

Ensuring Security of your Key Documents & Client Information



INTRODUCTION

This document identifies the growing changes for legal firms in the management of risk. Specifically highlighting the changing legislation, compliance and client pressures around information management. It explores the drivers behind these changes, the impact on the legal sector and the proactive measures that should be taken to address them.

CHALLENGES FACING THE LEGAL SECTOR

The UK Legal Sector is undergoing dramatic changes. In October 2011, the **Legal Services Act** will make the UK one of the more deregulated legal services markets in the world. The introduction of the **Alternative Business Structure** and the Solicitors Regulatory Authority's (SRA) move to **Outcome Focused Regulation (OFR)** will have a significant impact on the market.

The Law Society has long been in favour of choice, open markets and competition. They consider this to be good for solicitors and for the consumer of legal services. One definite impact of these changes will be an increase in both competition and innovation, with new highly commercial entrants gearing to provide the services clients want in the way they want it, all with a strong focus on doing this in a cost effective way.

Success in this new environment will come to those legal firms that quickly and proactively embrace change. Firms need to make the necessary structural and business changes to their practice, the products they offer, the way they deliver their services and respond to the increasingly sophisticated demands of their clients.

The recession has also accelerated technology-led change in the provision of legal services; the increasing use of fixed fees means that once a fee is set, the firm's profit depends on its ability to provide services cost effectively.

Along with this there is a marked growth in the **technological sophistication and demands of clients**. Not only are they increasingly concerned over the security with which their information is handled, clients are also demanding instant access to both documents and information.

These drivers are forcing law firms to become more business-like, more competitive, and to focus on efficiency. The following sections of this paper explore how these changes impact the need for law firms to safely and securely manage both client and internal information.

Changing World

The major changes in the legal Sector

- 1. Outcome Focused Regulation**
Requirement on firms to manage risk and report upon material breaches
- 2. Alternative Business Structure**
Increased competition in the market, with commercialised entrants leveraging information systems
- 3. Demanding Clients**
Actively differentiate between law firms on their competence in the management of risk.

INFORMATION RISK –A REAL WORLD PROBLEM

Across all industries there are countless examples of high profile organisations suffering reputational damage in the press as a result of accidental data loss. However, there has also been a sharp increase in the reporting of malicious attacks and information theft. Wiki-Leaks, Sony and numerous public sector bodies to name but a few.

The legal sector has not been immune to the press; there was a considerable amount of negative publicity over the data breach at ACS Law and the loss of 6,000 user's details. The public interest in this story was substantial and reflected badly on the legal sector, fuelling the public's growing paranoia regarding data security.

A survey¹ of 100 UK Law firms found that nearly a quarter of respondents admitted misplacing a mobile device containing confidential documents, putting case notes, contracts and client details at risk. With just 13 percent of the lost devices secured

¹ by Credant Technologies

Ensuring Security of your Key Documents & Client Information

and the information encrypted. The study also highlighted that as many as one in five lawyers surveyed were using personal USB drives, laptops or mobile phones to store sensitive client and company information.

The volume and use of electronically held information in business continues to grow at an exponential rate, this coupled with the increasing reliance on personal devices and awareness of the market to the risks this creates means that information security is no longer a factor that can be overlooked.

NEW REGULATION – OCTOBER 2011

The introduction of Outcomes Focused Regulation in October 2011 sees legal firms entering a new world in which they manage both their business and their relationships with their clients. The SRA's focus is shifting from specifying "indicative behaviours" to guiding by "Outcomes".

The SRA state that they have: *"stripped out a lot of the detail of the previous Code to empower you to implement the right systems and controls for your clients and type of practice. You will have more flexibility on how you achieve the right outcomes for your clients, which will require greater judgment on your part"*

The SRA have stated that they now seek to identify risk in a proactive way, historically they responded to risks that had already happened. Their new focus is to proactively identify the risks that exist in a law firm and manage them effectively. Law firms need to be wary that if risks can't be managed then the SRA can use its powers to intervene.

