METROPOLITAN
CORPORATE
COUNSEL®

MAY 2017

WWW.METROCORPCOUNSEL.COM

MCC INTERVIEW: T. Sean Kelly / FTI Technology

IN-HOUSE OPS

Ready for an Upgrade?

What you need to know about Microsoft Office 365

*T. **Sean Kelly**, a senior director at **FTI Technology**, spends a lot of his time helping clients implement, and conduct information governance and e-discovery using, Microsoft Office 365. Kelly previously worked for Johnson & Johnson, where he was responsible for e-discovery issues across business sectors, advising internal stakeholders and outside counsel on best practices in collection, forensic technology, document review and cost control. The interview has been edited for style and length.*

MCC: Who is adopting Office 365, and what are some of the business drivers you're seeing among those companies?

Kelly: The adoption trend for Office 365 has been soaring over the past 24 months. Individuals and companies are moving away from the traditional software suite to the cloud-based, evergreen Office 365. According to Microsoft, 88 percent of the Fortune 500 are part of the company's 1 million cloud servers, available in more than 125 markets worldwide. Moving to Office 365 is not a matter of *if* but *when.* Gartner's July 2016 report estimates that 54 percent of organizations will migrate to Office 365 within the next three years.

In addition to the Microsoft Office tools users are familiar with – Word, PowerPoint, OneNote, Excel, Project and Skype – Office 365 allows organizations to manage their data more efficiently (reduce cost), and do more with it (increase data value). Migrating to Office 365 reduces traditional information technology resources. Eliminating hardware expense and drastically reducing human resources creates significant savings for an organization. It's especially important for legal teams to understand that the product includes e-discovery functionality. It's now possible for companies and their managed service providers to manage, collect, process and conduct first-pass reviews without moving the data. We can do that today by securely accessing the company's tenant.

It's especially important for legal teams to understand that the product includes e-discovery functionality.

MCC: What are the benefits that individuals and companies perceive?

Kelly: For e-discovery, companies often use multiple software applications to handle discrete steps within the e-discovery process, from collection to processing to review, and these handoffs can increase the cost and risk of e-discovery. Microsoft Office 365 can streamline this since it has e-discovery features across the entire electronic discovery reference model (EDRM) and can be used on the data where it resides. Another key benefit is compatibility. You no longer have to worry if a colleague is using the same version of Office as you, or whether your PowerPoint builds will break mid-presentation. Security is another critical reason. Microsoft has invested significant resources into the security infrastructure of their cloud.

MCC: Since you bring up security, I'll raise an issue that I personally have been dealing with recently. I have sent emails to individuals who I've been talking to and have agreed to set up interviews with, and my emails have bounced. I got messages that explained that my email set off an Office 365 spam alert because I wasn't authorized.

Kelly: Part of the security features that Office 365 offers to users is the ability to manage and customize features such as connection filtering, spam filtering, transport rules and email authentication. Additionally, as long as the system administrator has not disabled them, there are many end-user managed settings that allow a user to customize the way they receive mail. For enterprise customers who have purchased advanced threat protection (ATP), connection filtering is further enhanced by spoof intelligence that creates "allow" and "block" lists of senders who are spoofing the organization's domain. ATP also allows Exchange administrators to create policies that help mitigate the risk of a user navigating to or opening an unsafe link.

MCC: When I just told you about my own experience, does this strike you as a good thing that shows that this product is more robust and on the alert than previous versions?

Kelly: It does. I think that increased security around information, especially business or other sensitive information, is always a good thing. It's unfortunate that perhaps the settings that were enabled might have been a bit too aggressive in your example, since your legitimate business email was not delivered immediately.

MCC: So I should lick my wounds and praise the vigilance of security improvements over recent years?

FTI™ CONSULTING | TECHNOLOGY

Kelly: Perhaps. Depending on the settings deployed by the system administrator, one feature that Office 365 offers for Exchange Online (Outlook) is flagging communication from a sender you have not previously communicated with. The end-user can then add the address to their safe senders list, preventing any future delivery restriction.

MCC: So they've anticipated these kinds of issues and given you a way to avoid derailing legitimate business communications.

Kelly: Yes. Each organization has their own tolerance for risk as it relates to incoming mail, so many of these features are enabled and configured by the enterprise client. It's not one-size-fits-all with Microsoft. They do give their clients the opportunity to configure certain aspects of the software to suit their organization's needs.

MCC: In-house lawyers in companies that may be making changes to their software – should these legal teams be involved? Should they be concerned about changes like this that their company may be undergoing?

Kelly: Being a former in-house e-discovery guy, I always think it's very important that Legal – specifically litigation or dispute resolution, whatever you might call it – have a seat at the table whenever there's any sort of organizational change that impacts records or information management, especially when it relates to technology as critical as your email system. It's also an area of opportunity for legal teams to reevaluate their e-discovery and information governance programs.

MCC: Let's say some of our readers agree with you, but they weren't invited to have a seat at the table. What would be some of the arguments a legal department could make to ensure that they are part of the process next time?

Kelly: Risk is the clearest argument. And efficiency and defensibility, especially if your organization has any sort of litigation portfolio. The litigation team needs to understand the messaging system that the organization utilizes: whether or not journaling is turned on, for example. These are all critical decisions as they relate to discovery, so I would recommend probably a top-to-top approach. Maybe the chief of litigation reaches out directly to the head of IT and just makes it known that they expect that a representative from their department is going to be involved in the project and considered a key stakeholder.

MCC: Let's say a legal team at a company isn't involved from the very start. Does that preclude them from weighing in later?

Kelly: The disadvantage there is that you're trying to change the tires on a moving car at that point. But the in-house folks need to do their best to protect the organization from risk, and certainly from the potential spoliation of any evidence. Even if the migration project is "off to the races," so to speak, it's important that they involve themselves and course-correct, if necessary. Additionally, it's an opportunity for the legal team to take a step back and take a holistic look at their e-discovery program – see if there are any changes that they can make to increase efficiency and reduce costs.

MCC: You talked about e-discovery, document data preservation, and everything related to litigation. Are there other areas that they should be particularly mindful of, and are you seeing them review their entire systems as they prepare for this kind of change?

Kelly: I think the most obvious of the areas where an implementation of Office 365 lends itself are records management and information governance. It's a good time for an organization to evaluate what their retention schedule is and whether or not they need to make changes. Similarly, they will need to evaluate (and make necessary changes to) their information governance policy, to account for the fact that there is sensitive data being stored in the cloud.

MCC: And if they don't have policies …

Kelly: It would be a good time to start writing them, and to get some good cross-functional collaboration between legal, information technology, records, and information management and compliance, to make sure that the organization has a solid information governance policy and plan in place.

T. Sean Kelly *is a senior director within FTI Technology's information governance and compliance services practice. He advises clients on all aspects of e-discovery and information governance, with a particular focus on developing and implementing legal hold processes and technology as well as assessing the legal impacts of migrating to Microsoft Office 365. He can be reached at Sean.Kelly@FTIConsulting.com.*