LTT LAW TECHNOLOGY TODAY

November 7, 2014

10 STEPS TO ENSURE DATA SECURITY AT YOUR LAW FIRM

BY BRIAN RUTHRUFF

Less than a year ago, the only entities that seemed concerned with data security were large corporations and health care organizations. With reports of security breaches making headline news on a weekly basis, data security has become top-of-mind for every business – and for every person who carries and uses a credit card. The threat of a data breach attack is a risk for law firms, too. The threat is reason enough to enact more stringent security policies, but there is another compelling reason: the security requirements of your own clients.

Small law firms might think that they are not a target, but even they have clients with desirable data. It could even be that your law firm is a much easier target than a corporate entity. It's a problem law firms cannot ignore, no matter their size.

So what can firms of any size do to better manage security?

Know the Threats

Law firms face threats from many different directions: state-sponsored hackers, such as those from China; industrial espionage by clients' competitors; disgruntled departing employees; and even individuals who use scripts or programs developed by others to scan for and attack computer systems and networks.

Control Chaos

Changes to security could bring production at a law firm to a standstill. If you need to make changes to security, the changes should be implemented in a way that does not impede attorneys' abilities to perform work for clients. Your firm should balance the need to protect client data and the need to access it.

Consider the remediation steps for preventing the CryptoLocker virus. You can lock down the firm's firewalls, desktops and email, but if done in an overly aggressive manner the changes could have potentially negative side effects:

- Users can't upload to court websites
- One-off applications, such as those common for litigation, may fail
- Email scanning false positives cause missed email

With planning, training, proper advance notification and staggering the change among users, the side effects can be minimized.

Prepare, Plan and Train

You can avoid disruptions in productivity through careful technology selection, planning and preparation. These days, maintaining a current firewall is not enough protection. Select the most appropriate security systems that provide the best mix of ease of use and security. Implement new systems and procedures only after they are vetted and tested by a small group of users. Prepare new users by giving them advance notice and creating a training plan that covers the topics in a language they understand.

Security awareness training is designed to increase end users' awareness of the firm's security policies and potential threats to the firm, and to increase their willingness to adhere to the firm's security requirements. Security awareness training is probably the most important step to preventing incidents, such as the CryptoLocker virus that has infected numerous law firms in the last few months.

You should plan to cover:

- Electronic communications
- Incident reporting
- Internet access
- Mobile device security
- Password policies
- Remote access
- Social media use
- The firm's Acceptable Use Policy
- Visitor policies
- Wireless access security

In your session, you should include an appeal to end users to use good judgment, and help them understand that good security starts with them.

Verify Your Vendors

Your firm's vendors must also follow proper security protocols. Vendors, especially those hosting your data in the cloud, need to pay particular attention to securing and protecting your data. Review every vendor's commitment to protecting your data, as well as their security certifications and policies.

Monitor Your Systems

Every firm should employ top-notch antivirus, antispam, malware and intrusion detection. Manage these critical systems to ensure that protection is active (e.g., not disabled by the end users) and up to date.

Routinely check firewall logs. These will highlight the extent to which your users are under attack and make you aware of administrative access and changes to your firewall. Periodically check the firewall configuration for unwanted changes.

You also should manage and monitor user accounts. Scan for user accounts that have not been accessed for a period of time, stale passwords and membership in administrative groups. Every IT administrator has added users to high-level security groups, such as domain administrators, in order to test and troubleshoot issues – only to accidentally leave them in groups where they do not belong.

Make System Entry Difficult

Law firms of all sizes should be using two-factor authentication. Two-factor authentication requires two things from a user before they are allowed to access a system: something the user has and something the user knows. The item the user has is a token – either a physical token or an application on a smartphone. The thing the user knows is his password or PIN. Together, these items provide a significant increase in the security of systems accessed remotely.

Prioritize Physical Security

Physical security is also important. Server room doors and cabinets should be locked when possible. You also many want to consider investing in an affordable security camera system that includes options for recording physical access. Stored data should be encrypted.

Your firm should consider implementing a clean-and-clear desk policy, which requires everyone to log off of their computers when not using them and to lock computers when they walk away. The policy should extend to laptops and other data storage devices, which should be locked when the employee is not present. No data, either printed or electronic, should be left unattended.

Engage a Third Party for Security Audits

After you've determined your new policies, put new systems and protections in place and trained your end users, you should consider bringing in a third party; someone not regularly involved with the firm's day-to-day IT needs to perform a security analysis. An outside security expert will perform a top-down evaluation of your systems, security policies and practices, and will review physical access to the systems.

Try to Break In

A penetration test (or “pen test,” in the security vernacular) is the process of trying to break into a system in order to identify any vulnerability. A pen test has to be executed with care, because if it is performed recklessly it can cause system or network damage through buffer overflows, Denial of Service (DoS) attacks and misconfiguration of systems. You should strive to repeat pen tests at least annually or with more frequency. If you change your firewall or other major systems throughout the year, you should also repeat a pen test.

Remediate Carefully

At the end of a security audit or pen test, you will receive a remediation plan. The IT department should carefully review the recommended changes before implementation to consider any possible adverse effects on other systems and end users.

Some believe that threats are irrelevant for small firms, but nothing could be further from the truth. It is increasingly common for clients of law firms to dictate security requirements, so all firms should make strengthening security policies a top priority. Now is the time to start a discussion about security within your firm.

Brian Ruthruff is the operations manager for Innovative Computing Systems, a leading provider of information technology services to law firms. Brian can be reached at bruthruff@innovativecomp.com.

Originally published November 7, 2014 by ABA Law Technology Today ABA Law Technology Today