The SRA Practice Standards Unit is set to conduct thousands of internal and external audits of UK legal firms to determine the degree of compliance with their policies, directives and standards. Within the next few years they aim to have visited most legal practices, therefore it's essential to remain compliant at all times to avoid costly SRA fines or the potential for the practice to come under investigation.

REQUIREMENT FOR A 'COMPLIANCE OFFICER FOR LEGAL PRACTICE'

A key element of the OFR is the requirement to appoint a Compliance Officer for Legal Practice (COLP) by March 2012. However, law firms need to have all of the required processes and measures in place before the COLP becomes responsible.

All Legal firms are required to submit their first annual compliance reports to the SRA by October 2012, covering the year from October 2011. This report must demonstrate the firm's position through a written compliance plan together with a risk register. Firms need to act now to get their processes in order by October 2011.

The COLP needs to oversee the creation of a risk and compliance plan that demonstrates the firm's procedures and practices as well as their on-going monitoring and review process. The COLP then has an on-going obligation to disclose all material gaps to the SRA maintain a list of all lapses in compliance and notify the SRA of serious concerns in any event.

This is a significant role and should not be underestimated, it is the COLP who will be responsible for ensuring that the firm has systems and controls in place to ensure its managers and employees, are complying with the SRA's regulatory requirements.

EXTERNAL REGULATORY PRESSURES

Recent changes to the Data Protection Act came into force in 2010 and are designed to deter data breaches. The Information Commissioner's Office (ICO) is now able to order organisations to pay up to £500,000 as a penalty for serious breaches of the Data Protection Act. The power to impose a monetary penalty is designed to deal with the most serious personal data breaches and is part of the ICO's overall regulatory toolkit.

Outcome Focused Regulation

How the SRA will operate from 6th October 2011, concentrating on the high-level principles governing practice and the quality of outcomes for clients, rather than tick-box compliance with rules.

Compliance Officer (COLP)

A COLP has three key responsibilities, to:

1. ensure compliance with the terms and conditions of their firm's authorization
2. ensure compliance with statutory obligations for example, the Legal Services Act 2007, the Solicitors Act 1974 and the Administration of Justice Act 1985
3. Take all reasonable steps to record and report to the SRA all failures to comply.

Ensuring Security of your Key Documents & Client Information

LEGAL CLIENTS SEE RISK MANAGEMENT AS A DIFFERENTIATOR

The 2011 UK law firm risk management survey², which spoke to risk professionals at 26 of the UK's top 100 firms, reported that only 21% of lawyers perceived risk management to be a "key priority", this is in stark contrast to their clients, with nearly half deeming it a key priority.

"Most clients view risk management as a key priority or a way to differentiate themselves from their peers. Lawyers and staff view it primarily as a necessary, but inconvenient pursuit"

The vast majority of clients have asked legal firms to restrict internal access to sensitive information. Recent high profile press coverage of embarrassing data loss across all industries, including the legal sector, means that clients are more focused on data privacy and data security. This has led to a noticeable change in a client's attitude and expectations regarding handling of their information.

Clients are becoming more aware and demanding that legal firms conform to recognised standards, as they themselves become more attuned to the risks inherent in sharing their own key information. Effective management of risk is viewed as a key differentiator when selecting a legal partner.

Increasingly sophisticated clients are putting pressure on firms to implement, and be assessed against, non-mandated standards like ISO 27001. Such standards require a Security Management System to be implemented that is based on an assessment of risk and for technology and process to be applied to mitigate these risks.

For the IT departments of law firms, that means making the management and control of information as seamless as possible for lawyers, using technology to support productivity and fee-earning. Legal firms must explore and implement risk management solutions that support the way the practice runs, rather than be seen to hinder lawyers doing their job.

Investigation shows that firms at the upper end of the market now view technology as an enabler. A comparison of the top 20 law firms and firms in the next tier down shows there is a significant difference in profitability. Whilst there are many factors that affect this, the speed at which those firms embrace technology is definitely a key part of it.

