LTT LAW TECHNOLOGY TODAY

October 18, 2016

SIX TIPS TO REDUCE SECURITY RISKS

BY MICHAEL KEMPS

Law firms, traditionally unregulated and self-reliant around technology decisions, have recently been surprised: their clients are auditing their security practices, controls and technology. Suddenly, confusion abounds. But why? It shouldn't. Law firm management should not expect their information technology services and infrastructure to be immune from client scrutiny. There are repetitive areas in which firms struggle to comply with client expectations. Audits vary from a couple of pages to numerous worksheets in length. Such evaluation will analyze specific architecture and configuration details, run penetration testing scenarios, examine hiring practices and more.

The following is a summary of typical areas that make sense to consider now – prior to an inevitable client request:

Two Factor Authentication

As the legal environment utilizes mobile devices and remote access with increasing frequency, Two Factor Authentication (2FA) has become mandatory. Clients demand that, at minimum, all remote access requires mandatory controls to ensure that two factors of authentication are employed.

Law firms are typically resistant. They have a desire to limit end user frustration. It's time to take this seriously, though. With two factors of authentication in place and all Active Directory accounts restricted, the environment immediately experiences a dramatic increase in security.

Encryption

Common practice with on-premises servers is to default operating systems and file systems not to encrypt data. While best practices have recently employed encryption of data in transit using Secure Socket Layer (SSL), encrypting data at rest is somewhat new to law firms.

Clients are increasingly concerned about unauthorized access to their data, and they seek assurances that it is fully encrypted even while sitting on internal law firm networks.

Data Loss Prevention

Data Loss Prevention (DLP) controls eliminate risk associated with data being accidentally or deliberately disclosed, typically via email or removal media. Systems must be employed to deliberately monitor outbound email activity and to lock down user access to USB ports/keys, remote or external hard disks and other removable media. These additional layers of protection will reassure clients that counsel are protecting data on the local network and preventing confidential information from being intentionally or inadvertently leaked.

Vulnerability Scans

Technology environments are constantly changing. Processes associated with adding and removing hardware, applications and employees require law firm networks to constantly adapt. New opportunities for security vulnerabilities continually arise. Ongoing, recurring vulnerability scans and even ethical hacks employed by third-party specialists to discover open ports, applications and potential threats – before they become a problem – are critical.

Backup & Disaster Recovery

When all else fails, backup and disaster recovery solutions are necessities to protect law firms from data loss. Without them, a natural or manmade disaster as small as a power outage can cause a law firm to lose important – and possibly all – client information. Cloud data storage prevents the loss of data that could result from relying upon on-premises backups. Further, it can speed recovery from security breaches by allowing instant remote access to replicated applications and data.

Security Awareness Training

With the best systems, processes and protections in place, all environments are subject to human use and interaction. Key security procedures may be forgotten and bypassed, or change controls misunderstood or not known. This has the potential to lead to a security breach. Law firm employees – including resistant Partners – should be trained, at minimum, annually about the firm's security practices and expectations in protecting firm and client data from unauthorized disclosure.

Clients are becoming increasingly selective. Not only do they seek top lawyers. They demand that law firms – whether boutique or large – employ appropriate security practices to protect their data, confidentiality and relationship. There is no reason a law firm should fail a security audit due to one of the above six items. Be prepared. Implement appropriate controls, processes, education and validation now. Review the typical questions that clients ask when conducting an IT infrastructure and security audit. Get serious about your network security – before the client audit.

Michael Kemps is the founder and chief executive officer at Innovative Computing Systems. He founded 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, Kemps is involved in ILTA (International Legal Technology Association) and the ALA (Association of Legal Administrators), as well as several local nonprofit organizations, and is on the advisory board of a community bank.

Originally published October 18, 2016 by ABA Law Technology Today