White Paper

Four data security measures law firms can't afford to ignore

Workshare®

Change matters

Four data security measures law firms can't afford to ignore

Your guide to what's inside:

Workshare
Change matters

Introduction

The first half of 2017 saw an incredible number of cybersecurity breaches across the world, and they were big ones. However, you don't need us to tell you data security is an issue and one that needs to be handled with some urgency. The regulatory demands; the facts; and the news stories speak for themselves.

As many commentators attest, it's not about if a firm will be the victim of a data loss event, but when that event will occur. Therefore the questions law firms need to ask are:

- Are we adequately protecting the data we process and that we are responsible for?
- Can we accurately monitor and track where and to whom company information is being sent?
- Will we be able to report on a data loss event should one occur?

According to the 3rd annual American LegalNet, Inc. (ALN) Risk Management Survey*, conducted at ILTACON 2017, when the legal IT professionals interviewed were asked: "Who bears overall responsibility for your firm's risk management function?" 29% gave the most popular answer – "Don't know". If law firms and the teams within them aren't clear who is responsible for risk management, the chances of effectively managing it are obviously slim.

When it comes to complying with outside counsel guidelines, and protecting personal and confidential data, your average law firm has a massive job on their hands. As law firms deal almost exclusively in confidential client data, the exposure to accidental or malicious data loss is high. This risk is compounded by the fact that responsibility is often unclear and detecting data loss events or data breaches is extremely hard.

Each client and matter has its own security protocol. What's considered acceptable in terms of sharing information and with whom that information can be shared varies from matter to matter and client to client. It also depends in what region of the world the data is being transferred. Most commercial solutions that successfully protect firms in other industries have blind spots when applied to the legal industry – they simply aren't flexible or sensitive enough for these nuances.

So, how do law firms stay on the right side of an ethical wall; meet outside counsel guidelines and the security expectations of their clients, as well as prevent data loss from occurring?

This paper explores four practical ways to deal with data security.

*"57.7% of legal IT professionals plan to increase investment in Risk Management this year."

1. Gauge criticality and maintain confidentiality

Confidentiality is something law firms understand very well. They deal in confidential client data as an every day occurrence, but while all data is important and has value, it has different levels of confidentiality based on how critical it is to a business.

Maintaining confidentiality simply means restricting access to certain information to ensure only those who are entitled to see it can actually access it. Therefore, it's important to understand what data you control, where it's stored, when and how it's shared, and its criticality to your business.

Businesses are responsible for and process multiple types of data: personal data, like employee records; confidential data, like business plans; and customer data, including case matters and files. The criticality of the data can be determined by the impact that a breach or loss event would have on the business overall.

Negative impacts of a data loss event can come in the form of reputational damage, loss of business, legal liability and, in some cases, financial loss in the shape of fines or trading restrictions.

Firms need to understand where their vulnerabilities lie when it comes to protecting their most critical, confidential data. Once it's understood which documents are the most critical, where they are stored, and who is authorized to access them, effective monitoring can begin.

What's often missed by firms is how and where confidential data is shared. Common examples of unauthorized access are:

- Job moves, when people aren't deleted from key groups
- Misconfiguration that allows access to restricted resources
- Sharing of credentials that allows access to restricted data
- Human error that causes confidential data to be exposed

There are two ways to ensure critical data remains confidential:

1. Restrict access to it
2. Audit all access points

Rules should be set to prevent people from accessing or receiving certain data, but it's also essential to continuously review and monitor this.

A safe assumption is that you lose control of data once it leaves your control systems. The best option, therefore, is to monitor entry and exit points – whether via email, a Document Management System, or another browser-based collaboration or sharing platform – and keep a full audit history.

To successfully maintain confidentiality, firms need to go through every system they manage, whether directly or with 3rd parties, and monitor the critical data being shared.

