Managing Information Across the Extended Enterprise:

A Look at the Top Five Information Management Risks for the General Counsel

Chances are good that you are reading this white paper on a smart phone or tablet computer. According to a survey by IDC and Unisys, 95 percent of IT workers already use their own technology for work, due to the ease-of-use and ubiquitous nature of portable technology among modern professionals.[1] Chances are also good that your company still stores a large amount of information in paper-based files in separate locations across your organization and beyond among an extended enterprise of business partners. For General Counsels the extended enterprise includes relationships that range from simple ad hoc collaboration with third party vendors to long-term partnerships with outside counsel or board of directors. Regardless of the relationship,tracking and managing critical information across a business can create significant challenges for general counsel.

While devices that enable the user to multi-task can be convenient and efficient, they also pose complex problems for in-house legal teams responsible for data management, protection, and preservation. In an environment where simply reinstalling the operating system on a computer a year after filing suit without first saving the electronic version of key documents could warrant a small spoliation sanction of $15,000,[2] or $3.2 million for intentionally deleting unallocated space contrary to an order directing the parties to refrain from disposing of relevant records, corporate legal departments must be hypersensitive to data concerns.[3]

Paper-based document storage still exists across many enterprises as well, meaning that key pieces of corporate information could be sitting in binders or filing cabinets. This often makes it difficult to locate, assemble, and review key documents within short timelines. Before using the IntraLinks platform Memorex's legal department, for example, had the headache of managing tens of thousands of documents through a system of paper-based binders. By creating a single solution for document storage, the time it took them to send documents to Hong Kong went from three days to ten minutes.

[1] Unisys Consumerization of IT Study, 2010, http://blog.unisys.com/files/2010/08/10-0190-CIT-SUMMARY_web.pdf

[2] *Herson v. City of Richmond*, 2011 U.S. Dist. LEXIS 89467 (N.D. Cal. Aug. 11, 2011) (Such action did not have to be in bad faith to warrant sanctions because plaintiff was on notice of the possible relevance of the deleted electronic documents.)

[3] Genger v. TR Investors, LLC, "TR Investors III", 2011 Del. LEXIS 371 (Del. July 18, 2011) (The court held that the deletion prejudiced the opposing party by preventing the discovery of different versions of documents or email chains.)

INTRALINKS®

1 866 INTRALINKS

New York + 1 212 342 7684
London + 44 (0) 20 7549 5200
Hong Kong + 852 3796 2733
São Paulo +55 0800 892 2247

www.intralinks.com

"The consumerization of IT and employees wanting to use personal devices for work has created challenges for in-house counsel."

– Vince Miraglia,
Chief Counsel for Litigation,
International Paper

While there are many cases of document mismanagement that make headlines in the legal press, it is often unintentional actions that cause the greatest concern. From losing track of documents and transmitting unsecured records to complying with regulations across jurisdictions and safeguarding sensitive material, there are new information risks and technologies and best practices to avoid them.

Losing Track

In a global marketplace of e-signatures, virtual agreements and shared responsibility for obligating an entity to an array of unusual commitments, corporate counsel must streamline the trail of information that passes through the extended enterprise. Remote work environments, overseas affiliations, and flexible information management protocols could result in document confusion or knowledge loss. The consequences of such results often cause substantial harm that in-house lawyers could easily avoid by implementing a solution that serves as a secure repository for document sharing coupled with a series of best practices.

For example, there are prominent electronic discovery concerns. As more employees with potentially discoverable information conduct operations on a tablet computer or smart phone with non-standard applications, they create security and archiving issues. Often, in order to open an attachment on such a device, software that uploads the document to a third party application is required. The document, including any modifications made to the record, is then saved to a third-party server outside of the company's firewall. That loss of control is a concern because of the complexity of managing disparate forms of data and the cost of ensuring proper record keeping protocols.

"The consumerization of IT and employees wanting to use personal devices for work has created challenges for in-house counsel," says Vincent Miraglia, the Chief Counsel for Litigation at International Paper. While employees seek to use their personal iPhones and iPads, for example, to work more efficiently than they can on less user-friendly company-issued equipment, the linkage of personal devices to a corporate network could create broad legal implications.

Organizations seeking to avoid losing track of their data should adopt a single solution that serves as a central location for document sharing and distribution and draft clear policies and offer viable alternative arrangements for enforcement. An IT team might consider allowing an employee to review documents on an iPad through an approved app, but prohibit editing that item in a separate third-party app.

