LJN LAW JOURNAL NEWSLETTERS

LJN'S LEGAL TECH Newsletter®

An ALM Publication

Volume 32, Number 1 • May 2015

Securing a Document Review Center: A Practical Guide

By Michel Sahyoun

Much ink has been spilled in recent years about information security, hacker exploits and hardware and software products used to thwart hackers. Not a single day goes by without news pertaining to the discovery of vulnerabilities in the software we use and cherish, and to hacker exploits affecting the companies we use in our daily lives. Compromises at JP Morgan Chase, Target, Home Depot, Ebay, Adobe and Apple, to name a few, have led to the leakage of hundreds of millions of records. These infractions lead to billions of dollars of aggregated losses and can be financially devastating to an organization. A 2014 study by the Ponemon Institute, for example, puts the cost of the average data breach at $5.9 million dollars and the cost per record of a breach in the U.S. at over $200. *See*, "2014 Cost of Data Breach Study: United States (May 2014)" (http://ibm.co/1yek7Mt).

The legal industry has been a late comer to the information security frenzy, but the situation has changed over the last 18 months, driven by corporations' realization that law firms and the legal ecosystem orbiting around them has access to some of their most sensitive data. This realization triggered a series of security audits targeting law firms and, in some cases, e-discovery vendors. Corporations spend millions of dollars on information security to build a defensive dome around their data (JP Morgan, for example, announced to its shareholders that it spent $250 million on information security in 2014), and their angst about the safety of that data when it resides on third-party networks is therefore understandable.

The one discipline that is increasingly under the microscope of Chief Information Security Officers (CISO) is e-discovery, where terabytes of some of the most sensitive corporate communications leave the relative safety of the corporation's defensive perimeter and are touched by myriad legal services providers spanning the EDRM continuum. Providing the tightest security possible to every step of this process is no longer optional. Service providers must implement stringent security protocols or risk losing their largest corporate clients.

The document review industry is becoming increasingly competitive, and profit margins are often razor thin. This translates into a reluctance to invest in anything not deemed absolutely necessary for conducting the review. Information security is often the first victim of this lack of funding, making document review centers an easy target for breaches.

This article will focus on the key factors to effectively maintain data security during the document review phase of e-discovery, and in particular, securing document review centers against malicious and inadvertent data leaks.

The Inherent Risks in Document Review Centers

Document review centers raise unique security concerns for several reasons, including, but not limited to the following.

Large numbers of personnel accessing the data.

Document review projects may employ hundreds of (often) transient attorneys, and each individual poses a potential insider threat through the voluntary or accidental disclosure of data. The well-publicized data leaks caused by Pfc. Bradley Manning and Edward Snowden serve as ominous warnings of the potential damage caused by insider threats. This situation can be further exacerbated by the fact that temporary employees may not feel the same obligation to protect their employers' data, nor will they likely face the same negative consequences of doing so (harm to reputation and career growth) as permanent, longer-tenured employees.

Hundreds of endpoints accessing the data.

Document review centers are equipped with hundreds of "endpoints" (in this context, a computing hardware device that is capable of communicating on a data network, such as desktop or laptop computers, smart phones, tablets, thin clients and printers) used by attorneys and other review staff to perform their

Michel Sahyoun is chief technology officer, senior vice president, client solutions at QuisLex.

work. Each one of these endpoints constitutes a potential data tap allowing for the extrusion of the data being accessed. The larger the number of endpoints, the higher the likelihood of a breach.

Lack of funding for cybersecurity.

The document review industry is becoming increasingly competitive, and profit margins are often razor thin. This translates into a reluctance to invest in anything not deemed absolutely necessary for conducting the review. Information security is often the first victim of this lack of funding, making document review centers an easy target for breaches.

Practical Defensive Measures

In order to mitigate the security risks inherent in document review centers, a number of measures can be taken that, if properly implemented, will significantly reduce the risks of data leakage. It is important to note that these measures are in many ways interdependent and must be implemented systemically in order to create the proper security shield.

The following is a look at the critical aspects of security: personnel, physical location, end-point, network and software applications.

Personnel Security

In order to mitigate the risk of insiders (document reviewers and other support staff) serving as the source of willful or inadvertent security leaks, the following steps should be taken.

First, conduct extensive background checks, including criminal, educational, employment and references, utilizing both the internal HR department and a reputable outside agency in order to identify past occurrences of unethical behavior and assess the employee's potential for engaging in subsequent offenses. Such checks, while necessary, do not guarantee the integrity of the personnel. It is worth noting that both Pfc. Manning and contractor Snowden had elevated government security clearances that were achieved through (presumably) thorough checks.

Second, mandate that all personnel sign enforceable confidentiality agreements. Such agreements serve as a moderate deterrent and, perhaps more importantly, as a reminder of the employee's confidentiality obligations.

Third, implement information security awareness training conducted by qualified personnel with the goal to prevent personnel from being an unwitting contributor to a security breach.