2. Mitigate the risk of sharing sensitive data

Information must inevitably leave the sanctuary of a firm's control systems, because sharing and collaboration are essential. For a firm to successfully maintaining control of its data, the next step therefore is to monitor the critical data being shared.

Distribution of sensitive data can, however, be accidental or malicious in nature. For example:

- Matter files or content maybe inadvertently emailed to a colleague who sits on the other side of an ethical wall
- Files could be sent to a personal email account to be reviewed from home or on a mobile device
- Autofill errors may occur in email, so the wrong recipients are selected during composition
- Sensitive matter files can be slowly emailed or uploaded to a sharing site at low volume by someone prior to leaving a firm

To mitigate risk when sharing sensitive data, there are three key things to consider.

1. The Content & The Medium
Sensitive data is shared in numerous ways: text in an email or chat channel; complex and structured files shared via email, secure file transfers or via a browser. Running checks on all content and sharing mechanism (not just email) is essential. What's the criticality of the content? Is there a risk sensitive metadata could be present in the file? What's the approved format for sharing this data, as agreed by the client on this matter?

2. The Recipients
Is the individual receiving the content approved to do so? Increasingly, outside counsel guidelines dictate that matters be associated with some form of ethical wall or whitelist (the people sensitive data can be sent to) or a blacklists (the people it can't). The permutations are endless and the risk of loss is high as just a simple autofill of a recipient in an email composition could see sensitive content breaching a control.

3. The Domain & The Destination
With clients and regulators increasingly nervous about data sovereignty, the next thing to consider is that sensitive data may be going to an intended recipient, but with an inappropriate address or domain e.g. gmail or Box.com. Blanket controls are not practical in law firms, as what is deemed acceptable to one client may be unacceptable to another.

So, what can law firms do?
Remove sensitive metadata from files before they are shared, regardless of how they are shared. Also, implement solutions that can draw control information from a document management systems or ethical wall solution to apply appropriate protections before sharing takes place. Firms can also implement network activity tracking solutions to prevent and warn users of risks and potential breaches prior to a sharing event.

3. Monitor data and perform risk analysis

File protection needs to become a core component of a law firm's IT architecture. With every action related to a company's files monitored and recorded. This gives firms the ability to highlight data anomalies, abnormal sharing behavior and potential data breaches. It also means informed decisions can be made about what actions need to be taken when a potential breach or loss event is flagged.

When files are loaded, deleted, renamed or exchanged, an audit log of actions can be created. The people responsible for security and compliance in a firm can then use this information to analyze risk, with flags sent up, anomalies spotted and potential data loss events investigated.

Staying compliant with security policies, client expectations and wider regulation, by using the data generated by the files themselves is the most obvious and accessible solution available to most firms.

It's possible to interrogate user activity on files and analyze their exposure to risk, then action can be taken to pro-actively manage it. For law firms, applying overlying knowledge of a matter and a client is an essential part of the process to ensure those responsible for investigating potential issues are not deluged with false flags.

One example would be to augment data monitoring with billing information, to identify where content is being accessed or shared with a user who never bills that matter. Through this process, they become an obvious outlier to investigate. The more data points that can be combined together to pinpoint outliers in sharing activity and behavior, the more precise investigations and controls can become. Either way, when it comes to protecting data and complying with guidelines its important to start somewhere. Waiting for the prefect solution only increases the likelihood of an event occurring.

> **28% of data breaches globally are caused by human error.**
>
> **$141 [is the] average cost per record lost.**

IBM – 2017 Cost of Data Breach Study

4. Identify data security breaches and report them

Finally, it's important to establish procedures to assess anomalies in sharing and sharing behavior to understand when a data breach may have occurred and whether it was malicious or unintentional. This is often an afterthought, but it is critical to robust data security and therefore a law firm's competitiveness.

Investigations are the challenge of the industry, because to report an incident effectively, you need to know one has happened. When assessing possible breaches, there will always be false flags, but in law firms there can be an extraordinary number, so constant process of monitoring and refinement is crucial.

