation without thorough direction on compliance requirements for legal holds.

Meanwhile, the legal department has its own challenges. Expenditures related to e-discovery have skyrocketed. The annual Socha-Gelbmann Electronic Discovery Surveys report that total expenditures in the electronic discovery market exploded from $40 million in 1999 to $2.8 billion in 2007.[1] At the same time, an increasing number of law departments are exploring ways to manage these costs by bringing collection and processing activities in-house.[2]

The company's legal function is also closely monitoring court decisions establishing higher expectations for the preservation, collection, and production of electronically stored information in litigation. In her most recent e-discovery decision, Pension Committee of the University of Montreal Pension Plan v. Bank of America Securities, LLC,[3] U.S. District Judge Shira Sheindlin states "[a] failure to preserve evidence resulting in the loss or destruction of relevant information is surely negligent, and, depending on the circumstances, may be grossly negligent or willful."[4] For spoliation sanctions purposes, Judge Sheindlin characterizes the following lapses in preservation, collection, and ESI review as likely constituting gross negligence: the failure to issue a written legal hold notice and the failure to collect relevant paper or electronic records, or relevant e-mail, for key players to the litigation.[5]

Beyond the tens of thousands of statutory and regulatory requirements for records retention found at federal and state levels, legal and business functions now also face an expanding sweep of information privacy and security requirements. The 2009 HITECH Act's expansion of HIPAA privacy and security requirements to a broader circle of "business associates" extended the reach of regulated protection of individuals' health information.[6] Nearly every state has enacted breach disclosure requirements regarding personal information, and some states, most recently Massachusetts, have gone further by mandating information security programs for any company possessing protected personal information.[7]

The first principle, convergence, is the corporate realization that these are not unrelated issues separately affecting different functions of the company. Instead, these issues are converging into a single underlying matter, which is how the company manages its records and information.

Ignoring this convergence and addressing information management issues in isolation will invariably result in unintended consequences and exposures. Thus, the IT department's practices for disaster recovery back-up, or IT initiatives to relieve storage volumes for e-mail, will directly impact company expenses and exposures in e-discovery. The chief financial officer's response to a business unit's budget request for multi-purpose scanner/copiers may have huge repercussions on the company's legal compliance with regulatory requirements for records retention in digital media. And legal department action on contracts with third party information custodians may create information security exposures under privacy laws, while legal department expectations and assumptions about ESI preservation and collection may be out of sync with in-house IT capabilities. At the root of all of these siloed

issues, decisions, and initiatives is a common core: the company's approach to managing its information.

CONNECTIONS

Once the organization recognizes how seemingly unrelated matters converge into the foundational issue of information management, the next step is to make connections. This means connecting the dots so that the underlying information management issue surfaces and can be dealt with in a coordinated, strategic manner. Planning, decision-making, and initiatives should connect in ways that address the various aspects of information management compliance. For example:

- The company's records retention policy can be transformed into a records & information management policy, addressing not only traditional records retention points but also information governance matters such as information ownership; compliant use of company computer systems and devices that create or store information; information privacy and security compliance; company standards for media conversion; e-mail and other e-communication usage that results in data in the company's custody; and so forth. Such a policy should also explicitly dovetail with the company's legal hold process, which takes precedence within the scope of the preservation duty.

- The company's records retention schedule can extend beyond a classification of records into record series with associated retention periods to also provide a back bone of structural classification for records tied to privacy and data security requirements, as well as dovetailing with data mapping, which is of crucial value in both meeting information security requirements and executing preservation and collection in legal hold processes. The retention schedule's structure can also be calibrated to be most effectively useful in the ECM systems used by the company, so that records management decision-making by employees is as intuitive and efficient as practicable.

- Strategies for retaining e-mail and other e-communication data can dovetail with "record worthiness" decision-making under the company's records retention schedule, allowing record-quality e-mail to be retained consistent with the company's records retention schedule and non-record e-mail to be timely disposed of in ordinary course of business conditions, absent applicable preservation duties.

- Backup practices can be clarified such that archival storage needs are addressed elsewhere, allowing backup media to be kept in the ordinary course of business for the minimum period of time needed for disaster recovery, thereby appropriately and compliantly reducing the unnecessary accumulations of data backup that exacerbate privacy risks and that must be dealt with once an applicable preservation duty arises in litigation.

- Privacy and information security strategies that address encryption and access protection can also focus upon knowing where information is actually kept and compliantly disposing of information in the ordinary course of business as soon as is appropriate under the retention schedule. One cannot have an information security breach regarding information that has been effectively and compliantly disposed of. Prompt, compliant disposal has the additional benefit of reducing the data volume exposure in e-discovery that results from the need to preserve, collect, and process data that the company could have appropriately and defensibly disposed of earlier in the ordinary course of its business, before the preservation duty arose.

