mimecast®
unified email management

THE CLIENT MANDATE ON SECURITY

Like most other organizations, law firms face new challenges every day when protecting their confidential information from accidental and deliberate data leaks. Unlike many other organizations, however, law firms must also protect their clients' confidential information. Law firms have long been required to secure some private information due to legal and regulatory requirements. Now corporate law departments, worried about the security of their own data that resides with their outside counsel, have started to scrutinize and audit their law firms' information security policies and technologies.

CORPORATE COUNSEL ARE CONCERNED

Clients have a host of worries around the security measures of their law firms, and for good reason. In addition to regulatory requirements, a breach can allow extraordinarily sensitive and strategically important business information to fall into the wrong hands. At *Corporate Counsel's* recent 25th Annual General Counsel Conference, Bank of America Merrill Lynch Assistant General Counsel Richard Borden discussed how the Office of the Comptroller of the Currency has raised concerns about data security at law firms. "They are coming down on us about security at law firms. So we have no choice but to check the information security and to audit—to actually audit—the information security of our law firms that have confidential information. We spend a lot of money and use a lot of law firms, so this is casting a very wide net," said Borden at the conference.[1]

[1] Catherine Dunn, "Outside Law Firm Cybersecurity Under Scrutiny," *Corporate Counsel*, June 6, 2013. http://www.law.com/corporatecounsel/PubArticleCC.jsp?id=1202603020503

As part of the audit, the nation's second-largest bank asks its law firms to demonstrate that they have an information security plan in place, and that it is being followed. The bank also has its own experts test law firms' information security systems. "It's been really interesting dealing with the law firms, because they're not ready," added Borden. "Some of them are, I should say, but there are many that aren't. And it actually does pose a threat."

DATA LEAK PREVENTION

Many law firms rely on traditional security protocols, which generally do a good job of blocking intrusive threats for data that sits comfortably behind firewalls. However, traditional security protocols often fail to maintain the data security of outbound emails. According to an eMedia survey commissioned by Mimecast[2], 94% of IT managers said they had no way of preventing confidential information from leaving their network. While some of this is caused by technological limitations, much is due to human error, such as senders inadvertently hitting "reply all" on an email.

In order to minimize the chances of confidential information being sent outside the organization, law firms should develop a "data leak protection" (DLP) plan. The approach should be holistic, and the different aspects should reinforce each other. By taking a cohesive approach to data leak prevention, law firms can address client concerns, minimize risk and improve compliance. This should not be considered just an IT problem. This involves the entire firm.

The DLP plan should include:

- **ENCRYPTION** Encrypting data is a key part of keeping it secure. Otherwise, one email with a highly sensitive document attachment can leave a client's most important information open to hacking or theft.
- **EMAIL HYGIENE** Email represents a particularly vulnerable area when it comes to keeping data secure. Proper email hygiene will alleviate many of these issues. A thorough approach should involve technologies to address spam, phishing and malware. Along with incoming threats, firms also need to understand and address the vulnerability of outgoing replies and links.
- **LARGE FILE TRANSFER** DLP-consistent email protocols only work if all email is sent from the organization's systems. These protocols too often include file-size limitations that are inconsistent with the needs of legal professionals. An effective DLP system must account for the need to send large files in order to ensure consistent enforcement of content policies.
- **DETECTION OF EMAIL LOSS** Law firms need to know when email and other data have been lost, and they also need to know how to respond to these types of losses. A policy to detect and address email loss should include appropriate technologies and responses that fit the needs of their attorneys, staff and clients.
- **INVESTIGATIONS** When data is lost, deleted or compromised—either deliberately or accidently—firms need to investigate immediately. The investigation should take a big-picture approach in order to understand the context of the loss, what data was involved, how sensitive the data was and the players involved. Firms need to determine whether the loss was due to human error, technological failings or both.

  The DLP investigative approach and systems must be integrated with the firm's other systems that monitor governance, compliance and risk management. By integrating systems, the firm can better identify areas of weakness and maintain the integrity of evidence throughout the investigation.
- **CORRECTIVE BEHAVIOR** Since many security breaches are accidental, law firms need to carefully think through their approaches towards training, enforcing policies and reprimanding attorneys and staff who break these rules.

WORK-AROUND WORKERS

Most law firms have diligently created official email policies and structures, which some attorneys and staff choose to ignore. Attorneys and staff are often comfortable melding their work and personal lives and don't think twice about using personal email accounts such as Gmail and other mechanisms to send work documents.[3] Attorneys and staff may be unaware of the security risks or frustrated with the

2 James Blake, Ph.D., "The Critical Role of Data Loss Prevention in Governance, Risk and Compliance." http://www.datamountain.com/files/The_Critical_Role_of_Data_Loss_Prevention_in_Governance_Risk_and_Compliance.pdf

3 For a more detailed discussion of "work-around workers," download the Mimecast Research paper "Generation Gmail: How businesses can bring them back into the fold" at http://www.mimecast.com/Resources/Whitepapers/Dates/2011/3/Generation-Gmail-Report/

outdated technology or restrictions on mailbox or file sizes. With the proliferation of personal mobile devices and the pressure to respond quickly and during off-hours to clients, attorneys and staff often find they have easier access to personal email accounts than work-issued ones. Law firm partners, especially, have a reputation for being "above" their own firm policies, especially when they can make an argument that they are serving the client.

