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 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.

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 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.
secure document can accidentally be saved into a public matter, and proof, 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.

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.

By being proactive, firms can protect themselves from malicious actors and coming to avoid getting blindsided. 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.