"Technologists are exploring the options too, but the technology does not seem as mature as necessary yet," says Miraglia. "At this stage, we are addressing the issue through policy and by limiting the access that people have," he adds.

Generally security is not as big of a consideration since devices can be remotely wiped if they are lost. It is the control of the data and the access to it that is of greatest concern. "If an employee saves a document to an app that is not officially sanctioned for use within our environment, it complicates our work from an e-discovery perspective," notes Miraglia. He also urges restraint in using personal devices for work-related matters. "It perpetuates itself," he cautions. "Despite an employer's instructions, once they have it on their tablet, there's a chance that they might synch that information with their iPhone, PDA or other devices, which then might interact with cloud."

Containerization, the lack of synchronization of all of the documents and e-mail messages to a corporate network, is also a concern. The legal team at the Atlanta-based mattress manufacturer Simmons Company went through a series of ownership changes, which resulted in fractured document management, storage, and retention practices. Legal files, contracts, and other important documents were scattered throughout various divisions and departments across the company until they adopted IntraLinks as a central document repository.

Mismanaging Contracts

Monitoring key documents throughout their lifecycle is critical for in-house legal teams, which have historically relied on business unit managers to track contracts and their key time frames. In fact, recent financial and health care reform has created new sweeping obligations to oversee the contracting process at each stage of its lifecycle. These changes have forced greater scrutiny and sensitivity to even the least important agreements. "We are now facing regulatory requirements to maintain additional documents, but the practical implications of responding to regulators, following internal preservation guidelines, and adhering to various litigation hold restrictions is a significant challenge," notes one in-house lawyer for a Fortune 500 corporation.

The overwhelming volume of information and increased demands on corporate legal departments trying to run more efficiently with fewer resources is so great that over the past few years, the National Institute of Standards and Technology (NIST), an agency of the U.S. Department of Commerce, has co-sponsored an interactive document review exercise that features both academic and commercial participants focused on electronic discovery, among other areas. And, according to Fulbright & Jaworski's 7th Annual Litigation Trends Survey Report, more than 40 percent of the largest U.S. corporations planned to increase their spending on electronic discovery in 2011 in part because of this burden.[4]

The risks of missed deadlines, non-compliance with material requirements or unsustainable agreements, are forcing chief legal officers to leverage a unified repository of all corporate records across the enterprise. And, with more than half of the largest companies in the U.S. employing at least five attorneys in their legal departments,[5] and those lawyers handling more of the work in-house as "almost as many U.S. companies have decreased their litigation budgets and litigation spend as have increased them," information governance is a prominent consideration.[6]

Yet, as specific business units maintain their key documents to increase efficiency and streamline their business development efforts, legal hold and internal investigations become more complex. Despite educating employees on recent regulatory requirements and internal document destruction policies, the disparate nature of data within most organizations creates a strategic task fraught with peril: the desire to preserve documents balanced with the challenge of destroying them on a legitimate and routine schedule.

Certain states are even considering new legislation mandating an enhanced audit trail for electronic health records, notes the in-house lawyer, who highlights that the burden of maintaining that audit trail can be substantial. This is an issue that all highly regulated industries, e.g., financial services, healthcare, and pharmaceutical have historically faced, but that may reach previously unaffected organizations due to new statutory requirements.

The hazard of mishandling contracts often arises at the intersection of records management, litigation hold, regulatory responsibility and privacy, highlights the in-house attorney. "They come together in a problematic way because there are different obligations and priorities," the lawyer says. In fact, "the enemy of streamlining and efficiencies that you can enjoy by virtue of having electronic records is the hybrid of paper documents and electronic information that all companies maintain," she adds. It often requires additional effort and separate systems.

Ultimately, it is important to create a culture of compliance with records retention schedules and to use technology to support the underlying processes to encourage adherence to a global records management policy. "The issue is knowing when to let something get destroyed and actually doing it," says the in-house counsel. "Many companies are doing a good job of implementing a legal hold, but not doing a good job of releasing it; you are creating liability where the whole process was to mitigate it," the lawyer adds.

The risk of missed deadlines, non-compliance with material requirements or unsustainable agreements are forcing chief legal officers to leverage a unified repository of all corporate records across the enterprise.

"The enemy of streamlining and efficiencies that you can enjoy by virtue of having electronic records is the hybrid of paper documents and electronic information that all companies maintain."

