Companies need information to succeed, including information on products, services, strategies, finances, customers, vendors, stakeholders, technology, business tools, the marketplace, regulatory requirements, employees, compliance, risks, and more. They also need to be able to secure their information, manage it according to regulatory requirements, gain timely access to it, provide for disaster recovery and business continuity contingencies, and efficiently mine and analyze it for business and legal purposes.
Striking the right balance is key. Keeping everything – when not needed for business or legal purposes – is a risk management strategy at an extreme end of the spectrum, one that is antithetical to good governance practices and prudent business strategies that otherwise seek to implement well-reasoned systematic approaches, drive efficiencies, and eliminate waste. For companies seeking to strike that balance, reasoned decision-making is fundamental to sound information governance and risk management practices.

This article explores some data realities, the importance of collaboration among various business functions and players, information governance considerations, the interplay of information governance and how it manifests itself in the litigation process, and some practical tips to consider in implementing information lifecycle governance practices to help minimize risks and improve readiness.

DATA REALITIES

We live in an “information age.” Increasingly, data and information sources are in electronic rather than in paper format. We’re expanding data types, sources, and channels, from computers and laptops to tablets and mobile and other devices; voicemail to email to instant messaging and text messaging; text-heavy information to infographics, visuals, and multimedia; desk drawers to warehouses of both hard copies and sometimes thousands of tapes; boxes to paper file systems to electronic document management systems; individual workspaces to shared collaboration workspaces and databases; customer call centers and website feedback channels to social media channels; and company-owned servers to vendor-provided servers to the cloud.

How we produce, gather, store, manage, and communicate business information has changed dramatically over the past few decades, and new technology advancements continue to transform information channels and data management practices every day. Additionally, companies are producing information at astounding rates, which is compounded by exploding data rates with high regulatory expectations for data protection, information security, privacy, and information management, all existing within a litigious environment. The end result: large volumes of data from a growing universe of data sources that need to be properly managed for business and legal purposes.

As the sheer volume of company data grows, so does the need for companies to be able to make reasoned decisions about how to defensibly manage information that is no longer needed. Keeping everything clutters information systems, hampers a company’s ability to swiftly and efficiently access needed information, drives up costs, and slows response time when government inquiries or litigation strikes and companies are forced to address data that was stored unnecessarily.

THE PLAYERS: CORE TEAM & WORKFORCE CONSIDERATIONS

Companies can address these challenges by focusing on team (i.e., “people”) and workforce considerations.

People issues include: 1) Identifying the right core team to collaborate on information governance lifecycle strategies; and 2) Integrating workforce considerations in setting strategies (e.g., employee on-boarding and exiting, access levels and confidentiality, legal hold considerations when people move from one position to another, managing user guidelines for mobile devices or company-issued devices, contractors, vendors, remote workforce issues, etc.).

Clear roles and responsibilities are important. Equally important is taking a matrix approach so that overall strategy is antithetical to good governance practices and prudent business strategies that otherwise seek to implement well-reasoned systematic approaches, drive efficiencies, and eliminate waste. For companies seeking to strike that balance, reasoned decision-making is fundamental to sound information governance and risk management practices.

Multidisciplinary Core Team to Set Strategy

Establish an inclusive, multidisciplinary team to bring together people with knowledge of the company’s organization, systems, technology, policies, records management practices, legal requirements and relationships with outside vendors who may provide technology or other services in connection with the company’s data. Key players to consider for the core team include representatives from business units, IT, legal, human resources, records management, security and/or risk management and procurement.

Strategic initiatives for the core group can include:

- **Data sources and technology systems**: Identify technology systems and data sources.

- **Employee and contractor access issues and movements**: Identify employee and contractor access issues; integrate information governance policies and practices with people movements (e.g., on-boarding, exiting, moving to new positions).

- **Information governance policies**: Assess and develop information governance policies.

- **Information security considerations**: Assess data types, sources, access rights, regulatory requirements, and integrate with overall information governance initiatives.

- **New business and technology initiatives**: Assess information governance considerations in connection with new business strategies, data mining practices, and technology initiatives and integrate with policies and practices as appropriate.

- **Training and communications**: Develop communications and training on information governance policies and practices.

