LJN LAW JOURNAL NEWSLETTERS

Cybersecurity
LAW & STRATEGY®

as featured in...

CORPORATE COUNSEL | Legaltech news

An ALM Publication

May 2017

The Top-Five Critical Security Controls to Consider for Corporate Counsel Evaluations

Corporations consider many different factors when deciding whether to hire a law firm. Security wasn't usually a major factor, and law firms used to fly under the radar when it came to questions about keeping client data secure. That has all changed.

By Joe Kelly

Corporations consider many different factors when deciding whether to hire a law firm. Fees, clients, industry knowledge and capabilities have always been important aspects of the hiring process. Security wasn't usually a major factor, and law firms *used* to fly under the radar when it came to questions about keeping client data secure. That has all changed.

Now, law firm security breaches regularly make headlines. Large and respected firms have been "weak links" for malicious exploitation, and their clients can pay the price with publicly exposed information about cases, strategies, acquisitions, intellectual property and more. Corporate counsel, and the C-suite to which they report, are becoming increasingly mindful of this risk. They are starting to demand that their outside counsel adhere to strict security protocols and undergo in-depth evaluations.

One way law firms can address clients' security concerns is to apply Critical Security Controls. These controls are established by the Center for Internet Security (CIS) and are designed to be a "concise, prioritized set of cyber practices created to stop today's most pervasive and dangerous cyber attacks," according to the organization. Experts from around the world are called on to develop, refine and validate the controls.

In order to prepare for any grilling by corporate legal departments, here are the top-five CIS controls law firms should consider. By anticipating these questions and preparing to address concerns, firms will offer a secure relationship with corporate clients and score a competitive advantage.

1. CIS Control: Require secure configurations for hardware and software on mobile devices, laptops, workstations and servers.

Corporations must ensure that their law firms protect confidential data. They will most certainly ask how law firms keep data safe, regardless of how it is accessed or shared.

Encryption is one of the best ways to ensure that data remains

Joe Kelly is the founder and CEO of Legal Workspace, a cloud-based host for law firms. He also serves as founder and CEO of Business Network Consulting (BNC) Systems, a company that delivers enterprise-grade IT support. He can be reached at Jkelly@legal-workspace.com.

safe — especially critical legal information such as mergers, intellectual property and discovery. Encryption must extend to any device that may access the information such as mobile devices or USB drives. However, less than one in three law firms regularly encrypt data on USB drives and mobile devices according to one recent survey.

Firms should strive to make the encryption process painless and automatic in order to solve these issues. Whenever possible, firms should adopt hardware and software that have built-in encryption standards, including full-disk and file encryption. That includes laptops, cloud-based storage and mobile devices.

Here are key questions you should ask your IT team to determine compliance with this CIS control:

Does the firm's file, application and email server utilize encryption?

Does the onsite and offsite backup employ encryption?

Are all devices configured to support encryption?

2. CIS Control: Institute continuous vulnerability assessment and remediation.

Corporations will want to know what your firm is doing to stave off attacks from evolving threats that access through points of vulnerability such as phishing, worms and un-patched software. They will ask how often your law firm conducts vulnerability reviews and assessments and if it has the technological capability to scan an environment for vulnerabilities in their system.

Firms should regularly consult with outside experts that can test their networks and systems to see where issues could arise.

Firms should also ask IT these questions to root out weaknesses in compliance:

- How often does the firm conduct network scans and assessments?
- How often does the IT staff perform updates and patches?
- Are these policies documented and continuously followed?

3. CIS Control: Develop a boundary defense.

Navigating the exchange of information between networks is sometimes a challenging task, yet one that is essential when handling a corporation's confidential data.

Law firms should regularly review configurations for network boundary defenses, such as firewalls, inbound and outbound proxies, email gateways and other approaches. Law firms should also be able to quantify how their systems can reject communications from unknown or suspicious IP addresses. If firms aren't currently using defenses such as two-factor authentication to improve security, they need to begin immediately.

During an evaluation by a corporate legal department, firms should work in close collaboration with the organization to understand its needs and technical capabilities. For example, there are varying types and strengths of encryption methods. When firms and clients all use email servers with a TLS 1.2 or higher encryption strength, both sides can ensure that their data is much safer.

Speak to the firm's IT provider or contact to determine:

- What network defense perimeters the firm has in place.
- If the firm is filtering both inbound and outbound traffic.
- How often the IT team reviews and monitors the defense systems.

4. CIS Control: Create an inventory of authorized and unauthorized devices.

The Internet of Things (IoT) is quickly grafting itself into law firm networks. Each time a new device latches on — such as a smartphone, tablet, smartwatch, health accessory or thumb drive — it elevates the potential of risk.

While this connectivity offers many advantages to its users and their productivity, it also leaves systems extremely vulnerable by providing more avenues for unauthorized activities. Once people with malicious intent have gained access to a law firm's network, they can access emails, client files

and other vital information. This can be a concern for law firms as attorneys gather and add information using devices not necessarily vetted by IT for data access outside of the office.

Corporations should ensure that law firms allow only authorized mobile devices to sync with email and line-of-business applications such as Salesforce or case management systems. Otherwise, a company's data may be vulnerable from many different access points.

Companies should — and will — specifically ask their law firms about their policies around mobile devices and the processes for offboarding employees. Find out the answers to the following questions to pinpoint the firm's compliance level:

• What safeguards are in place to prevent new devices from accessing email and data?

• Can devices be remotely wiped if lost or stolen?

• What is the offboarding process to avoid information from leaving when people do?

5. CIS Control: Conduct security skills assessment and provide training to fill gaps.

The firm can have a rigorous cyber defense program, but without the proper policies and training for the firm's users, it won't be successful.

People play a large role in cybersecurity success and the best tools and systems are only as good as the people who use them. If attorneys and staff are not receiving security training and following proper procedures, client data is vulnerable.

Test phishing emails administered by security professionals are relatively common to determine which staff members could use additional cybersecurity training. Firms need to make sure everyone understands what to look for to identify a malicious email or phone call and how to properly deal with it. That requires regularly assessing how staff and attorneys are working, making sure everyone is aware of emerging risks, and providing training that is relevant and useful.

In some situations, training may not be optional. For example, the Health Insurance Portability and Accountability Act (HIPAA) represents one area where firms may have vulnerabilities around training of which they may not even be aware.

Under HIPAA, firms that have access to protected health information need to provide end-user security training. This specifically includes minimizing risks such as offering education about what malware attacks may look like or how the firm's policies affect day-to-day activities. Without training, firms may be at risk of regulatory investigations and significant fines if a breach of protected health information occurs.

These questions can help you determine the firm's level of compliance:

• How does IT determine gaps in an end user's cyber security knowledge?

• Does the firm have a security awareness program that educates employees on emerging and common ways cyber attackers are targeting end users?

Conclusion

Law firms need to know where their vulnerabilities lie, and what concerns clients may have. In order to minimize risks and stay on top of security threats, law firms should prepare to answer tough questions about how they can anticipate and close security gaps before they become an issue.

—❖—