[4] Fulbright & Jaworski, *7th Annual Litigation Trends Survey Report, 2010 at 28.*

[5] *Id.* at 18.

[6] *Id.* at 26.

As new software, business arrangements and strategic developments impact what regulations apply to which pieces of information, it is virtually impossible for a handful of data guardians to secure the process alone.

Failing to Comply with Regulations Across Jurisdictions

Mitigating liability in a sea of new restrictions seems more like using a row boat to cross the Atlantic Ocean than operating a modern legal department, but there are key components of a successful management program.

That said, in the current economy, the level of regulation is increasing at a rapid pace in the U.S. and overseas. From the Dodd-Frank Wall Street Reform, Consumer Protection Act, and the UK Bribery Act the government is requiring unprecedented reports, accountability and adherence to strict operating guidelines. Those organizations that centralize control of regulatory filings for financial reforms, employment, environmental concerns, permits, and licensing, among others, relating to all past, pending and future matters will be better equipped to respond to the changing landscape and manage regulatory demands across multiple jurisdictions.

Immediate availability and accessibility of information pursuant to sudden requests could mean the difference between a short-term inquiry and long-term investigation. In fact, says one in-house attorney with a Fortune 500 company, "regulators occasionally get a different sense of accessibility when confronted with a well-managed document retrieval system."

This perspective transformation requires a coordinated effort between members of the legal team and their counterparts in information technology, records management, and compliance. As new software, business arrangements and strategic developments impact what regulations apply to which pieces of information, it is virtually impossible for a handful of data guardians to secure the process alone. From regular meetings to an interdepartmental task force, organizations that provide enterprise-wide updates and instructions often reap the rewards of their skillful administration.

In addition, the increased emphasis on privacy over the last several years has sensitized individuals and institutions about their responsibilities related to protected information. Nearly two-thirds of health care companies, 60 percent of insurance companies and close to half of the technology/communications, retail/wholesale, and financial services sectors encountered issues involving privacy and data restrictions in 2010.[7]

And, state legislators are now creating what the in-house lawyer describes as "a patchwork quilt related to privacy in terms of compliance," the area is dynamically shifting on a routine basis. To adequately evolve with this rapid pace of potential change, organizations much rely on both harmonized interaction between internal leaders and a key focus on advanced tools that can match the rate of evolution.

"It is often a classic situation of technology outstripping our ability to manage it because every time you have a technological innovation, it raises questions in terms of storage, security, accessibility and transportability." Those entities that take a holistic approach to marrying their information architecture with the talent of their teams can quickly address seemingly sudden changes to a once familiar regulatory framework. This is critical because "expectations among all respondents [to the Fulbright & Jaworksi survey] of more [internal] investigations outweigh[ed] those of fewer such investigations by more than two to one."[8] In fact, a third of the U.K. companies surveyed reported having had one or more proceedings initiated against them in 2010, which was up significantly from 9 percent in 2009.[9]

[7] *Id.* at 49.

[8] *Id.* at 30.

[9] *Id.* at 30.

Transmitting Unsecured Documents

As colloquial and casual communication is becoming more widely accepted, corporate employees are transmitting information requiring various levels of protection in an increasingly unsecured fashion. Whether via e-mail or in hard copy using an overnight mail carrier, the modern transfer of information must maintain the proper threshold of control given the ability to reproduce, distribute, and abuse data in the digital marketplace. From social networking to network security, maintaining a proper document trail from creation to destruction of each record is critical for reducing risk. With 65 percent of adult Internet users exchanging information through social networking sites like Facebook and LinkedIn, this an increasingly significant problem.[10]

In the past, an employee could only transmit documents and information via a secure network protected by a vast corporate infrastructure and enterprise-wide series of protocols. Today, most individuals can access the Internet at work through their standard-issue computers and PDAs, as well as via personal devices that have unsecured 3G or 4G access, or a Mi-Fi tool that creates yet another unsecured personal hot spot.

This might enable employees to sync their device at work for information purposes, but give that device the flexibility to bypass those security protections (by accessing another gateway to the Internet) when he or she is interested in visiting a restricted site. This could lead to sexual harassment concerns, trade secret theft and violations of legal holds.

For instance, an employee taking harmless pictures of patented machinery and uploading them to Facebook may cause irreparable harm to an institution, or exchanging text message about both lunch and business-related concerns. "The proliferation of these devices is making it a far more complicated task to collect, preserve, and produce documentation in a lawsuit or event in a simple records management matter," highlights Miraglia. "Spoliation of potentially relevant information in a lawsuit can result in significant damages," he advises.

