SECURITY AUDITS:

Prepare Your Firm to Meet Your Current and Potential Client Requirements

netdocuments® | Kraft Kennedy

AUTHORED BY

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

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 global and smaller firms have led companies to increase scrutiny of their outside counsels' cybersecurity. International banks, major corporations, and government agencies are focused on 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.

It is important to understand that modern document platforms are cloud-based, offering a single service worldwide. This gives Firms and Legal Departments that adopt the cloud platform a quick solution to remedy all the extensive security issues described in this article. Inheritable governance with 3rd party attestations and certifications were not possible with prior document technologies based on on-premises or hosted cloud solutions, because every on-premises implementation requires its own physical deployment and each hosted cloud service requires its own virtual implementation with its own specific private URL. A true SaaS multi-tenant cloud service, with a single global "one cloud" architecture, provides the significant advantages of auto-inheritable security, governance, and compliance benefits.

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 document management systems 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, usually implemented with a unique encryption key for each digital file. Security conscious financial institutions are now very explicit in demanding this particular security control.

A critical aspect of encryption is ability to store the encryption keys in key-vault systems (HSMs) so the keys cannot be accessed by the software engineering team (the cloud vendor) or the security system administrators from the vendor or from the Firm.

KEY STORAGE REQUIREMENTS: 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. Microsoft names its HSM in the cloud as Azure Key-Vault. Major banks are not only encouraging HSM cryptography, but also requiring 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 .

A critical aspect of encryption is ability to store the encryption keys in key-vault systems (HSMs) so the keys cannot be accessed by the software engineering team (the cloud vendor) or the security system administrators from the vendor or from the Firm. The concept is to ensure that not even the security caretakers can breach security. In fact, the cloud vendor and the Firm security administrators are the very individuals who can cause the most damaging security breaches. FIPS 140-2 Level 3 is the security standard which ensures that the key-vault (HSM) is tamper-resistant, meaning that not even the software which drives the key-vault can remove the security keys out of the vault (HSM) itself (keys are held captive in the HSM, providing the highest level of key security).

Achieving Level-3 is difficult. Those simply using Microsoft Azure Key Vault for key storage as a multi-tenant HSM only archive FIPS-140-2 Level 2 (not level 3). There is a tremendous gap in security between

Level 2 and Level 3 (Banks requires Law Firms to have Level 3). Level 2 means the key vault is tamper-evident, meaning a breach is detected and logged. Level 3 means that the key vault is tamper-resistant, meaning that key removal is not possible, because the keys inside the HSM are further encrypted by the HSM hardware crypto processor. Level 2 detects the breach; Level 3 prevents the breach.

Law Firms should be aware that modern document systems today do provide HSM-based encryption with tamper resistant circuitry for full encryption at-rest, in-transit, and "in-use" within the internal network, making these solutions capable of satisfying the strictest regulations. Encryption in-use means that keys stored in the HSM (key-vault) can only be used inside the HSM, but cannot be removed from the key-vault, ensuring protection against self.

GRANULAR CRYPTOGRAPHY: Instead of having a single crypto key for all content, a secure environment also has a unique key per matter and per specific time period. Granular cryptography protects against the risk of a total security breach should a single crypto key be compromised. Sophisticated document technologies can provide law firms with granular cryptography by supporting a unique AES-256 crypto key per document, with each unique document key further encrypted by a unique key per matter and by another unique key per time period.

Granular cryptography also provides a way a Firm could block a subpoena to its cloud vendor, since the Firm manages one level of the cryptographic keys. Because there is a crypto key per matter, the Firm could disable any matter key, and all access to that matter by users and the cloud vendor would be immediately stopped. Without granular cryptography, a Firm would have one single key for the whole document library, meaning that keys to a particular matter could not be revoked, because the single library key would stop access not just to that matter, but to the whole document management library.

DMS systems that have unique encryption per document and a single key for the whole library fall short in providing this important level of targeted protection. Advanced cloud systems that have unique encryption per document and unique keys per matter offer advanced access protection.

ENTROPIC ENCRYPTION: The National Institute of Standards & Technology (NIST) strongly recommends *against* generating encryption keys via software algorithms (referred to as pseudo-random number generators). Instead, NIST urges the use of strong technologies that rely on true random number generation based on natural phenomena instead of weak software key generation (pseudo random) methodology.

Encryption strength is critical in defending against attacks by nations or other sophisticated hackers.

Encryption strength is critical in defending against attacks by nations or other sophisticated hackers. 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 true randomization (full entropy) as a main defense against such threats, satisfying the highest security standards.

CUSTODY OVER CRYPTOGRAPHIC KEYS: International banks and other sophisticated clients are demanding that firms obtain custody over encryption keys used to secure client documents to prevent the firm's service providers from disclosing documents upon receipt of a subpoena issued to the provider. Furthermore, these banks and other companies may soon want custody over such encryption keys themselves. These actions are being driven by a growing concern over "silent subpoenas" potentially being issued to the service provider. A silent subpoena mandates document production and prohibits the service provider from disclosing the existence or content of the subpoena to the firm. In response to this evolving challenge, cloud technology offers dual encryption custody, in which two separate organizations each hold a unique entropic cypher key (or half of the key), so provider and customer can work cooperatively to manage data. Dual encryption technology offers firms a way to limit unilateral responses to these subpoenas by the service provider alone.

