Bloomberg Law

Digital Discovery & e-Evidence®

Counsel and the Cloud: A Lawyer's Role in Office 365 Migration

BY T. SEAN KELLY

Data security risks—data breaches, employee fraud, regulatory changes—are what keep legal, security, IT and compliance professionals up at night. These professionals are challenged to support the modern workplace environment, which includes mobile phones, remote employees, cloud collaboration sites, social media, instant message platforms and chat rooms. And they must keep this data secure and easily retrievable for legal or regulatory needs. While it's clear that these concerns affect many different groups within an organization, these groups are often not on the same page when it comes to identifying, selecting and implementing solutions.

T. Sean Kelly is a Senior Director within FTI Technology's Information Governance & Compliance Services practice. He advises clients on all aspects of eDiscovery and information governance, with particular focus on developing and implementing legal hold processes and technology as well as the legal impacts of migrating to Microsoft Office 365. He leverages more than a decade of experience in both legal technology and litigation support to advise clients on evolving technologies and the shifting landscape associated with cross-border transactions for global enterprises. Sean previously worked for Johnson & Johnson, where he was responsible for eDiscovery issues across business sectors, advising internal stakeholders and outside counsel on best practices in collection, forensic technology, document review and controlling cost.

Enterprise migration to Microsoft Office 365 (O365), a cloud-based communication and collaboration platform, is a growing area in the broad landscape of data challenges. O365 has more than 60 million commercial customers, a number that grows at a rate of 50 percent quarter over quarter.

Over the last five years, Microsoft has evolved its offerings around data governance, including eDiscovery and retention capabilities, to enable users to more efficiently handle regulatory requirements and litigation matters. These features, along with enhanced security capabilities for detecting email-borne threats and preventing data breaches, are included in O365, making it an attractive choice for businesses. The convenience and cost benefits of the cloud are further spurring adoption.

Organizations that are currently migrating to O365, or preparing to do so, may hit legal and compliance roadblocks. The movement of critical corporate data to the cloud raises security and data protection concerns, and we are seeing advanced email threats on the rise for corporations of all sizes. For these reasons, O365 migration should be viewed as a critical business initiative for which the legal department must be one of the primary decision makers every step of the way.

But although O365 migration presents some legal challenges, it also gives a company powerful tools for meeting its eDiscovery obligations.

eDiscovery has become integral to any organization's compliance program. Limiting the preservation of data to what's legally required is a top priority.

Analytics have made a big difference in streamlining these efforts. In the early days of eDiscovery, businesses didn't have access to the type of features that are available now in O365 and other emerging cloud solutions. The robust analytics, such as data visualizations and machine learning, that are available today have been critical in providing important information and insight in real-time. These advancements also make it possible for legal and compliance teams to identify and access critical information quickly and ensure that their programs are complementary.

When a company makes the shift, counsel must first and foremost determine its role in the migration. Is the legal department driving the implementation for risk management and responsiveness, or is it responding to a business requirement coming from another group? It is critical to determine who and what the internal drivers are for a migration, as these will influence how the migration is conducted.

But whether legal is at the helm, or is merely being called in by IT or another group to make sure legal requirements are met, the handful of best practices discussed below will ensure a smooth transition and mitigate legal and compliance risk.

Define stakeholders and drivers. O365 implementations may be driven by a variety of internal sponsors, all having varying needs and goals. The CFO or finance department might want to reduce year-over-year spend by remediating data and increasing storage efficiency. The IT department cares most about reducing big data and ensuring that the organization doesn't suffer from network overload. The legal team is focused on data governance to ensure e-discovery and legal hold compliance and fulfillment of regulatory requirements.

The team of stakeholders should be fully aligned and transparent about the goals of the project. Collaboration across groups including legal, IT, compliance, records management and security is the most effective approach to ensuring downstream success. A single executive sponsor who has internal recognition will help keep things on track and ensure that everyone is engaged at the right level. Executive sponsors can also be touted in email pushes, internal videos about the project and training programs to help drive company-wide adoption of new programs and technology.

Build around eDiscovery and retention requirements. For more than half of organizations, legal hold requirements lead to over-preservation of data. This puts a strain on the network system and drives up storage costs. Making sure that the organization is not over-preserving is critical, as is thoroughly fulfilling the duty to preserve and thereby avoiding the risk of a spoliation challenge. Corporations must establish migration processes and in-house policies that are tailored to the organization's existing eDiscovery needs, legal hold obligations and regulatory preservation requirements.

With O365, retention settings can apply to an entire mailbox, and retention periods can apply to a specific folder. Counsel must work with IT to ensure that these capabilities are leveraged to avoid legal hold or regulatory violations. It is important to align the varying retention periods across different data types to avoid legacy data problems and ensure comprehensive legal hold compliance.