The uniform use of an enterprise-specific tool to exchange information can help organizations to navigate information governance. From a practical perspective, organization's should select a tool that is seamlessly integrated into the most popular practices of the organization's employees to ensure adoption. In addition, users should receive training and access on as many platforms as possible to encourage integration into their work. That upward trend in investigations is a key consideration in document security.

Safeguarding Sensitive Material Enterprise-wide

In a hyper-competitive and hyper-collaborative business environment, these small, but potent, strategic advantages are crucial for success and legal teams must preserve that positioning by safeguarding information necessary for key transactions and macro decision-making. Documents exchanged with the members of a board of directors regarding corporate governance, those relating to intellectual property rights and protection, sensitive strategic plans, and other material can impact the future trajectory of an entire entity. As a result, proper maintenance of that data is vital for modern records management.

In an instant, an employee who mistakenly hits 'reply to all' or has a malicious interest in intentionally causing confusion could dramatically affect an organization's business. In addition to establishing business practices to protect against this, technology can also support the protection of sensitive material managing and tracking access to sensitive materials — automatically reducing the risk of disclosure.

The uniform use of an enterprise-specific tool to exchange information can help organizations to navigate information governance.

[10] Pew Internet & American Life Project, What Internet Users Do Online, Rev. Summer 2011, http://pewinternet.org/Trend-Data/Online-Activites-Total.aspx.

With fewer resources to provide this granular level of oversight, it is natural to turn to technology to help manage oversight and minimize risk. While most document management systems offer this basic capability, the varied nature of how one transfers information, forum, and character of the details require more advanced options.

Organizations facing these different obstacles must address them on an enterprise-wide basis. In addition to taking affirmative steps to encrypt e-mail, legal teams must coordinate with the company's technologists to limit the ad-hoc levels of security driven by individual users merging their personal and professional communications. Tools exist to promote greater uniformity by removing the decision-making authority from the user and returning it to the institution. Leveraging them will make the safeguarding process more seamless.

The Future of Risk Readiness

While document tracking and management are certain to remain critical concerns as the future of information governance becomes the present, organizations that apply the right technology and best organizational practices will remain competitive. Leaders within legal departments and on technology teams who foster collaboration, knowledge sharing and coordinated advancement will set the foundation for managing information across the enterprise.

About IntraLinks

For more than a decade, IntraLinks' enterprise-wide solutions have been facilitating the secure, compliant and auditable exchange of critical information, collaboration and workflow management inside and outside the enterprise. For simplifying business processes such as board of director communications, post-merger integration, acquisition management, corporate finance and legal matter management, the IntraLinks platform can help improve operational efficiency and reduce time and costs while adding increased security and control to processes. More than 1,000,000 users across 50,000 organizations around the world rely on IntraLinks, including 50 of the 50 top global banks, 10 of the top 10 life sciences companies, 25 of the top 25 law firms, and 14 of the 15 largest private equity firms.

To learn how IntraLinks can transform your business, visit **www.intralinks.com** or contact us at:

Tel: 866 INTRALINKS (USA)
Tel: + 44 (0) 20 7549 5200 (EMEA)
Tel: + 852 3796 2733 (APAC)
Email: **info@intralinks.com**

Terms of Use

Although IntraLinks has made every effort to provide accurate information in this document, IntraLinks makes no representations as to, and does not warrant, the accuracy and/or completeness of the information herein or its suitability for any particular purpose. The reader assumes all risk and responsibility for his or her reliance on, or use of, any of the material contained in this document.

ALL INFORMATION IS PRESENTED "AS-IS," AND INTRALINKS DISCLAIMS ALL EXPRESS OR IMPLIED WARRANTIES AND CONDITIONS WITH REGARD TO THE INFORMATION, INCLUDING THE IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NONINFRINGEMENT. IN NO EVENT SHALL INTRALINKS BE LIABLE FOR ANY DAMAGES WHATSOEVER, INCLUDING BUT NOT LIMITED TO DIRECT, INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING WITHOUT LIMITATION LOST REVENUES OR LOST PROFITS, THAT MAY RESULT FROM THE USE OF THIS DOCUMENT.

1 866 INTRALINKS

New York + 1 212 342 7684
London + 44 (0) 20 7549 5200
Hong Kong + 852 3796 2733
São Paulo +55 0800 892 2247

www.intralinks.com