- **Vendors and external providers**: Manage information governance issues with vendors and external service providers. This includes issues such as data security, retention and retrieval, business continuity, and any disposal obligations.
Workforce Considerations

Having policies and tools is important, but implementing, communicating, training, and executing them systematically is critical. Are there different requirements for different levels or categories of employees? How does the company manage information governance expectations for contract personnel or third party vendors and suppliers? Do company information governance policies apply to the Board?

Some workforce-level issues to consider include:

- **Access and security:** on-boarding, mobility, termination: Are there different levels of access or security at the system or device level for categories of employees or individual employees? How are these tracked so that security is maintained when employees move to new positions within the company or exit the company? What happens when contract personnel change job function or their contracts are terminated? Do human resources department checklists or other contractual arrangements include information governance considerations to address access and security issues?

- **Communications and training:** How does the company communicate expectations regarding information governance? Is training provided? How does the company refresh, retrain, and remind its workforce regarding information governance expectations?

- **Information governance policies:** What types of information governance policies apply to employees (e.g., email, electronic communications, social media, records management, litigation hold, mobile device or Bring Your Own Device, etc)? Do information governance policies apply to contract personnel and/or vendors and third parties and, if so, do only some policies or all policies apply? How are these policies communicated? Does the company train on these policies? How does the company refresh, retrain, and monitor?

- **Legal hold considerations:** Are there processes to track and address employee mobility within the company and any impacts on legal holds? What happens if company-issued technology or personal devices need to be repaired? Do legal hold policies extend to contract personnel, vendors, and third parties and how are they managed?

- **Personal devices:** What types of information governance policies apply to contract personnel, vendors, and third parties? How are these communicated? Does the company offer training or refresher training on these policies? How does the company monitor and enforce these policies?

- **Social media:** Does the company use social media channels for business purposes? Does the company have policies regarding employee use of social media for business purposes? How are these communicated?

- **Third party considerations:** How are access and security issues managed for contract personnel, vendors, suppliers, and third parties? Do information governance policies and practices extend to third parties? What about legal hold considerations? What types of service level agreement provisions in vendor contracts may be needed? May contract personnel use personal devices to conduct company business and, if so, what types of guidelines, policies, or practices apply? What happens when contracts or third party arrangements are terminated?

INFORMATION GOVERNANCE: DATA SOURCES, POLICIES, PRACTICES

As noted above, striking the right balance is key. Critical to the success of any programmatic implementation is ensuring that the overall approach and implementation pace and strategy are appropriate to the organization.

Establish an inclusive, multidisciplinary team to bring together people with knowledge of the company’s organization, systems, technology, policies, records management practices, legal requirements, and relationships with outside vendors who may provide technology or other services. Key players to consider for the core team include representatives from business units, IT, legal, human resources, records management, security and/or risk management and procurement.

With the core team identified and assembled, consider the tool sets that will be most effective for the organization.

Data Sources and Technology

Understanding data types, sources, and location is an important early step. Is the data structured or unstructured? Is it hard copy, electronic, or some other media form? Is data on corporate systems, personal devices, third party systems, in storage, other? Is it in a format that can be “read,” or is it legacy data in an antiquated format?

In order to understand your data types, sources and location, consider the “who,” “what,” “where,” “when,” and “how” of data:

- **Who:** Identify individuals generating and maintaining company data, both inside and outside the company as well as how and when information governance policies apply.

- **What:** Identify what types of data are generated and maintained and in what formats. Your organization likely has many forms of business information and data, including active and archived data, back-up and legacy data, data produced by individuals and in collaboration spaces or social media platforms. Consider types of systems and technology tools used by the company’s workforce. Consider company data that may be maintained by third parties. Consider special regulatory requirements for certain data types. Consider data and information that may be subject to preservation or legal hold requirements.

- **Where:** Consider where the data may be located. This includes company systems and devices, personal devices, social media platforms, records management facilities, vendor platforms, the cloud, etc. Consider corporate transactions (such as acquisitions, divestitures, joint ventures, etc.) and strategic partnerships. Assess jurisdictional requirements that may come into play, including data protection and privacy requirements.

