Security and Compliance Play Critical Roles in Protecting IT Assets of Law Firms and Their Clients

Executive Overview

Within the legal sector, IT system security and compliance have changed dramatically in the past decade. They used to just be afterthoughts, but many law firms have reversed 180° to the point where security and compliance are now primary IT initiatives. This shift has been driven by a sharp increase in regulation activity and many publicized breaches, some for which the blame has been pointed directly at the legal sector.

Google Aurora, a state-sponsored cyber security incident where evidence was found of advanced persistent attacks, penetrated dozens of major U.S. companies.[1] Many security experts think the IT infrastructures of the legal firms these companies relied on were the main infiltration routes used by the hackers.

And then there's the Canadian Potash Hack involving a group of law firms handling a $40B acquisition bid.[2] When hackers penetrated one of firm's computer networks and leaked information, the entire deal was cancelled.

To combat breaches like these that seriously threaten the IT assets of the legal industry as well as the IT assets of clients, law firms need to deploy advanced security and compliance measures that identify, lessen and mitigate the risks. Just as importantly, law firms must gain the ability to prove the measures they have deployed satisfy the requirements of clients, regulators and business partners.

Breaches now occur at an accelerated pace as cyber criminals increase the sophistication of their attacks. In response to those breaches—and evidence that indicates companies lack the necessary controls to prevent breaches—regulators are enacting stricter compliance requirements. Law firms thus face a formidable challenge. Add in that firms also now rely more heavily on cloud computing, and the challenge to maintain security and compliance grows even more complex.

This white paper from All Covered, the IT Services Division of Konica Minolta, presents an overview of the security, compliance, attestation and cloud-computing challenges faced by law firms along with an approach to solve these challenges. Doing so is paramount—not only for law firms to protect their own IT assets, but also the IT assets of their clients.

The Need to Defend Internal IT Assets While Also Protecting Clients

The examples above are just two of the many cases where cyber criminals accessed a client network through a law firm's network. Some hackers have even managed to snoop on conversations by law firms handling major stock market deals. Such activity is perhaps more damaging than a law firm's own network being hacked successfully. The financial impact of such breaches can quickly spiral into billions of dollars for law firm clients—who are sure to then quickly switch to new legal representation.

Opportunities like these exist because weak IT infrastructures deployed by law firms present an opportunity for cyber criminals to not only penetrate a law firm's IT assets to steal information, but also to access the IT networks of the law firm's clients. The hacker community knows only too well that one of the best ways to penetrate a company's network is to first infiltrate the networks of its business partners.

And given the confidential nature and the financial value of the information companies share with their law firms, the legal sector has become the prime target for cyber criminals. With law firm and client systems sharing so much information, unauthorized access to one network often leads to easy unauthorized access of the other.

The legal sector is thus on the hook for protecting its own internal IT assets as well as the IT assets of clients.

Client Partnerships Require Compliance with Multiple Regulations

In the compliance realm, there's an obligation to identify risk and treat that risk in a manner that's demonstrable to customers, regulators and business partners. Regulations such as HIPAA have evolved to the point where the applicability to law firms is no longer debated—firms that process and handle patient information are encumbered by the requirement to comply with HIPAA on behalf of their healthcare clients.

In addition, more and more states are enacting laws regarding the ways that businesses handle personally identifiable information (PII). California, Massachusetts and Wisconsin in particular have added significantly to the burden on businesses to keep confidential customer information safe from breaches. As more breaches occur, states across the U.S. will accelerate their efforts to enact more stringent requirements for protecting PII.

SOX, PCI-DSS and many other federal and international regulations also come into play for law firms. With every industry impacted by varying sets of regulations, firms that serve clients from multiple sectors likely need to address a host of compliance requirements. This includes overseeing the compliance of their internal systems in relation to the legal industry as well as making sure their systems that process client data comply with each of their client's industry regulations.

Cloud Computing Compounds the Challenge

Applying the necessary security and compliance measures has grown more complex as law firms embrace the cloud—moving some or even all of their applications and data to the cloud to take advantage of the many improved business-process efficiencies and the IT-provisioning cost-savings that the cloud offers. Many firms are already leveraging cloud services such as Microsoft Office 365 and SharePoint, Google Docs, Apple Cloud and a host of platform hosting providers.

This also means there are one or more other entity's infrastructures that law firms must now assess and monitor for sufficient security. No firm wants to tell a client that a network breach was caused by insufficient due-diligence when vetting the security measures that the law firm's cloud hosting provider deploys.

For this reason, some firms try to take the stance of never moving any applications and data to the cloud. But this can hamper the efficiency of lawyers and support staff, which in turn may lower the amount of billable time they accrue.

And even if a firm's primary network does not operate in the cloud, there's always some cloud activity occurring—whether it's a staff member using Google email to send large files, or lawyers using a service like Dropbox or Box.com to share files with other lawyers. In many cases, files and emails sent through the cloud end up stored on mobile devices, which adds even further to the security and compliance challenge. Some firms also run cloud-based email filtering or save their system back-ups to the cloud.

One way or another, the cloud thus needs to be addressed through a risk management program that proves proper security measures are in place. In addition to law firms implementing their own internal security measures and policies, they also need to make sure their third-party cloud providers provide proof they manage and process data using prevailing best practices—in a way that aligns with the security and compliance objectives of the law firm as well as the objectives of the firm's business partners and clients.