However, with speed and efficiency comes increased risk, the easier it is to access information; the easier it is for it to fall into the wrong hands, be this malicious or accidental, the damage to your reputation and business is the same.

SUMMARY

Law firms need to act now to meet the new regulation and their client's information security demands. This should not be seen as a 'necessary evil' but embraced as an enabler to demonstrate a competitive advantage over their peers.

Law firms must take the necessary steps to prove to their clients that information is safe in their hands, demonstrating that they appropriately manage all information and have taken all reasonable steps to ensure its integrity.

Industry Standards - ISO 27001

ISO 27001 is the globally recognized information security management standard increasingly adopted by organisations in all sectors

1. Systematically examine the organization's information security risks, taking account of the threats, vulnerabilities and impacts
2. Design and implement a coherent and comprehensive suite of information security controls and risk management
3. Adopt a management process to ensure that the security controls continue to meet information security needs on an on-going basis

² 2011 UK Law Firm Risk Management survey. IntApp

APPROACH – WHAT YOU NEED TO DO

FOCUS YOUR ACTIVITIES

It is important to understand the different types of sensitive data a law firm may have. A Forrester Research study³ examined the type and value of documents that contained intellectual property, and found they formed two groups, 'Company Secrets' and 'Custodial Data'. (See box right)

Understanding and recognising the different types of information a firm makes use of will help determine where security investments are needed. Often a firm will focus on trying to prevent accidents with Custodial Data, due to regulatory pressures, but an additional and often overlooked risk is theft of sensitive Company Secrets.

Company Secrets are the data "crown jewels" and represent the most sensitive activities; this information is of critical importance to the future success of the firm. Keeping it safe should be amongst the highest priorities. In terms of actual damage and cost to a business, research shows that the loss of Company Secrets is 4 x more likely to happen and 10 x more costly than the loss of Custodial data.

When considering solutions for the protection of sensitive information, both data types should be considered and, where possible, processes combined in order to derive maximum return for the organisation.

UNDERSTAND HOW YOU USE INFORMATION

Research shows that nearly all law firms have some form of current software in place to enforce information barriers. Barriers prevent unauthorized access to protected information and maintain ethical walls, however once information has been appropriately shared outside of the firm the barrier is effectively 'breached' and the information is vulnerable to negligent or malicious actions. The ideal would be to compliment these barriers by maintaining a persistent level of security and access controls over information even after authorised sharing, this way the integrity of the information is never at risk.

SECURITY IS ONLY AS STRONG AS THE WEAKEST LINK

Until very recently protecting information through its life-cycle involved integrating a number of independent security technologies that can help secure stages of the data custody chain (figure below). These individual technologies tended not to take into account the overall company process they were operating alongside and rarely gave an end-to-end solution: at some point valuable data will be exposed.

While there are many good point solutions that operate within each of these technology areas, in combination they often suffer from the same problems:

- At some point an item of data has to be unprotected in order that it can be used
- Once an item is sent out from its owner and arrives with a recipient, control is lost
- Information Security risks tend to be associated with human activity (absent mindedness leading to loss, malicious actions leading to theft, poorly designed business processes leading to compromise, etc.). These activities more often than not span more than one step of the custody chain, thus technology lead solutions tend to be misaligned with the risks they are trying to mitigate
- Few of these solutions are designed to work together, leading to expensive and complicated integration work and difficult to follow workflows, making it difficult to demonstrate compliance.

Understand your Information

Company Secrets:

Valuable confidential data such as client papers, case notes, Key documents, financial reports, research etc.