The above are merely examples of how companies that see the convergence of issues into the central matter of information

management can then connect their understanding of the issues, connect their fact finding, connect their identification of legal and business requirements, connect their problem solving, and ultimately connect their solutions to information management challenges. Ideally, such companies will develop a coordinated, strategic approach to managing their information assets, just as they already have for their financial assets, their physical assets, and their people assets. While a mature model for such coordination is labeled Information Governance, much headway can be made short of that sophistication by simply connecting the information-related issues and challenges, laying them out on the same table, and looking for connections of needs, requirements, and solutions.

COLLABORATION

Connecting assessment, decision-making, and response to information management challenges requires collaboration between company functions. Legal, IT, compliance, records management, and business units must reach out beyond their traditional turf. This means more than siloed decision-making that is then "run past" the other functions for approval. Instead, the various functions should be represented at the earliest stages of decisionmaking, when issues are identified and clarified and fact finding is done, all prior to identifying the legal compliance, technology, and business process requirements that support strategic decisions regarding information management.

While a formal Information Management Steering Committee or Information Governance Committee would fit well in the culture of some companies, forming such an interdisciplinary group is by itself neither required nor sufficient. What is needed are yet more "C"s: knowledgeable contacts connecting across functions, fostering consistent communication and developing and using a common language.

COMMITMENT

Above all, there must be commitment at the highest level of each involved function, and also sponsorship by the company's senior management, to make compliant and effective information management a priority. A high profile for information management is no longer a wish list item. Instead, corporate commitment to information management is now a legal compliance imperative.

For example, the FACTA Red Flags Rules of the Federal Trade Commission require that the Board or senior management oversee required identity theft programs and receive program compliance reporting at least annually.[8] Also, the Federal Sentencing Guidelines, which are highly influential in U.S. Attorney office decisions to prosecute, explicitly focus on whether organizations have in place an effective compliance and ethics program, known and overseen by the organization's governing authority and high-level personnel.[9]

The strategic approach discussed above requires dedicated effort to become reality. Fortunately, helpful standards and frameworks are available, such as ARMA International's GARP (Generally Accepted Recordkeeping Principles); ISO 15489, Information and Documentation - Records Management; ISO 27001, Information Security Management Systems; and ISO 27002, Code of Practice for Information Security Management. But to navigate the storm and chart a safer course, companies should first take a fresh look at the "C" change in information management: convergence, connections, collaboration, and commitment.

1. Public results for the annual Socha-Gelbmann ED surveys can be found at www.sochaconsulting.com.
2. 2009 Socha-Gelbmann ED Survey, *Id.*
3. *Pension Committee of the University of Montreal Pension Plan v. Banc of America Securities, LLC,* 2010 WL 184312 (S.D.N.Y. Jan. 15, 2010).
4. Id. at 11.
5. Id. Judge Scheindlin adds that the following lapses likely constitute negligence for spoliation sanction purposes: the failure to obtain relevant documents and ESI from employees other than key players, and the failure to assess the accuracy and validity of selected search terms. Id. For a contrasting approach emphasizing proportionality, see Judge Rosenthal's analysis in *Rimkus v. Cammarata*, 2010 WL 645253 (S.D. Tex. Feb. 19, 2010).
6. 42 U.S.C. 17931. 42 U.S.C. 17934.
7. 201 CMR 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth, requiring full compliance on or before March 1, 2010. For examples of other states' laws that extend beyond breach notification to require an information security program or procedures, see ARK. CODE ANN. 4-110-104(b) (Arkansas); CAL CIVIL CODE 1798.81.5(b) (California); MD. CODE COM. LAW 14-3503(a) (Maryland); 603A NEV. REV. STAT. 210(1) (Nevada); OR. REV. STAT. 646A.622(1)&(2) (Oregon); 11 R.I. GEN. LAWS 49.2 2(2) (Rhode Island); and UTAH CODE ANN. 13-44-201(1)&(2) (Utah).
8. 16 C.F.R. Part 681 Appendix A.VI
9. Federal Sentencing Guidelines Manual Section 8B2.1.

Contacts for Information Management:

Peter Sloan
Kansas City, MO
peter.sloan@huschblackwell.com
816.983.8150

Deborah Juhnke
Kansas City, MO
deborah.juhnke@@huschblackwell.com
816.983.8150

About Our Information Management Team

Husch Blackwell's Information Management Team helps clients with information retention, preservation, and compliant disposal. The team is part of the firm's Information Governance Group, which provides interdisciplinary expertise in Privacy, Data Security, and Information Management to help clients satisfy information compliance requirements and manage risk while maximizing information value.

About Our Firm

Husch Blackwell is an industry-focused, full-service litigation and business law firm with 16 offices across the U.S. and in London. We represent national and global leaders in major industries including energy and natural resources; financial services; food and agribusiness; healthcare, life sciences and education; real estate, development and construction; and technology, manufacturing and transportation.