Breaches may range from a low-risk event to an all out attack. Low-risk could simply be that some of the control systems have become out of sync with the distribution controls. This might be the result of someone changing a control in one system, but not in another, or it could be a lack of understanding at an end user level.

Whatever the risk profile, a process should be defined that allows an event to be accurately identified and then quickly and thoroughly investigated. If appropriate, the end user should also be contacted to determine the cause of the event, so they're able to confirm whether a breach has occurred and its source.

A reporting and crisis management process should also be prepared and established. This should include internal communications, reporting to the appropriate authorities (internally and externally), and PR. The criticality of good communication cannot be overstated. A good response can make the difference between containing a data breach and a company suffering irreparable damage.

When security policies and controls are in place, data monitoring is occurring, and communication plans are established, it then becomes a matter of regular reviews, taking learnings from any events and the way they are handled, to continually improve data security.

> **Confidence in Capability to Address and Mitigate Risk…A large contingent, 76.69%, responded they were capable, more than capable or extremely capable.**
>
> American LegalNet, Inc.
> Risk Management Survey Study

Conclusion

While cybersecurity events are increasing, along with regulatory demands and the complexity of data exchange, it's possible to use those exchanges to audit and monitor activity associated with the critical data being shared by a law firm. This enables law firms to handled the reporting of data security events with the appropriate authorities and the appropriate level of urgency, should one be identified.

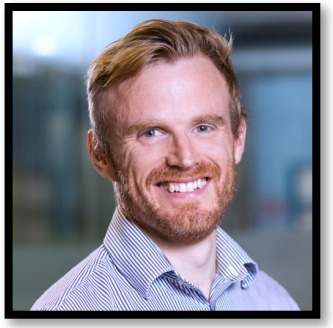
It also means that the firms managing data security most effectively will gain competitive advantage, both in terms of maintaining their reputations and their finances.

It's still vitally important, however, for many firms to clearly identify who is responsible for risk management. Even though companies may feel equal to dealing with threats, ownership is vital to ongoing refinement and improvement.

It may be inevitable that a breach will occur, so firms need to display controls, handle incidents effectively and show they can learn from their experiences. After all, it's widely accepted that it's not necessarily an event occurring that causes problems, it's how the event is handled.

By adequately protecting the data a firm is responsible for, by accurately monitoring and tracking where and to whom confidential information is being sent, by being able to report on a data loss event in a timely way, law firms can go a good way towards improving data security, staying compliant and gaining competitive advantage.

When it comes to protecting sensitive data, the average law firm has a hill to climb, but it's not insurmountable by any means.



Nick Thomson
Chief Revenue Officer,
Workshare

About Workshare

Workshare is dedicated to helping professionals compare, protect and share their high stakes documents. Since 1999, Workshare has developed and released intelligent technology for business services firms Now, more than two million professionals use Workshare around the world.

Acknowledgments and additional resources

- Association of Corporate Counsel: Model Information Protection and Security Controls for Outside Counsel Possessing Company Confidential Information
  https://www.acc.com/aboutacc/newsroom/pressreleases/outsidecounselcybersecurityguidelines.cfm
- https://www.legaltechnology.com/legal-it-newswire/american-legalnet-aln3-2017-risk-management-survey-finds-law-firms-have-concerns-about-risk-security-and-lawsuits-and-inadequate-tech/
- 2017 Cost of Data Breach Study - IBM® Cyber Security Analysis
- Prosperoware: Milan InfoGov
  https://www.prosperoware.com/milan-infogov-products
- Workshare Secure: Metadata cleaning & risk analytics
  https://www.workshare.com/product/secure

t: +44 (0)20 7426 0000 / +1 415 590 7700 w: www.workshare.com e: sales@workshare.com
a: 20 Fashion St, London, E1 6PX o: London | San Francisco | New York | Sydney

Workshare®
Change matters