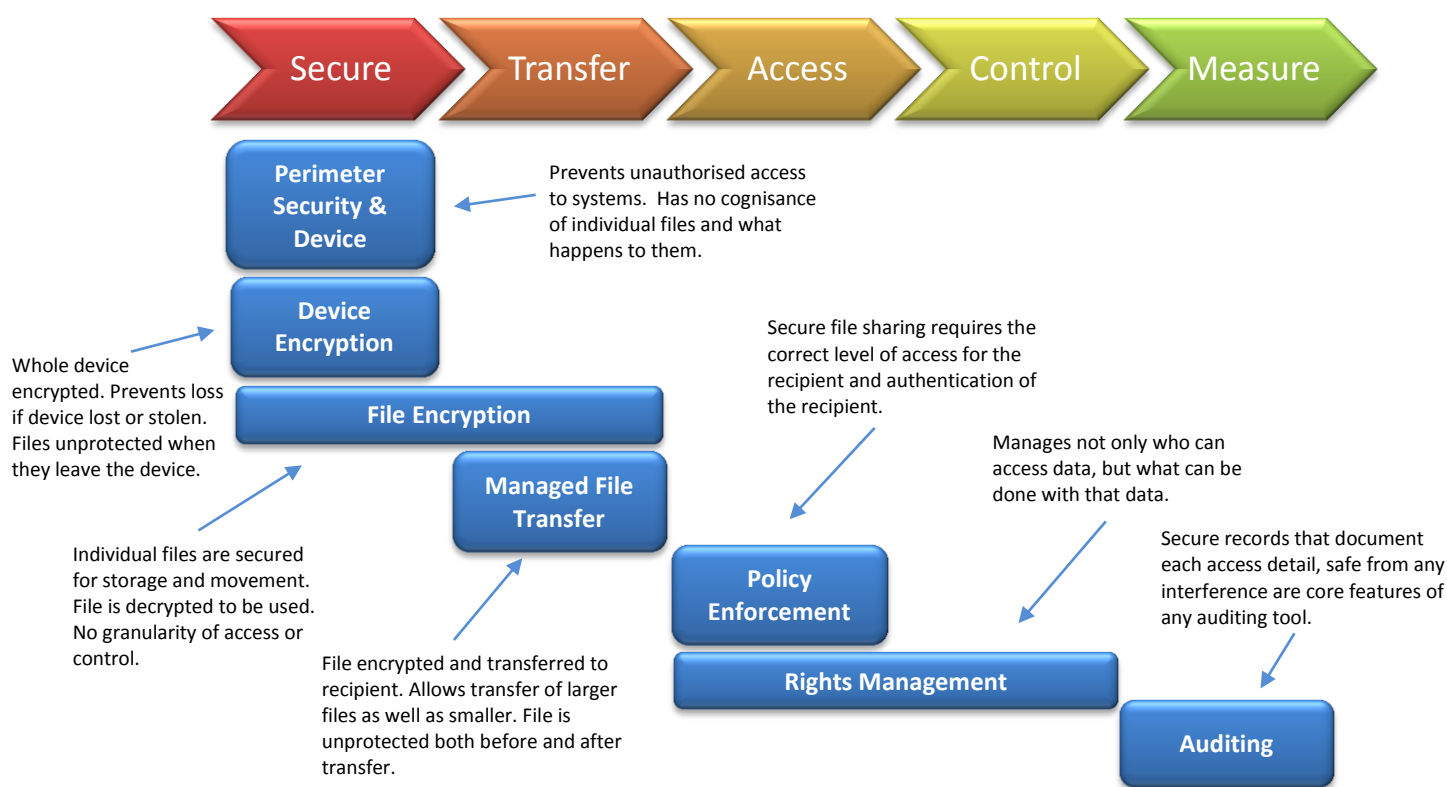
Custodial Data:

Data held on behalf of others such as client details, employee information etc.

Loss of Company Secrets is 4 x more likely to happen and 10 x more costly than the loss of Custodial data

³Forrester Research: Selecting Data Security Technologies. December 2009.