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 the firm's internal staff, especially situations in which IT staff having indiscriminate access to the firm's documents. This requirement of "protection against self" will become even more pervasive in the near future. Mitigation practices, such as segregation of duties and "need to know" limits, 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 the risk of internal staff acting in 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. This can be achieved by implementing a cryptography architecture where every document is encrypted by two cyphers: the matter key under the custody of the Firm, and a time key under the custody of the vendor. This dual-custody encryption technology, already mentioned earlier as a limitation against subpoenas, also effectively provides real "protection against self."

Data Center Best Practices

These questions are often raised in RFPs and Audits:

- **Removable Media Disablement –** This requirement specifies that IT workstations accessing the data centers 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 data center 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 into their operations.

Perimeter Defense

Perimeter defense must encompass web application firewalls (WAF), threat management gateways (for IPS and IDS protection), strong security policies, layer-7 firewalls, and best practices for managing ingress. The presence of a simple firewall is not enough. A distributed denial of service (DDoS) attack, for example, is a complex problem. If your organization is faced with an average DDoS attack intensity of 48 gigabits per second, a typical Internet line of 1 gigabit per second will be flooded with "garbage" beyond the ability of standard DDoS technology to inspect the incoming communication packets. The inadequacy of most firms to have adequate perimeter defense is a serious concern. Fortunately, modern cloud services for DMS are well equipped with enterprise-level DDoS and perimeter defenses scaled to handle even the largest and most pervasive attacks.

Law firms 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.

End-User Protection

According to the 2016 ILTA Large Firm CIO Cloud Security Survey, the top front-end security concerns for law firm CIOs 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%).

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 data loss prevention (DLP), and strong controls for mobile devices should 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 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.

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. Users should never have the ability to access everything in the firm. A scalable and easy-to-use ethical wall management service should be present in the DMS to govern the matter workspaces. These end-user and device security controls must be built into the secured DM solution to ensure comprehensive but seamless security. Modern document services that focus on end-user security have the above requirements readily available.

DATA LOSS PREVENTION (DLP): Law Firms can lose data because end-users can be careless, naïve, or malicious. Clients demand that Firms use modern technology to stop data leaks and data loss. Depending upon the sensitivity of the matter, certain end-user actions must be prohibited. Actions such as printing, downloaded, emailing, copying, or sending via DMS collaboration services should be either allowed or denied, depending upon the sensitivity of the matter.

While ACLs and Ethical Walls determine whether or not the end-user can access certain documents, they cannot determine what actions are permissible. ACLs and Ethical Walls controls access, but DLP controls actions once access is granted.

DLP integrated into the DMS provides the Firm governance over end-user actions based upon the specific data classification of the matter. Modern cloud DMS systems have a fully integrated DLP system to assure unauthorized data is not externalized accidentally or maliciously.

Certifications

Vendors can claim all sorts of capabilities for security, privacy, and governance, but unless certified by credible 3rd party audits, such claims are of little value. For this reason, cloud DMS should have built-in certifications, including ISO 27001, ISO 27017, ISO 27018, ISO 27701, Type 2 SOC 2, HIPAA High Tech, and FIPS 140-2 Level 3. Each certification or audit focuses on different security standards, and together they provide a comprehensive, independent validation of a vendor's security architecture. All such certifications should be renewed annually and should apply to the entire service, including

the vendor's organization, employees, and methodologies, and not just the host data center. Make sure that the Vendor also provides the Firm access to all related certification documents to enable easy responses to client inquiries and audits. More importantly for the Firm, these DMS certifications should be inheritable, meaning that by adopting the cloud DM, the attestations will pass through to the Firm.

Inheritance

This document reveals a tremendous amount of information regarding security technologies, methodologies, best-practices, and certifications, which are practically impossible for Firms to implement on their own. The beauty of a One-Cloud Technology implemented under a SaaS elastic multi-tenant technology is that by adopting the cloud DM platform, the Firm automatically inherits entropic dual-custody granular cryptography, security best practices, compliance certifications, end-user protection with DLP, and perimeter defense. While the security capabilities are extensive, the benefits are easily and immediately inherited upon adoption.

Recommendations

Large financial institutions are leading the way in asking their attorneys to meet compliance demands and undergo security audit reinforcement. To meet these requirements, you need to look for DMS solutions 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 DM systems with no DLP, and firms with entropic, granular, HSM-based DM systems that provide protection against self with data loss prevention and verifiable security audits.

Many vendors say they offer products that meet this demand. As you consider cloud-based vendors, carefully evaluate their services against the standards outlined in this document, and ensure the vendors you select are providing entropic multi-custody granular cryptography, best practices, end-user security with DLP, strong perimeter defense, and protection against self. Eventually firms that delay adopting high security standards – and resist using vendors which also meet those same standards - will find themselves scrambling to improve their platforms, especially when breaches become more publicized and costly.

ABOUT NETDOCUMENTS AND KRAFT KENNEDY

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.

For more details, or to request a demo, please click here.