By Alvin S. Tedjamulia and Michael S. Kraft

Are the Firms Who Represent You Ready?

Now, more than ever, it is essential for organizations to work with law firms that effectively safeguard their documents against ever-evolving threats. Recent high-profile data breaches at international firms have led companies to increase scrutiny of their outside counsel's cybersecurity. International banks, major corporations, and government agencies are increasingly vetting the internal controls and security practices of legal document systems and requiring extensive disclosures on compliance and information governance practices.

Below we discuss the challenges and potential solutions of storing and sending documents to help you consider the security measures that your outside counsel offers.

Encryption Requirements

Taking into account the advances in cryptography in modern document management systems (DMS) and the increased necessity for encryption to secure documents, it would be irresponsible to hire law firms that continue (1) storing and (2) moving documents in internal networks in clear text format.

Encryption at Rest

Sensitive company information is at risk when it is left unencrypted at rest (that is, in storage). Surprisingly, many law firms today still have not implemented basic at-rest encryption in their traditional DMS due to cost, complexity, and lack of native support for encryption in traditional systems.

A limited number of firms have implemented this kind of encryption in a traditional, on-premises DMS. Many of these implementations, however, are based on ineffective hardware encryption methodologies (self-encrypting disks) or file system encryption. These methods are inadequate not only because they do not protect data from internal IT staff, but also because all internal network traffic between the DMS and the storage remains in clear text. The only effective cryptography method is application-based encryption. Security-conscious financial institutions are now very explicit in this particular requirement.

Many clients now require their law firms to store cryptographic keys in a hardware security module (HSM), which is a purpose-built, advanced security container for cypher key storage. Major banks are not only encouraging HSM cryptography, but also requesting that the HSM be accredited to the Federal Information Processing Standard called FIPS 140-2 Level 3 with tamper detection circuitry. Notice the "Level 3" explicit requirement.

Law firms should be aware that modern document systems today do provide HSM-based encryption with tamper detection circuitry for full encryption at-rest and in-transit within the internal network, capable of satisfying the strictest regulations.

Granular Cryptography

Instead of having a single crypto key for all content, a secure environment has a unique key for each matter and for each specific time period, implemented through key rotation. Granular cryptography protects against the risk of a total security breach in the event that a single crypto key is compromised. Today, modern document technologies can provide law firms with granular cryptography, supporting a unique AES-256 crypto key for each document, which is further encrypted by a unique key for each matter, and another unique key for each time period.

Entropic Encryption

NIST (National Institute of Standards & Technology) strongly recommends against generating encryption keys via weak software algorithms (referred to as pseudo-random number generators). Instead, NIST urges the use of strong technologies that rely on random, entropic natural phenomena, such as the photons in a laser beam.

Encryption strength is critical in defending against attacks by nations. Government-sponsored hacks have prodigious computing power and are easily able to break into documents with weak encryption keys through the use of brute-force trial and error. Secure cloud technologies provide entropic encryption using quantum physics technology for randomization as a main defense against such threats, satisfying the highest security standards.

Custody over Cryptographic Keys

International banks are demanding that firms obtain custody over encryption keys to stop their service providers from disclosing documents upon receipt of a subpoena. Furthermore, banks and other companies may soon want custody over such encryption keys themselves. "Silent subpoenas" issued against the service provider represent the greatest risk. They mandate document production and prohibit the service provider from disclosing

■ Alvin S. Tedjamulia, is a co-founder of NetDocuments and serves as its Chief Technology Officer. He is in charge of strategic planning, "cloud" engineering, R&D, and SaaS software development, as well as datacenter operations in Arizona, Utah, Nevada, London, Wales, Harrogate (UK), Sydney and Perth, Australia. Michael S. Kraft is co-founder and the general counsel of Kraft & Kennedy, Inc., a consulting and systems integration firm formed in 1988. He is a member of the Bar Association of the City of New York, the New York State Bar Association, the American Bar Association, the Association of Corporate Counsel, and DRI.

the silent subpoena to the client. Cloud technology has evolved to the level of dual encryption custody, in which two separate organizations hold a unique entropic cypher key (or half of the key), requiring both organizations to work cooperatively to respond to subpoenas, rendering unilateral actions impotent.