Ensuring Security of your Key Documents & Client Information



Components of the Information Security Lifecycle

A BETTER PERSPECTIVE – FOCUS ON YOUR INFORMATION NOT TECHNOLOGY

Losing your laptop (or memory stick) is certainly very inconvenient, but what really matters is actually the loss of the information that is contained on it. The value is in the information you want to protect, not the device upon which it resides. Yet traditional approaches to information security focus on the protection of devices, so that your information has to move from one protected domain to the next.

To ensure security, you need to have complete and persistent control over all the potential places your information may reside. If these places are outside of your systems or network this is a practically impossible task. With the proliferation of personal storage, laptops and smart phones, the mediums for transferring information continue to grow at an alarming rate. If the link between these domains/devices is not 100% assured and seamless, your information will eventually move to a place where it is unprotected.

The reason that traditional solutions have the problems described above is that they focus on securing areas of technology, rather than the higher level problem of mitigating the information security risks associated with the activities of business. What is required is a security paradigm that includes the following considerations:

- Secure both Secret and Custodial data with the same rigor
- Secure Information irrespective of where it lies within the custody chain
- Secure Information wherever it ends up
- Remove human error where possible
- Support compliance needs
- Be driven by the needs of doing business – using but not losing data.

BECOME DATA-CENTRIC

A recent development in this field is the concept of Data Centric Security. The philosophy of Data Centric Security moves the focus away from securing devices, to securing the actual information itself. This makes sense as the asset firms actually need to protect is the value of the information to their business. This is particularly relevant to law firms as essentially they are information businesses, with client's information the most valuable asset of all.

By following a Data Centric paradigm, security is directly applied to the data/information itself, regardless of where that information is stored, or who has a copy of it. Effectively information is 'encased' in a secure wrapper that only grants access to the appropriate person, regardless of where they are. Therefore, even when information moves outside of your environment, it always remains protected, as the security moves with the data itself.

Another key benefit of this approach is that in addition to the persistently applied security, it gives you the ability to enforce Rights Management, i.e. dictate what the intended recipient can actually do with your information once they have received it. For example, by using these techniques you can actually stop the recipient making electronic copies of your information, re-sharing it with others or even printing hard copies.

This approach advances the security of key information to a new level and enables law firms to assure their clients of the security of their most valuable information, even when it needs to be released or collaborated on both inside or outside of the organisation.

Data Centric Security

The key points of Data Centric

- o Protection should be applied directly to the data
- o Information is persistently secured during storage, transit and after delivery
- o IT technology agnostic, crossing both technology and company boundaries
- o Authorised recipients can only use information in the intended manner
- o Information owner has a comprehensive audit trail of their information

BUSINESS BENEFITS

It's a given that employing effective security in any business is a good thing, however in today's economic environment any investments made by a firm needs to demonstrate true value back to the business. Investment in Information Security should not be approached as an insurance policy, or just a necessary sunk cost.

When security is effectively integrated into the operational processes of a business, it can be used to quickly liberate and exploit the value in information. This greatly increases the speed and efficiency with which a business can operate, confident that the risks are being controlled and managed.

Calculating Return on Investment (ROI) for Information Security is a complicated task; is it about making money, saving money or not losing money? You can calculate the potential cost of a security breach and estimate the risk of this occurring to form a mathematical value figure, but interestingly ROI and risk questioning tends to stop abruptly when a security breach occurs.

A lot of professionals fail to understand the impact an insecure information infrastructure can have on the business. Many believe that IT is simply there to setup new users and trouble shoot technical problems, perceiving that Information Security is there to manage the firewall and keeps the anti-virus software running. They fail to consider all the other systems and business processes for which IT and Information Security are responsible.

IMPROVE REPUTATION & CLIENT CONFIDENCE

The more progressive organisations are actively employing security as an enabler for their business, they no longer see security as a 'nice to have' but consciously use it as a differentiator to drive new business, build brand equity and assure their clients. This is true of the implementation of technology into the legal sector as a whole, with the top tier firms making marked advances in efficiency and profitability.