For those in the legal sphere, the ability to send large files quickly is an important consideration. When outside counsel need to send a file that exceeds the firm's limits on size, their response is often to find a way around the policy. Some will use home-based systems that may have higher limits, such as Gmail. Others may turn to cheap commercially available systems designed to store and move large files, such a Dropbox. However, Dropbox and other services may not be up to security standards, and files sent through them may not only be hacked or lost, but the firm has no control over the files once it leaves the official systems.

Law firms can take several steps to bring these work-around workers back to official, secure communications channels.

The first step is to develop more user-friendly email policies, rather than trying to force attorneys and staff to toe the line with systems that are less than optimal. Firms need to understand what the frustrations are, why people use work-around solutions and what they want to see with their email systems. Keep an eye on the objective, which is security, but understand that an overly restrictive policy is likely counterproductive as the same tactics workers employ to circumvent file-size limits also circumvent the organization's DLP systems.

The **second step** is to educate attorneys and staff about the risks involved and the need to keep data secure by using the firm's email systems to send all work-related emails.

For the **third step**, firms need to develop email tools that obviate the need for a workaround. Work email should be accessible and reliable, not locked behind firewalls. This may require firms to figure out how to let attorneys and staff access their business email on their smartphones just as quickly as their Gmail account. Email in-boxes should also be big enough that no one needs to worry about going over storage capacities and there should be DLP-compliant tools for sending large files securely so no one is tempted to use services like Dropbox.

SECURING ARCHIVED EMAIL

At many law firms, attorneys and staff use their email servers as a de facto storage mechanism for content and filing. This leaves data that can be disorganized, repetitive and doesn't get backed up. Email archiving is a starting point, but a comprehensive file archiving system, which encompasses all the of firm's content, represents a better model rather than a piecemeal approach such as email archiving. Through file archiving, records retention policies can be better implemented and firms can more thoroughly track and control files.

Since files tend to be less concentrated than emails and may be scattered on a myriad servers, desktops and laptops, a file archiving project is an ambitious undertaking. The trend towards "BYOD," or Bring Your Own Device, has significantly increased the number of types and places where files can reside.

Even when files are concentrated on a server that is regularly backed up, firms rarely actually archive the content of those files. That means most firms need to actually look at each file individually to determine whether it is confidential, strategically important or worthless. Even when important files have been identified, firm don't usually track and control them for future use.

Along with security risks involved with the use of Dropbox and other file sharing technology, file archiving becomes even more challenging when attorneys and staff turn to these tools. Law firms have no way to control, monitor or back up the data that moves through these tools.

When researching file archiving options, law firms should look for several critical functionalities. These include:

- **CONTROL** Law firms need to be able to determine when files must be held in place or moved to a centralized repository for further processing or review. This functionality should extend to both workflow processes and technology.
- **TRACKING** The file archiving system must also be able to keep tabs on files across the entire lifecycle. This includes knowing who can access the files, where they are sent, where they are stored, how they are modified and other information.

- **CLASSIFICATION** Not all files are created equal, and the right archiving solution will help to rank which ones are most important. Law firms in particular need to know which files contain highly sensitive and confidential information that must never leave the firm without being encrypted or secured in some other way.[4]

QUESTIONS TO ASK PROVIDERS

Along with internal policies and procedures around email usage and file archiving, law firms must work closely with their communications vendors to ensure data security. Without a trusted provider who closely monitors and manages security, the best internal procedures may not be sufficient. Here are some questions that law firms should ask their providers:

— What type of physical and virtual security protects the data centers and the information that resides within them?

— What type of backup procedures and business continuity planning are in place?

— In what jurisdiction does the data reside?

— Who has access to the firm's data and email?

— How do connections to and from the system work?

— What certifications and screenings are in place for the provider and its employees?

As businesses become more concerned about the security of their data, law firms must respond. A data security breach cannot only destroy client relationships. It can lead to bad publicity and legal and regulatory problems. In order to minimize that possibility, law firms need to understand their vulnerabilities that people and technology bring, and work to eliminate them.

How Mimecast Helps Firms Meet Client Obligations

At Mimecast (www.mimecast.com), we understand the risks that law firms, businesses and other organizations face when data is left vulnerable. Mimecast is a Software as a Service (SaaS) - or cloud - provider that delivers an email management solution as a single service that helps firms slash on-premise email storage requirements, ensure complete email availability, email security and email compliance, while providing services to help attorneys and staff get more from their email. We call it "Unified Email Management".

We're continuously processing email messages across our customers' millions of mailboxes, and we store petabytes of email data for customers who archive with us. This is a huge responsibility, and one which we take very seriously: Our customers trust us as appropriate custodians for their email data. As such, we go to great lengths to protect customer data, to ensure confidentiality, availability and integrity of data and the systems that process it. Our internal controls and support have won us industry recognition, as well as allowed Mimecast to earn certifications such as ISO 27001 which demonstrate the extent to which we are committed to Information Security.

We deliver cloud-based email management for Microsoft Exchange, including archiving, continuity and security. By unifying disparate and fragmented email environments into one holistic solution that is always available from the cloud, Mimecast minimizes risk and reduces cost and complexity, while providing total end-to-end control of email with these benefits.

4 For a more detailed understanding of file archiving, download the Osterman Research Report "The Importance of File Archiving" at http://www.mimecast.com/Resources/Whitepapers/Dates/2013/6/The-Importance-of-File-Archiving/