SPHERE TECHNOLOGY SOLUTIONS

Mastering Data Governance

Whitepaper: Law Firm Data Security

Table of Contents

Industry Scope: Law firms are the weakest link in their clients data security landscape 2

Evolving trends and what they mean for you.. 2

Assessing our immediate data security risk 3

Reevaluating your data governance strategy.. 3

Your data governance checklist.. 5

About SPHERE.. 6

Industry scope: Law firms are the weakest link in their clients' data security landscape

Global law firms and clients are on high alert when it comes to data security. The unique nature of law firm network environments coupled with the size and scope of the sensitive unstructured data housed within them exposes firms, and clients alike, to a heightened level of vulnerability. Outdated security infrastructure and funding oversights for proactive IT-security investment have made the legal space an entry point for data breaches targeting sensitive client data. Particularly, those of firms in the financial realm who operate within strict compliance environments.

LAW FIRMS REPORTEDLY SPEND SLIGHTLY UNDER 2% OF THEIR ANNUAL REVENUE ON PROTECTING CLIENT DATA

Alongside changing business pressures, cybersecurity resources continue to thin and fragment, further painting law firms as the weakest link from a data security standpoint.

Evolving trends and what they mean for you:

The legal industry has witnessed vast shifts, driven chiefly by the greater data security ecosystem. For multinational and niche-oriented law firms alike, several trends are influencing fundamental change in the space:

Cyberattacks amplify: Ransomware attacks and massive data breaches are sending rippling effects across the legal space. The litany of negative press is unending: "Yahoo General Counsel Ron Bell Resigns Amid Data Breach Controversy," "Uber ousts in-house counsel who suppressed information about 2016 data breach," "Ransomware Attack on DLA Piper Puts Law Firms, Clients on Red Alert," "Equifax looks to InHouse Lawyer to 'Build a New Future' After Massive Breach." Hacks have accounted for millions of leaked attorney-client privileged documents -- from intellectual property to financial information -- and ensuing losses for data recovery and reactive security, as well as immeasurable reputational damage.

Compliance arrives alongside intensifying client pressure: Outside forces are squeezing law firms twofold. First, the arrival of GDPR is putting proactive data governance and protection at the forefront of shifting compliance requirements for any firm working with European data subjects. The expansion of digitization and e-justice services is also fueling the compliance fire. With the proliferation of advanced technologies in the legal space, law firms need to ensure that IT remains compliant with regulatory requirements, particularly when it comes to data security. The second force is primarily client-driven. Clients are powering meaningful security overhauls at law firms. ALM Intelligence's latest cybersecurity study reveals that 82% of law firms surveyed are faced with pressing client requirements to upgrade cybersecurity protections. Financial service (FinServ) clients are spearheading the trend, requiring validation of information security in line with strict compliance standards.

Business pressures shift: To add to security-oriented stress, law firms are facing uphill battles across a wide array of business fronts. Increased competition for sought-after laterals, pricing pressures, and evolving operational efficiencies are driving increasing downward rate pressure. Firms that are undifferentiated and overcapacity as market demand softens are struggling the most. Additional shifts include the rise of alternative fee arrangements (AFAs) -- firms continue to face difficulties in this effort as proper data identification and usage to inform AFAs lags. Finally, law practices are seeing increasing pressure to achieve effective practice group development and management.

Assessing your immediate data security risk

It’s clear that among all the landscape shifts across the legal industry, effective data security is a chief driver in determining which firms lead as others are left behind. Building a comprehensive data governance strategy to mitigate the risk to law firm environments and client data requires firms to balance a number of considerations.

FACTORS TO CONSIDER: ADOPT A HOLISTIC DATA GOVERNANCE PROGRAM THAT MEETS AND EXCEEDS THE COMPLIANCE NEEDS OF YOUR CLIENTS THROUGH:

- TECHNOLOGY-ENABLEMENT
- AUTOMATION
- PROVEN METHODOLOGIES
- FLEXIBILITY AND CUSTOMIZATIONS

What are your highest data security threats? Determine what your biggest vulnerabilities are and where they lie. There are a number of evolving threats, internal and external, that law firms need to evaluate. Email systems, vast unstructured data, employees and human error, cross-border exchanges of personal data, ransomware, malware, and wiperware are just some of the highest threats facing law firms today.