Protection Against Self

The highest level of risk in any organization is posed by its own internal staff. Wall Street firms, for example, are asking law firms to eliminate the risk posed by their internal staff, especially situations in which IT staff having indiscriminate access to the firm's documents. This requirement of "protection against self" will be more pervasive in the near future. Mitigation practices, such as segregation of duties and "need to know basis," can help. These minimize the risk of internal nefarious actions that require collusion among multiple people.

For classified documents, however, segregation of duties is not good enough, and some clients are increasingly requesting complete protection against internal staff acting under collusion. Law firms must anticipate this upcoming security standard and realize the near impossibility of implementing such protection on their own. How do you effectively protect against yourself if you're in control of the system?

A viable solution for protection against the firm's own IT staff is to deploy a technology with multi-custody entropic cryptography.

Datacenter Best Practices

The following requirements are often raised in RFPs and audits:

- **Removable Media Disablement** – This requirement specifies that IT workstations accessing the datacenters directly must have removable media (DVD, USB, memory stick) automatically disabled during the login session to prevent the downloading of unauthorized sensitive data to personal computers.
- **Defective Media Retention** – This requirement prohibits defective disks in the datacenter from being recycled and replaced by the manufacturer. Defective media must be degaussed and destroyed.
- **Audit Log Isolation** – All computer logs, whether generated by the operating system, applications, network devices, or security modules, must be managed by a third-party organization to prevent the internal IT staff from maliciously altering log contents and concealing their footsteps.

Fortunately, the most advanced document services meet the above requirements and were designed with such best practices built-in.

Perimeter Defense

Perimeter defense must encompass distributed denial of service (DDoS), web application firewalls (WAF), threat management gateways (for IPS and IDS protection), strong security policies, and best practices for managing ingress. The presence of a simple firewall is not enough. DDoS, for example, is a complex problem. Facing an average DDoS attack intensity of 48 gigabits per second, an internet line of only 1 gigabit per second will be flooded with "garbage" beyond the ability of the DDoS technology to inspect the internet packets. The inadequacy of most firms to have adequate perimeter defense is a serious concern. Fortunately, modern cloud services for DMS are well equipped for DDoS and perimeter defenses.

End-User Protection

According to the 2016 ILTA Large Firm CIO Cloud Security Survey, firm CIOs' top front-end security concerns include data leakage from end users circumventing their DMS (81 percent), nonadherence to internal security policies or procedures (76 percent), and compromised passwords or hacked credentials (52 percent).

Your law firm should use technologies that not only improve the safeguarding of client data from a back-end standpoint, but also from the front-end or end-user standpoint through the enforcement of 1) strong passwords and password rotation through federated identity integration; 2) two-factor authentication on all devices, especially mobile devices; 3) restricted access based on devices and IP addresses; 4) validated audit trails and history logs; and 5) access control restrictions for externalizing or emailing specific documents. Further, sensitive files should either be prohibited from being externalized through DLP, or strong controls must be in place such as remote wipe, device authorization, and blocking. For mobile device document editing, security restrictions must be permitted for Microsoft Office applications to read and write files directly to the document management system, thereby eliminating the security risk of having documents locally stored, even temporarily, on tablets or phones, or on Microsoft OneDrive or Google Drive.

Expect firms to adopt a pessimistic security model for document access control and restrict every user's access to only those matters that he or she is working on or the matters within the particular practice group. They should never have the ability to access everything in the firm. These end-user and device security controls must be built into the secured DMS to ensure comprehensive but seamless security. Modern document services focusing on end-user security have the above requirements readily available.

Recommendations

Look for firms that have strong, modern security offerings. Leading firms embrace modern technology platforms with security and compliance in the primary design architecture. This creates a clear differentiation in security capabilities between firms with legacy, unencrypted, or inadequately encrypted DMS and firms with entropic, granular, HSM-based DMS that provide protection against self.

Large financial institutions are leading the way in asking their attorneys to meet compliance demands and undergo security audit reinforcement. Many vendors offer products today that anticipate this demand. Cloud-based vendors, especially, are providing entropic multi-custody cryptography, best practices, end-user security, strong perimeter defense, and protection against self. Eventually, firms that delayed adopting high security standards will find themselves scrambling to improve their platforms, especially when breaches become more publicized and costly.

To participate in a roundtable discussion on this topic, please contact info@kraftkennedy.com.