LAW PRACTICE MANAGEMENT

The Next Wave of Security

By Brian Podolsky

Brian Podolsky leads the Enterprise Content Management (ECM) Practice Group in the New York office of Kraft & Kennedy, Inc. He has extensive experience implementing and supporting Microsoft Office, iManage, NetDocuments, OpenText eDOCS, and Worldox document management systems, as well as third-party integrated add-ons to these systems. He also drives Kraft Kennedy's research on the latest ECM technologies including email management, enterprise collaboration and search, and provides guidance and best practice standards to clients implementing ECM solutions.

It happens all the time. Every year clients seem to want heightened security from their legal representation. New technology and products promise to meet all your security needs, but then clients knock you back with a new wave of even newer security policy demands. It can be daunting both for attorneys and their firms' IT and risk managers.

Years ago, for example, the firewall was the first security barrier most firms deployed. Firms could stay safe by allowing only certain activity (for example, inbound email and Citrix remote access) into the network. Today, however, malware and phishing from emails often defeat firewalls. This has led firms to invest in email hygiene engines such as Mimecast. Unfortunately, hackers always seem to be one step ahead of these solutions, so they are not foolproof. Moreover, firewalls and email hygiene scanners do nothing to protect firms from internal threats.

Anticipating the future demands of clients is the key to ensuring a safe enterprise. It can also lead to a prosperous enterprise if you can quickly prove you can answer a security audit completely and to the client's satisfaction.

The Threat Within

To control access within the internal network, firms implement identity-based access lists and content-based ethical walls. The idea is simple. Certain users have permissions to particular areas of their computers and networks. The problem with this solution is that it requires an extremely strong password policy to ensure that credentials are not stolen or shared. Weak passwords can be hacked relatively easily by malicious scripts.

Attorneys are sometimes required to use complex passwords, but many take the highly inadvisable step of writing them down on a Post-It stuck to their desks or monitors. It's also common for a partner to provide login information to an associate or administrative assistant. Common, but still a major no-no. Additionally, attorneys and staff are often the targets of email phishing campaigns, where a hacker spoofs the email address of an IT admin, making it seem like IT is asking a user for their credentials to troubleshoot a computer issue. Never send your password to anyone over email.

With ethical walls, certain content within a document management system (DMS) or elsewhere can be restricted such that only particular users know it even exists. The problem here, however, is that the method relies on proper filing of the material. A secure document can accidentally be saved into a public matter, and *poof*, it's not secure when an attorney thought it was.

The one thing all these security caveats have in common is they involve you, the attorney. The individual user is the hidden riptide that can pull a firm into the sea of data breaches. You don't see it, but it's there, it's dangerous, and it's a killer. Sometimes the intent is malicious, but usually it's not. The results are the same, and they can be costly. If confidential data leaves the walls of the firm and gets into the wrong hands, the firm can suffer major losses to its data, reputation, and finances.

Security to the Rescue

There are several new technologies and philosophies gaining steam in the legal industry to meet the latest security requirements. First is a shift from an optimistic to a pessimistic security model. In other words, rather than assuming that a document should be publicly available to the entire firm by default, the security is instead granted on a "need-to-know" basis. The thought process behind this is that the fewer documents exposed to the entire firm, the lower the risk of content being shared inappropriately. While this may make it tougher for employees to find relevant documents, firms shouldn't shy away from the "need-to-know" security model.

As Keith Lipman notes in his July 2017 article *Knowledge Management in the Age of Need to Know Security*,[1] firms can track additional metadata for the matter into a matter profile. With information such as matter type, area of law, tags, deal/settlement amounts, court, jurisdiction, or industry saved into matter profiles, attorneys can determine which matter or responsible attorney to contact and can obtain the relevant information they need.

Next, major legal vendors are beginning to provide solutions that bring Digital Rights Management (DRM) technology to law firms. We've seen DRM technology in consumer products for years. It's the reason you couldn't copy music from certain CDs and why you could only use Keurig coffee pods in Keurig machines. Over the past few years several technology vendors have brought DRM to electronic documents and files. The process works by essentially attaching the electronic equivalent of a physical string to the document at all times, no matter where the document lives, so you can always have a connection to the document. The string checks and verifies that the person attempting to access the document has the proper permissions to do so. At any point, you can pull the string and take access away from the recipient.

The challenge with DRM has always been ease of use, both when sharing and collaborating on files. Without going out of the way, can an attorney easily secure a document? Is it straightforward for the recipient to view or open a document? Vendors have tried for years without much success. Some products required program wrappers around the file, meaning that the recipient had to install special software to view and edit the file. Others required viewing within a web browser only. Understandably, none of these workflows have been deemed acceptable in the legal workplace.

> The challenge with DRM has always been ease of use, both when sharing and collaborating on files.

The proper solution should be seamless and integrated into both the Windows desktop environment and the DMS. Recently, two products are showing signs of breaking the usability barrier and integrating with the legal DMS. Litera IRM and Seclore Rights Management are integrating with major DMS players in the market. Each offers a different DRM engine, with Litera leveraging Microsoft's Azure Rights Management and Seclore with its own proprietary policy engine. DMS vendors may look to bring this technology within their systems as well to ensure security of firm work product both inside and outside the confines of the DMS.

Finally, with security audits and assessments growing more and more demanding, some legal vendors are going right to the source and designing their systems to meet the latest requirements of these audits. It started as encryption in transit, but has evolved to encryption at rest and now encryption in use. NetDocuments, for instance, has been spending time and effort on meeting the demands of the JP Morgan Outside Counsel Manual. Once it does, it will be compliant with HIPAA, SEC and FINRA, SOC2 Type 2, and SOC 2+ regulations. The idea is if it's good enough for JP Morgan, it should be good enough for law firms. It's a solid theory.

Law firms need to see the next wave coming to avoid getting blindsided. By being proactive, firms can protect themselves from malicious actors and from themselves. ■

[1] 3 Geeks and a Law Blog, July 7, 2017, www.geeklawblog.com/2017/07/knowledge-management-in-age-of-need-to.html.