What does the cybersecurity landscape look like for multinational law firms? The legal industry as a whole faces relatively high risk for data breaches. Even in the face of these threats, firms have been unable or unwilling to invest in the proper data governance framework required to secure sensitive data and meet increasingly demanding compliance requirements. A plurality of firms -- as high as 80% -- fail at basic security protocol, such as two-factor authentication, USB, email and laptop encryption, as well as intrusion detection and prevention systems.

What technologies and/or processes are in place to protect clients' sensitive information? Assess current unstructured data and overall network environments. A data governance program should be minimizing the risk associated with data breaches and internal threats. Is there a program in place that meets the unique needs of the network environment? Are the compliance requirements for law firms and their clients being met? Strict security and compliance policies should dictate this framework.

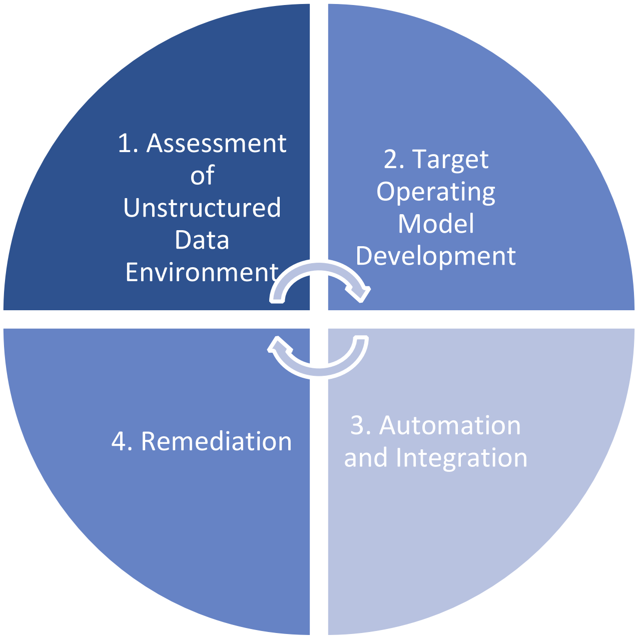
Reevaluating your data governance strategy

Proper data governance frameworks will enable you to create reasonable end-state requirements. You can then focus on remediating security and compliance concerns, streamlining the management of your data, and reducing the costs associated with the retention of stale data. Regardless of your firm’s particular vertical, certain frameworks exist to take a data-driven approach to your governance strategy.

Implement Preventative Measures: Assess your current environment, particularly your unstructured data governance. You'll need to gain greater visibility into the risks associated with your current data. Knowing who the data owners are, who has access, what they have access to and having sufficient insight into risks and security issues, such as segregation of duties, will allow for increased visibility.

Finding a Trusted Partner: The data security landscape is complex and growing even more so as technology advances and data threats multiply. Find a seasoned partner that can take you through the entire data governance process, from file share assessment to long-term remediation. Your partner will institute custom policies and procedures in line with your target operating model and highest priority threats.

Build your data governance framework: Cover your bases and implement a multi-dimensional, datadriven approach towards the management of your unstructured data.


1. Assessment of Unstructured Data Environment
2. Target Operating Model Development
3. Automation and Integration
4. Remediation

1. **Assessment of Unstructured Data Environment**: Take stock of your data with a complete data inventory, full analysis and risk ratings. You will examine the kind of data, its structure and status, policies for governance, ownership and access, as well as its security and standardization level. This initial assessment will dictate the appropriate strategies and processes for data governance within your unique network environment.
2. **Target Operating Model Development:** Build your guide to remediate immediate areas of risk considering existing control standards, gaps and deviations from industry best practices, risk rating parameters, staffing levels, existing or planned technology and tools and any regulatory or compliance requirements.
3. **Automation and Integration:** Stop the bleeding by implementing the controls and framework based on your target operating model so you can begin managing your unstructured data

proactively. take a phased approach if necessary so you are taking steps in getting better controls in place.

