Preparing for the Future of Law Firm Security

Client audits are an increasing concern to key stakeholders. Compliance issues continue to grow. Internal fears and reputational repercussions from breaches, ransomware file encryption, and related business interruptions are real. Client security audits are becoming more detailed, and requirements are expanding. Internal IT teams and external vendors are evaluating their information security postures.

by Michael Kemps

By fear or by force, law firms are being dragged into the realities of crafting and managing a secure technology environment. What does the future have in store? More firms than ever will be held to the same exacting standards as bigger firms. Firms will need to comply with client-required technologies and associated remediation. Lawyers will no longer be able to resist security measures perceived to cause an inconvenience.

While businesses in other industries are adopting innovative approaches to cybersecurity, most law firms lag behind in implementing modern information security solutions. Through associations like the International Legal Technology Association (ILTA) and the Association of Legal Administrators (ALA), leaders can look to the experiences of other firms and businesses when searching for appropriate technologies for their firms. Reviewing and addressing each of these areas within your technology environment will lay the groundwork to secure the firm and prepare you for the future.

Advanced Firewalls

Firewalls are in place to protect unwanted ports from being accessed over the internet and to log network connections traversing security boundaries. Logging should include source Internet Protocol (IP) address, destination IP address, destination port, protocol type (e.g., Transmission Control Protocol (TCP), User Datagram Protocol (UDP) and Internet Control Message Protocol (ICMP)) and date and time of the attempt. Geographic considerations should limit traffic from specific locations. An example would be allowing Remote Desktop Protocol (RDP) or virtual private network (VPN) traffic to originate only from within the United States of America.

Advanced firewalls support utilizing sensors and appropriate current signatures, identified as intrusion prevention sensors (IPSs) or intrusion detection systems (IDSs). IPS/IDS alerts typically contain the following attributes: unique identifier, date, time, priority level identifier, event description, notification sent to security team and event status.

Two-Factor Authentication

Securing account access is, in many ways, the simplest solution to locking down an environment. Numerous vendors provide cloud-based authentication solutions that utilize mobile device applications to provide secondary authentication to an Active Directory domain login. An end user connects to the network, and, after a login attempt, the mobile application prompts with a validation request. This confirmation is logged in conjunction with the login event. The idea here is not only to secure the environment from intrusion but also to match login times with other events. This could include file transfers, data exports, confidential email forwards and even malicious behavior. Nevertheless, utilizing two-factor authentication does not alleviate the need to protect, change and use complex passwords.

Directory Management, Auditing and Notification

Default operating system configurations around auditing and notification generally are insufficient. Firms should employ software and processes that produce an audit trail and notify appropriate personnel of critical events. Examples include the creation of new accounts with administrator access, large data exports or identification of Active Directory accounts not accessed within a maximum period.

Operating System and Application Patching

This might sound obvious, but it bears repeating. Applying current operating system and application patches is critical. Software vendors remediate known vulnerabilities within update periods. Missing even one critical update can expose law firms to known security risks.

Endpoint Protection

By now you undoubtedly have heard a story around ransomware infection. Traditional antivirus platforms that depend solely on virus signatures are no longer sufficient. Patterns of behavior must be monitored and logged, with unknown attempts blocked and false positive events approved. Chat applications can create more false positive results. An example is Spotify, which uses varying ports. Endpoint protection software is resistant to this kind of behavior and frequently stops it, pending approval. The priority is stopping risky behaviors before they can encrypt, relocate and delete critical files.

Encryption

Encryption is now a commonplace requirement. Assets in transit over wireless or untrusted connections commonly employ encryption mechanisms such as Secure File Transfer Protocol (SFTP), Secure Sockets Layer (SSL) or Transport Layer Security (TLS). To ensure that the versions being used are the most current to address known security vulnerabilities, SSL and TLS should use a minimum of 128-bit key strength, with 256-bit key strength preferred. Each web server involved in SSL or TLS communication should have a valid digital certificate from a trusted certificate authority (*e.g.*, Comodo or VeriSign).

Data at rest should be encrypted with at least a 256-bit key strength. Centralized management of encryption keys is critical. This includes developing a scheduled rotation and a defined process for the immediate rotation of encryption keys should a suspected or confirmed compromise occur.