- **When:** Assess when data was generated, and business and legal retention requirements. Understanding the history of the company’s technology practices and strategic technology and records-related relationships for data and information management can be helpful. Essential to
Policies

While policies on their own are not sufficient to establish good information governance programs, they help set the framework for good governance. No one size fits all. Policy names and the number of information governance-related policies will vary from company to company. In addition, teams or departments ‘owning’ the various policies may vary from policy to policy and company to company. For example, in some companies, a single team may ‘own’ all information governance-related policies; in others, a records management function may be responsible for records retention policies; the IT department may be responsible for Bring Your Own Device (“BYOD”) or policies relating to personal devices; and the litigation group within the law department may be responsible for policies and procedures regarding legal holds. In still others, different functions may be responsible for these policies.

In addition, for each policy, consider scope. Is scope limited to employees? Does it extend to contract personnel? Are vendors or other third party service providers addressed? Do these policies extend to the Board?

Following is a summary list of some common information governance-related policies included within information governance tool sets and some issues to consider in connection with each:

- **Electronic communications:** Some companies may have a single policy that covers all forms of electronic communications while others may have a collection of policies (e.g., email, text messaging, blog/social media, etc.) each addressing a specific form of electronic communications.

- **Company-issued devices:** If your company issues various devices (e.g., laptops, iPads, tablets, mobile phones) for business purposes, confirm that provisions such as user guidelines and practices such as asset management and tracking are integrated with overall information governance policies and practices.

- **Personal devices:** Also known as BYOD considerations in evaluating these policies and associated practices include: user guidelines, prohibited uses, restrictions on applications that may be accessed or downloaded, controls and security and privacy.

- **Preservation and legal holds:** Consider the scope of these policies such as who they apply to, how communications pursuant to the policy to issue holds are made (and refreshed), how the policies integrate with other electronic communications and information governance-related policies and how administering and tracking legal holds occurs. Consider how people movements (e.g., employees leaving the company and turning in equipment) are addressed and consider what happens to information that is no longer subject to legal holds once the hold is lifted.

- **Records retention:** Consider the definition of “records” for purposes of these policies and how records retention policies are communicated. Assess practices to refresh and train. As new data types and sources are created, consider practices to assess whether they are covered under existing definitions and practices or whether they need to be updated.

- **Social media:** If the company has company-sponsored social media channels, consider any policies and controls regarding employees posting to that channel. Consider also whether any social media policies extend to personal social media accounts or posting to third party social media channels.

- **Strategic initiatives:** Consider how information governance considerations are integrated into broader corporate strategic initiatives, including new technologies, new vendor relationships for services or technologies, new business ventures or corporate transactions (including mergers, acquisitions, divestitures, joint ventures), new practices for collaborating or communicating within the company or with third party service providers (including collaboration workspaces). Determine whether any strategic initiatives checklists might include information governance considerations.

**INTERPLAY OF INFORMATION GOVERNANCE & E-DISCOVERY**

As mentioned earlier, in many organizations responsibility for information governance-related issues is a records management or compliance function and responsibility for legal holds and e-discovery may be considered part of the legal/litigation function. Increasingly, issues of information governance and e-discovery are integrated. Good information governance practices help improve overall litigation readiness and e-discovery process defensibility.

How might this interplay manifest in the litigation process? Are there certain practices to consider? Rarely is a case won on excellent discovery. However, information governance is important to overall defensible litigation practices, which can help avoid costly and distracting discovery-related disputes.
Key considerations include:

• **Early dialogue on where data resides:** There is an expectation that litigants will engage in an early discussion of where data resides. This may be a structured dialogue, may involve discussions of systems, when they were put in place, nature and form of data and the lifespan in the ordinary course of business. For many, this isn’t a difficult discussion. But for some companies it is and it is helpful to be careful how the record is defined.

• **26(f) stage discussions:** A common scenario during this phase is being asked the following question: “You told us that data resides here. Tell us now about how the data ought to be kept, what your policies are, etc.” Different companies are often at different levels in their ability to respond. For some companies, certain data types may not be covered by a given policy.

• **Policy infrastructure and practice:** Another area of inquiry relates to whether practices are working in accordance with policies. Who is responsible for managing legal holds programs? How are auto-delete suspensions executed, who is in charge and how does this work? These are areas where disciplined communications and integrated information governance practices can be helpful in establishing defensibility.

• **Forensically sound collection and tracking:** Being in a position to show that the company is consistent and faithful in execution of its data collection and tracking measures is helpful.