Examine security and back-up needs and capabilities. An estimated 1.37 terabytes of data are uploaded to O365 each month by the average organization, and about 20 percent of those documents contain sensitive data. The scope of potential security vulnerabilities is vast. It is critical for cloud security parameters to be closely scrutinized by internal IT, information security, risk, compliance and legal teams to ensure the cloud provider meets the organization's unique needs. This is particularly important for corporations in financial services, pharmaceutical, healthcare or other highly regulated industries.

Back-ups and disaster recovery are additional areas that should be evaluated and discussed among stakeholders early on in a migration process. The team should discuss questions such as:

- Where will back-ups ''live''?;
- How, when and with what frequency will they be done?;
- What steps are taken during a disaster?; and
- In the event of a disaster, how will critical and sensitive data be protected and recovered?

Select a migration methodology. Many organizations struggle to identify the best migration methodology. Choosing correctly will help get the job done with minimal disruption to end-users. There isn't a one-size-fits-all approach, given the many variables that come into play, including regulatory profile, size of the organization, stakeholder risk tolerance, etc. The most common and effective approaches are imap, cutover, staged, or a hybrid of these.

To summarize: 1) imap uses the exchange admin center or exchange management shell to migrate the contents of users' mailboxes from the local exchange server to their cloud mailbox; 2) cutover moves all on-premise mailboxes to the cloud over a period days or weeks, and is primarily used when the organization is migrating all of its email files without any prior remediation or archiving; 3) staged is when all of the mailboxes, including archived mail, are migrated in batches, with the ultimate goal to permanently decommission on-premise servers to save money on hardware and infrastructure overhead; 4) hybrid means a combination of approaches that gives a seamless look and feel for end-users, while stakeholders are monitoring the migration on the back-end.

The biggest legal concern when selecting the migration methodology is how it will affect document retention. Attorneys may often prefer a hybrid deployment, because it provides an intermediate step that allows IT to get the cloud up and running quickly, but also enables on-premises control so that counsel can ensure compliance.

Address international factors. Legal teams within large organizations must take foreign legal requirements into account. There are existing and emerging data protection regulations that govern what data can be migrated and how employees in certain jurisdictions must be notified if any of their data is moving to the cloud. Obligations vary greatly by jurisdiction. Legal needs to have a voice across efforts in all locations, so that it can build multi-national considerations into the migration plan.

For organizations that have a significant international presence, involvement of local counsel or outside providers in each region will help the company understand the nuances of the various data protection regulations.

Technical considerations to vet with IT. There are a handful of additional factors that legal should raise with the IT department in advance of and during a migration. These technical issues will not require legal's hands-on involvement, but it is important for in-house counsel to be aware of potential issues and keep the team of stakeholders accountable. One of these is identifying network upload capacity, which will dictate how much data can be moved at a time, and thus will affect the overall migration.

Similarly, legal teams often overlook compatibility testing and data validation. IT should evaluate and test mobility of applications on the network and third party tools such as Salesforce, Skype, WebEx and others that will interact with O365, to ensure smooth integration. After data has been migrated, IT must validate that everything was indeed moved successfully. Anything that was inadvertently overlooked or left on-premises may pose a risk; migrations may drop critical files, and those mistakes must be identified so there isn't an impact to business operation, legal hold or other regulatory compliance.

O365 has a collection tool that can locate, copy and/or delete PST files (i.e. A file format used to store copies of messages, calendar events and other items within Microsoft software) that aren't necessarily in an end-user's mailbox. Legal should discuss with IT whether this extra step is needed to meet preservation obligations.

Reality Check.

In the ideal migration, all of the key stakeholders are involved at the outset, legal has the opportunity to evaluate the process and solutions, and outside counsel confirms that the methodology is sound. Having an opinion from outside counsel can help defend against spoliation charges, or violating the duty to preserve relevant evidence. But within most organizations, especially those in unregulated industries, migration in reality often looks much more reactive than proactive.

When legal is not the driver of migration, the eDiscovery team or in-house counsel may be alerted to the process after the fact, or when an active eDiscovery matter arises. When legal is brought in late in the game, the head of litigation needs to put a time-out on the project to get everyone on the same page. A best practice in this scenario is to bring in outside providers that will recommend how to plan the project and head off problems.

A migration to O365 presents a prime opportunity to establish or refresh new information governance and email security policies, as well as a plan for their enforcement. A new policy should specifically address Exchange online, and build in measures for automated enforcement of policies and legal holds. O365 offers functionality to support this, and other tools built for legal hold and security can be integrated during migration to proactively layer-in the necessary level of protection and enforcement. The key is that the organization's leaders view a cloud migration as a major system overhaul and IG initiative that requires cross-functional input, executive sponsorship and a thorough, strategic implementation plan.

To contact the editor responsible for this story: S. Ethan Bowers at sbowers@bna.com