Secure File Transfers

Data transferred between law firms and their clients or vendors must be accomplished through a centralized secure infrastructure. This can be enabled utilizing third-party tools if they are provided as an extension of the firm's existing enterprise. Many well-known data transfer tools that are not specific to securing client data are, in fact, not secure.

Data Leak Prevention

The leakage of intellectual property is a critical concern to law firm clients. Data leak prevention (DLP) solutions review email body and attachment content to identify and control personally identifiable information, code names and other sensitive data. Emails found to contain critical data are routed to a designated administrator for review prior to sending. Frequently, DLP tools also will employ or add encryption to outbound emails not already secured.

MICHAEL KEMPS

Michael Kemps is the founder and Chief Executive Officer at Innovative Computing Systems. He started the company in 1989 after developing relationships with several law firms that eventually became early clients. His interest in technology began when he was 13 years old and developed bulletin board systems with friends and repaired hardware and software for family and friends. Today, Michael is involved with the International Legal Technology Association and the Association of Legal Administrators, as well as several nonprofit organizations. He also is on the advisory board of a community bank. Contact Michael at mkemps@innovativecomp.com.

Each web server involved in SSL or TLS communication should have a valid digital certificate from a trusted certificate authority.

3 SECURITY TIPS TO APPLY NOW

These practical initiatives will set your firm on the path to data security right away:

1. **Password Security:** Password complexity and protection have gone to a new level with two-factor authentication. Requiring users to confirm their identities using a second means is a must for every law firm seeking to capitalize on information security advances. Also, consider implementing software that generates complex passwords and stores them for use under a single sign-in.
2. **Endpoint Security:** Antivirus software is no longer enough. Dated definitions and virus signatures cannot keep up with today's hackers. Deploy advanced endpoint protection solutions to identify and block suspicious behavior before it becomes an information security nightmare.
3. **Training:** Up-to-date, thorough information security training is key to keeping clients' data secure. User behaviors, protocols and awareness of lines of attack will be most effective in countering cyber threats in the years to come.

Many well-known data transfer tools that are not specific to securing client data are, in fact, not secure.

Mobile Device Management

Advanced mobile device management (MDM) solutions provide two critical advancements for those that utilize personal devices (*i.e.*, devices not issued by the firm). Application controls allow a law firm's IT department or managed services provider to control specific applications on mobile devices. Firm-managed email, document management, time and billing, and litigation support solutions tend to provide access via mobile applications. When a relationship was terminated in the past, the only option was to destroy the contents of the entire device. MDM solutions allow only firm-managed applications and data to be centrally administered and removed from devices. This is accomplished without negatively affecting the remaining applications and data on the device.

Penetration Testing

The most brilliant, well-intentioned information technology experts are human. Employing a third-party penetration testing firm with experience and tools provides tremendous value. A report is provided with initial remediation recommendations, and repeated testing continues over a contractual period.

Physical Media

The management and administration of physical media are areas of information technology security frequently forgotten. Tracking chain of custody, from the time received through destruction, should be used when transporting client information between law firm locations and/or law firms and third parties. Physical media should be sealed securely in nontransparent packaging.

Business Continuity Plans

Law firms approach business continuity in highly varied ways. Technology solutions must ensure the recovery of services during a time of business interruption. These plans must be tested and approved on a periodic basis, but not less than annually. Validation of successful transitions, data integrity and performance are all critical.

Incident Management and Response

In the event of an incident, is your firm prepared for the next steps? Firm personnel should know procedures for reporting incidents that could affect a firm's operations or disrupt or diminish the quality of services provided. Developing provisions in advance for notifying some or all clients of suspected or confirmed security breaches will likely save your firm from potential embarrassment or worse: client losses!

Exceed Expectations

Advancements in law firm cybersecurity are exceeding client-created demands for compliance. Now, law firms need to implement those solutions. Law firms that fail to implement information security protections to the same degree as other businesses will lose clients, productivity, respect and money. Ensuring a successful future requires law firms to catch up to current strategies and remain at the cutting edge of cybersecurity technology. P2P