There have been a number of high profile instances in recent years of confidential messages being disclosed to the wrong people with disastrous consequences. The Enron/Arthur Andersen affair is probably one of the most notorious. But, along with any bad publicity this can bring, there is also the impact this can have on a law firm's professional indemnity cover insurance premiums, which have suffered steep rises over the last four years.

USE SECURITY TO REDUCE COSTS

Security can be like buying any form of insurance, if you don't suffer a breach you could be forgiven for seeing it as a sunk cost with no direct return. However, firms can also use security to remove cost from the operation of the practice.

The UK legal profession uses Document Exchange extensively; it is an integral part of the legal sector, providing time-critical documents earlier and the ability to send them later in the day. This creates valuable additional working time and relieves pressure on fee-earners. However, there is still an associated cost based on the volume of documents sent and once a document is delivered to the recipient it is effectively out of your control.

By employing a Data Centric Security approach, documents can be sent electronically and delivery is free and instantaneous. With Rights Management the transmitting party also retains control over what the recipient can do with a document.

Investing in the appropriate information security solution can have immediate financial benefits, for example with the cost to send documents via Secure DX around £4 per kg, each lawyer would only have to send 20 documents electronically per year to recoup the cost of a typical secure Data Centric solution.

IMPROVE SPEED OF OPERATION

By ensuring that all their work is stored electronically, a firm can have access to every bit of data within their practice at the push of a button, which leads to efficient document and information management and hence huge administrative cost savings.

A Data Centric Security approach can be used to liberate information flows within the firm, enabling remote on demand working, with staff having secure access to the same level of information, just as if they were at the office.

EASE OF COMPLYING WITH REGULATIONS

In many cases regulation or clients mandate the implementation of security for the handling of information. A reactionary approach can lead to a poor implementation, where the technology is seen as a 'necessary evil' and hinders professionals from doing their job.

By approaching the security as a holistic system it can be integrated around normal business processes and hence be a seamless part of the work flow. Not only does this greatly increase the speed of operations, but it also improves internal acceptance and staff morale.

CONCLUSION

Compliance is a major spend within a firm's security budget, but does not necessarily equal secured data and commercial advantage when it comes to sensitive information security. Firms need to consider placing more focus on securing critical secrets that confer long-term competitive advantage, as well as accidents involving custodial data.

By approaching the problem from a point of view that considers the business requirements that lead to information risks and selecting systems and solutions that share this approach, firms will be better placed to support the needs of compliance and address the security of their own secrets.

Legal firms should consider Data-Centric Security technologies that provide a unified platform to protect both types of data. They should specifically be able to accommodate unstructured information, provide the correct level of access to necessary parties and place emphasis on retaining control of information at all times, even when sharing or collaborating with third parties. Files should also be secured with persistently applied measures, allowing the file to always be protected as its minimum state, and access controlled wherever it is used, sent or stored.

The Cost of Paper

An article by BusinessGreen.com, stated that on average, filing and maintaining 500,000 pieces of paper costs:

- o £162,000 in workflow management
- o £75,000 to research lost files
- o £98,000 in storage and disposal costs.

Cutting annual paper use by 500,000 sheets can save a company £336,000 a year

more than 65p saved per sheet conserved, according to JP Morgan

Ensuring Security of your Key Documents & Client Information

In the current market, firms need solutions that both deliver against their risk mitigation requirements, and add commercial value. By employing the right business-enabling software organisations can fundamentally transform their 'IT costs vs. benefit' model to deliver quantifiable value. The ability for a firm to keep up with the pace of business change, client requirements, changing processes and legislation significantly accelerates the time in which they can derive the benefits.

ABOUT SECUREGRADE

SecureGrade is the UK distributor of Boole Server and an exponent of the Data Centric Approach to Information Security. If you would like to discuss any of the topics raised in this paper in greater detail please feel free to contact us on the number below.



SecureGrade Ltd ©

Reg No: 07211961

Registered Office: 42-52, Charlbert Street, London. NW8 7BU

Postal Address: 70 High Street, HARPENDEN, Herts. AL5 2SP