The Need to Prove Reasonable & Appropriate Security and Compliance

In addition to applying the necessary security and compliance measures, law firms also need to ensure they can attest to the measures they apply. This means providing demonstrable proof to clients, business partners and regulatory agencies that the deployed measures are sufficient and satisfy the guidelines and requirements of those clients, business partners and regulatory agencies.

Each audience likely has a different set of requirements and needs to view attestation documentation in a different way. Law firms thus need a flexible way to respond to attestation requests. They also need to be able to respond to attestation requests quickly. If a breach occurs, it's important to immediately present the security and compliance measures the firm deployed—hopefully proving the firm was not at fault.

Attestation to demonstrate security and compliance may or may not be complex depending on the size of the law firm and its relative practice areas. It may simply consist of a penetration test and a letter of attestation that shows the types of tests conducted and what those tests discovered.

In other cases, firms may need to acquire ISO 27001 certification with a scope statement and attestation as to which systems are secure and compliant. This form of attestation is much more robust as it's backed by an Information Security Management Systems (ISMS) audit—vetted and validated by ISO registrars. Firms may also be required to obtain SOC 2 Type II service order reports, which run anywhere from a few pages to nearly 100 pages long, with documentation describing the security controls deployed by the firm.

Large law firms often must also conduct full third-party audits that include an ISO 27002 gap assessment, for which ISO registrars check the firm's conformance to 114 information-security best practices. The auditors go beyond conventional network security to analyze the overall security design and components such as password policies, employee screening, validating the assignment of legal reviews, and physical security.

Taking Security and Compliance Beyond Hardware and Software

Security and compliance solutions do not necessarily require new hardware and software purchases. The answers may actually lie more so in gaining a better understanding of the risks the firm currently faces and then determining the best way to manage that risk. It's often about developing the right processes to manage the risk.

For example, if there's a risk of employees selling data, then the firm needs to develop stringent employee background checks that would be completed upon hire and then on a continuing, regular basis. Security and compliance management can also involve following recurring processes for reviewing user accounts and terminating employee access as well as vulnerability and configuration management.

Supplier relationship management is another important aspect to consider. How do the third parties that process data for the firm apply controls to manage their risk? Are there mechanisms in place to conduct periodic checks in case that level of risk changes?

Identifying an Effective Security and Compliance Partner

When evaluating IT partners to assist with security, compliance and attestation, it's important to realize that some IT firms specialize in just one or two areas, but not always all three. A firm with expertise in deploying security and compliance measures does not necessarily possess knowledge of the best way to attest to those measures.

And in many cases, it makes sense to collaborate with a different partner for attestation. If a solution provider helps you deploy a secure network with a vulnerability and configuration management program, you probably want to work with another solution provider to conduct the penetration test that proves those measures are effective and sufficient for attestation. The firm that deployed the security measures likely lacks the necessary objectivity to conduct the penetration test properly and then attest to your security posture.

For regulation compliance, working with a consultant that helps you satisfy ISO certification requirements will likely give you a very robust and mature form of attestation. But the actual attestation audit should still be conducted by an ISO registrar. Independent objectivity will then be baked in.

The partner you select should also offer multiple attestation options and know which ones are necessary for your firm to properly position its security posture:

- Vulnerability Assessment & Penetration Testing
- ISO 27001/2 Consulting and/or Gap Assessments
- Shared Assessments—Standardized Information Gathering Questionnaire (SIG) and/or Agreed Upon Procedures (AUP) Assessment Preparation

ISO 27001 and ISO 27002 are particularly beneficial when it comes to compliance. They contain a super-set of standards that lets you build an information security management system encompassing all the major regulations. Consultants that offer ISO expertise are also likely to have expertise in HIPAA, SOX, PCI-DSS and other major regulations.

This is particularly beneficial for law firms working with clients across a range of industries. ISO is also recognized as the standard for information security management in the legal vertical as declared by the International Legal Technology Association's LegalSEC council.

When choosing an IT partner to assist with security and compliance, you ultimately want to collaborate with a firm that understands the legal vertical and its challenges along with a combination of expertise across security, compliance and attestation. They should know how to identify and quantify risk, and how to secure you against that risk as well as comply with regulations.

Act Now, Before Security and Compliance Deficiencies Lead to Losing Clients

IT security and compliance in the legal vertical are radically different than even just a few years ago. Today, law firms not only need to be secure and compliant, they also need to demonstrate their security and compliance safeguards to regulators, business partners and most importantly, their clients.

This change in the legal sector is tied to a number of inter-related shifts that have taken place over the last decade—an increase in regulations governing sensitive data, greater reliance on third-party cloud providers, and a remarkable rise in data breaches. The breaches are growing bigger and gaining greater publicity—with the legal vertical tied into many cases. Many law firm CIOs are even being contacted by FBI personnel.

The key to responding to this challenge is to develop a strategy for addressing the increased risk, the more stringent compliance, and the more challenging attestation requirements. The process requires several months to reach the point where a law firm can be demonstrably secure and compliant. The time to start is now—before the lack of security or compliance costs you a client.

By partnering with All Covered, law firms can receive the necessary guidance to address their security and compliance requirements. For more information, contact All Covered at legalteam@allcovered.com.

Citations

1. "Google Aurora Hack Was Chinese Counterespionage Operation," *InformationWeek*, 5/21/2013, http://www.darkreading.com/attacks-and-breaches/google-aurora-hack-was-chinese-counterespionage-operation/d/d-id/1110060?

2. "China-Based Hackers Target Law Firms to Get Secret Deal Data," *Bloomberg*, 1/31/2012, http://www.bloomberg.com/news/2012-01-31/china-based-hackers-target-law-firms.html