Michel Sahyoun

Physical Security

Physical security helps prevent data breaches through physical means, or through a combination of physical and other technical means. When establishing a document review center, a data security team should:

1. Locate the review center in a secure building that includes a manned lobby equipped with an access control mechanism such as turnstiles.
2. Physically segregate different review projects. This will limit access to client data to only the reviewers working on a given project, and prevent the sharing of information between review teams on different projects.
3. Provide physical access to all areas of the review facility on a strict need basis. Access permissions must be reviewed periodically, preferably daily, to ensure accuracy, in particular where review personnel are temporary employees.
4. Limit access to the printing of materials relating to the review project (insofar as printing is necessary at all) and prevent the movement of paper outside each respective review area.
5. Prevent the entry of personal electronic equipment such as external drives, laptops, tablets, cameras and cell phones, which can be used to take photos of confidential information on the computer screen and help in the exfiltration of data.
6. Monitor the facility through the use of CCTV cameras. Ideally, these cameras should be viewed live by qualified personnel. This will act both as a deterrent and a means to detect any attempts to bypass the security controls.

Endpoint Security

The endpoint, which typically consists of a PC, is one of the most utilized vectors for data breaches. It is therefore essential to protect a review center's endpoints through a wide variety of measures, including:

1. Select endpoints judiciously. The use of laptops as endpoints can be problematic, especially in cases where physical security is not particularly robust. Laptops are easily portable and can be more easily stolen (along with the data they contain) than bulkier desktops. The preferred endpoint platform for document review centers is the diskless thin client, which holds no data on its own and is used merely to view, but not store, data. Thin clients also offer a much smaller "attack surface" (defined as "the set of ways in which an adversary can enter a system and potentially cause damage" by the Department of Homeland Security's NICCS) than their desktop and laptop cousins. Thin clients must still be properly secured to prevent the use of external storage devices, and must be carefully configured and audited before they are used in order to ensure that there are no loopholes or vulnerabilities that would allow the extrusion of data. For example, certain thin clients allow users to take screen shots or mount USB storage devices.
2. Provide users the minimum permissions on their endpoints neces-

sary for a reviewer to perform the work. Any additional permissions will only increase the endpoint's attack surface for both internal and external threats.

3. Block external devices or media from connecting to endpoints. This includes, but is not limited to, blocking USB ports, Bluetooth and Wi-Fi connections, and CD/DVD drives. In addition to blocking these devices, endpoints must be monitored against attempts to connect such devices, and any such attempts must generate an alarm to the information security team.
4. Utilize a constantly updated (preferably on an intraday basis) endpoint protection suite that prevents malware from running on the devices. This is particularly pertinent for desktops and laptops. Ideally, the endpoint security software should be capable of stopping threats by using behavior based heuristics in addition to relying on malware signatures.
5. Sanitize endpoints between projects. All project data must be securely wiped (and not merely deleted) at the end of each review project to prevent the disclosure of the project's data to the next set of endpoint users. This is an area where diskless thin clients have an advantage as they have no storage capacity of their own.

Network Security

Since the network is the most commonly used conduit of malware and data exfiltration, it is a vector that must be carefully secured and monitored. The following measures should be considered:

1. Segregate the center's network to limit the propagation of any breach, and to prevent one project's data from being accessed by the staff of another project. Inter-network traffic must be restricted on a network and port level.
2. Utilize a high-end next generation firewall to protect the review center's perimeter. The firewall, along with additional intrusion prevention and detection systems (IPS and IDS), will protect the network from external threats. Ensure that your perimeter devices are constantly updated with the latest definitions and most secure firmware. Audit the firewall's rules on at least a monthly basis to ensure that all rules are still valid and have the proper justification.
3. Block all network access from inside and outside the network and only allow essential traffic to and from known destinations in order to limit the network's attack surface and to prevent insider exfiltration.
4. Block all unnecessary ports, protocols, and services from the network.

Application Security

The application layer is the final layer of security that must be properly configured and protected. The following measures will ensure a secure application layer and complete the shield defending the document review center:

1. Limit applications on endpoints and servers to the absolute minimum required for an effective review. Each application is likely to have vulnerabilities, whether known or unknown, and the addition of unnecessary applications merely heightens the security risk.
2. Ensure that all remaining applications, operating systems, and firmware are patched as soon as patches are available and properly tested.
3. Ensure that any new application installed within the review center cannot be utilized for data leakage. This is especially critical for collaboration applications such as messaging or data sharing as they are meant by design to ease the spread of information.
4. Block all Web access, except to those sites that are necessary for conducting the review (*e.g.*, the review platform URL). Audit any open sites to ensure that they cannot be used for data exfiltration.
5. Utilize an e-mail gateway that intercepts any potentially malicious e-mail and ensure that the e-mail gateway is always up to date with respect to patches and firmware.
6. Block external e-mail access except to known addresses that are essential for conducting the review and have been authorized by a centralized security function. This will prevent the exfiltration of sensitive documents through e-mail. E-mail access should be granted to only those review personnel who require such access to perform their review management functions.

Security Audits

Once these security measures are in place, they must be regularly audited to ensure their efficacy. A robust audit program will consist of frequent internal audits by an audit group that is both qualified and distinct from the team that implemented the security measures, in order to prevent potential conflicts of interest when identifying lapses in adherence to security protocols. Best practice dictates a separate reporting structure for the security audit group and IT.

Additionally, periodic third-party audits that include vulnerability assessments and penetration tests (VAPT) provide a non-vested opinion of the review center's security posture. Rotating the third-party conducting the audits will reinforce the benefits of such exercises.

Conclusion

The above measures, if properly implemented, will go a long way in securing any document review center and will provide peace of mind to the clients who are entrusting some of their most sensitive data to the document review service provider. The measures described above are onerous, especially to smaller organizations, both in terms of capital and operational expenses, but they are essential in providing corporate data the level of security needed when it is being accessed outside of the relative

For more information please visit http://www.quislex.com or email info@quislex.com