4. **Remediation:** A targeted and scoped remediation effort of your identified risks will gauge future long-term remediation needs. Being able to understand where risk resides is key -- remediation is prioritized based on the highest risk areas.

Your data governance checklist:

When evaluating a trusted partner for data governance, you want to be able to maximize the security and compliance standards of your unstructured data, while minimizing total cost of ownership of data security and ongoing remediation. In evaluating a multi-dimensional data governance strategy, consider the following:

Take stock of your data:

- What data exists within file shares?
- How is the data structured?
- Is the data stale or active?
- Who owns the data?
- Who has access to the data?
- Where is access non-secure or non-standard?
- What are the policies for governing the data?
- Who's using the data?
- What to evaluate in terms of data management:
- Do you have a Document Management System/Case Management System?
- How can you be sure your employees are keeping all of their sensitive unstructured data there? ▪ When was the last time you cleaned up home and group drives or looked at local admin users?

How to handle cross boundary data:

- How do you ensure case data doesn't cross boundaries between clients with competing cases/patents/IP?
- What is the best way to separate and bucket collections of data; practice groups are a logical approach

What to do with sensitive case data during transitions:

- What data policies are in place for when partners/paralegals/executive assistants leave the firm?
- How do you ensure that emails, unstructured data, and permissions are transferred to the people taking over the case when they leave?

How to manage various distribution lists?

- How do you manage your internal and external lists and ownership?

- How do you curate them and ensure that there aren't people receiving information via email that shouldn't?
- Do you make sure to add/remove people from AD groups (Distribution Lists) when they leave move/join/leave the firm?

Start building your data-driven governance strategy. To learn more about how top 100 multinational law firms are doing this today contact sales@sphereco.com or call (201) 659-6204 to talk to one of our data security experts.

About SPHERE

SPHERE is an award-winning woman-owned cybersecurity company focused on unstructured data security, Privileged Access management and Identity and access Management solutions. SPHERE has created a technology-enabled service model leveraging:

Subject Matter Expertise

Ranging from strategic security advisory to SWAT-team remediation projects, SPHERE provides solutions to help companies understand their risks, create policies for a target end state, and remediate major vulnerabilities. We have experience remediating nearly 1 million AD groups, 26 million file shares, and 60,000 privileged accounts.

Leading Edge Products

SPHEREengine: Our enterprise-ready architecture is built for top 100 firms but used by companies of all sizes. We love data and our architecture allows us to ingest, correlate, analyze and report on all types of data so we can provide critical security and risk reporting for all your governance needs.

SPHEREboard: When it comes to unstructured data, wrong permissions are a major danger for your organization. SPHEREboard focuses heavily on many different access control issues across your file shares and other unstructured data repositories.

Partner Solutions

SPHERE recognizes the need for third party products and works with the industry's best-of-breed solutions. SPHERE provides guidance, along with technology integration capabilities to both the client's technologies, along with SPHEREboard.

Reference List:

https://securityintelligence.com/the-inconvenient-reality-of-law-firm-security-challenges/
http://www.kleos.wolterskluwer.com/en/law-firm-trends-2018/

https://blogs.thomsonreuters.com/answerson/prepared-law-firms-face-cyber-security-threats/
https://trushieldinc.com/the-4-biggest-cyber-security-challenges-facing-law-firms-today/
https://rossintelligence.com/top-trends-challenges-advice-law-firms-2018/
https://www.law.com/sites/ali/2017/12/10/the-state-of-cybersecurity-in-the-legal-industry-are-thingsimproving/?slreturn=20180327171419
https://biglawbusiness.com/law-firms-to-spend-6-9m-to-keep-client-data-secure/