Client Security Audits:
IS YOUR LAW FIRM READY?

netdocuments®

Client Security Audits: IS YOUR LAW FIRM READY?

Alvin Tedjamulia, Chief Technology Officer, NetDocuments
Michael Kraft, General Counsel & Founder, Kraft & Kennedy

Recent high-profile data breaches at international firms have led companies to increase scrutiny of their outside counsels' 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. Now, more than ever, it is essential for law firms to safeguard their clients' documents against ever-evolving threats.

This white paper illustrates some of the most challenging security issues modern law firms must address and the available solutions from modern technologies. We encourage and invite the legal community to participate in an open discussion about security challenges and potential solutions in today's demanding world of legal document compliance.

Below are examples of challenging document security issues and potential solutions. Note that cyber security progress, like all technology innovation, happens more rapidly in the cloud than on premises. While issues such as those listed below can be addressed one time in the cloud, they must be corrected individually in on-premises deployments.

ENCRYPTION REQUIREMENTS

Taking into account the advances in cryptography in modern Document Management Systems (DMS) and clients' increased demand for encryption to secure their documents, it would be irresponsible for law firms to continue (1) storing and (2) moving documents in internal networks in clear text format.

- **Encryption at Rest** – Sensitive client 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.

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.

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 per matter and per specific time period, implemented through key rotation. Granular cryptography protects against the risk of a total security breach should a single crypto key be compromised. Modern document technologies can today provide law firms with granular cryptography supporting a unique AES-256 crypto key per document, which is further encrypted by a unique key per matter, and another unique key per 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 via 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 will 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 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 are asking law firms to eliminate the risk of their internal staff, especially 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 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

These questions 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 NetDocuments Large Firm CIO Cloud Security Survey, firm CIOs top front-end security concerns include data leakage from end users circumventing their DMS (81%), non-adherence to internal security policies/procedures (76%), and compromised passwords or hacked credentials (52%).

Organizations want their law firms to 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 for robust governance controls such as remote wipe, device authorization, and blocking. For mobile device document editing, security restrictions must be permitted for Microsoft Office applications to directly read and write files 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.

Clients expect firms to adopt a pessimistic security model for document access control and restrict every user to accessing 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 DM solution to ensure comprehensive but seamless security. Modern document services focusing on end-user security have the above requirements readily available.

SUMMARY & PREDICTION

Law firms and corporate legal departments are under significant pressure to do more with less and to be more agile with their technologies. Such pressures are even more evident when it comes to security and compliance.

Based on our collective observations and work with numerous senior law firm and corporate security and information governance professionals, there are four phases in the current document legal compliance space:

- **Phase 1:** Large financial institutions pass regulated compliance demands to law firms with strict security audit enforcement. Phase 1 is a strong definitive state ment that security is a primary concern and will be required in the legal industry.

- **Phase 2:** Vendors, especially those that are cloud-based, provide entropic multi-custody cryptography, best practices, end-user security, strong perimeter defense, and protection against self. This creates the capability of meeting the fiduciary responsibility for Firms to safeguard documents commensurate with their clients' expectations. In Phase 2, security consciousness migrates from the major banks and government institutions to the corporate world in general.

- **Phase 3:** 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 DM systems and firms with entropic, granular, HSM-based DM systems that provide protection against self.

- **Phase 4:** Clients demonstrate bias in favor of firms that have strong, modern security offerings. Firms that delayed adopting high security standards find themselves scrambling to improve their platforms, especially when breaches become more publicized.

INVITATION

Kraft & Kennedy and NetDocuments are collaborating with a number of firms who are interested in discussing best practices and potential solutions around the overwhelming challenge of client-driven audits and cyber security. If you or your colleagues would like to be part of such discussions and regional executive meetings, please let us know as we are in the early stages of this initiative.

Contact Alvin Tedjamulia, alvin@netdocuments.com
or Michael Kraft, kraft@kraftkennedy.com for more details.

netdocuments®

nd netdocuments