• **Sufficiency of preservation:** Increasingly, litigants are conducting discovery on discovery and employing tactics to attack sufficiency of preservation and adequacy of discovery process. Spoliation allegations can lead to adverse inferences and game-changing sanctions. Integrating information governance with broader litigation readiness helps ensure that defensibility considerations are at the forefront.

• **Adequacy of search and production:** Because litigants are also increasingly attacking discovery processes regarding adequacy of search and production of documents, be mindful of these assertions and implement practices up front to address attacks on discovery approach.

• **Role of attorney-client privilege:** Certain discussions regarding preservation and discovery require legal input. Be mindful of maintaining attorney-client privilege and of communications that may be unprotected by privilege.

### INFORMATION LIFECYCLE GOVERNANCE: DEFENSIBLE DISPOSAL CONSIDERATIONS

With data being produced at explosive rates, and the importance of good information governance, come considerations of how best to manage the overall lifecycle of information. What happens when information is no longer needed for business or legal purposes? As noted above, a “keep everything” approach may not make good business or legal sense.

For companies considering defensible disposal measures as part of information lifecycle governance, steps to explore include:

• **Assemble the team:** Similar to assembling information governance players for overall information governance strategies, assemble a multidisciplinary team including representatives from legal, records management, IT and business professionals with knowledge of company policies, business needs, the legal hold process, technology systems, organizational structure and system constraints.

• **Assess current practices and requirements:** Consider applicable legal requirements. If the company has a centralized approach to legal holds and records management, assess how policies address information that is no longer needed for business or legal purposes. Among various considerations, determine when current litigation hold policies were implemented, how policies treat backup media, how policies treat duplicate data, whether vendors (current or former) have responsibilities in connection with maintaining corporate data and records and what those responsibilities are. Identify any special considerations that may be applicable.

• **Create and implement a project management plan:** Clearly defined responsibilities and workflow practices are important to the overall approach. Consider documenting the project, including creating a project plan that identifies key steps and documenting disposition decisions and the supporting legal analysis. Establish a plan and create an inventory that identifies and categorizes data populations and available information on those populations.

• **Implement the plan:** Analyze the data and requirements, including applicability of legal and business retention requirements and implement the plan, building upon prior steps.

• **Disposition:** Once data is identified for disposition, thoroughly document the steps taken and supporting analysis to arrive at a decision of whether or not to dispose of data. If disposal determination is made, implement measures to ensure that confidentiality and privacy is not compromised.

### CLOSING INSIGHTS

Information governance is an ongoing process. Just as technology and business strategies are changing in today’s dynamic business environment, so too must approaches to information governance be flexible to address the realities of new data types and technology tools and solutions, organizational changes and business arrangements.

While each company will design its own approach appropriate to the business and culture of the company, some general keys to success include:

• **Tone at the top:** Most companies are not in the business of information governance, they are in the business...
of producing products or services. Having top leaders emphasize the importance of information governance is a key success factor to inculcating information governance throughout the organization.

- **Team:** Information governance is not the responsibility of a single person. A strategic team should include professionals with line of sight into technology, human resources, legal requirements, records management, risk management, security and business practices who can help best position the company to design and execute programs and policies tailored to the needs and business practices of the organization.

- **Culture:** As with any organizational policy, information governance policies and practices that are designed to fit the overall corporate culture will be most easily integrated into everyday practices and the fabric of the organization.

- **Policies and training:** Policies help set the framework. Policies need to be communicated and refreshed. Training on the policies is also important to execution.

- **Sustainability:** As policies and programs are designed, consider how to establish practices that will be sustainable.

- **Get started:** Devoting time and effort to information governance practices can be a daunting endeavor. Start somewhere, demonstrate success and value and build upon those efforts.

**AUTHOR BIOGRAPHIES**

John D. Martin is a partner of Nelson Mullins Riley & Scarborough LLP. John’s practice focuses on product liability and business litigation, electronic discovery and information management. He is a leader of the Nelson Mullins Electronic Discovery and Information Management practice group and Nelson Mullins Encompass E-Discovery and Document Review Solutions. Renee Danker is of counsel to Nelson Mullins Riley & Scarborough LLP in the Columbia office. Renee’s areas of focus include electronic information management and governance, E-discovery, client relations and business intelligence.