LexisNexis

Internet Law
Bulletin

2017 . Vol 20 No 5

Contents

Information contained in this newsletter is current as at August 2017

LexisNexis®
Butterworths

Time to get serious about protecting information

Ian Bloomfield IGNITE SYSTEMS

The importance of cybersecurity is unquestionable. The recent global ransomware epidemics involving "WannaCry" and "Petya" should have been evidence enough for anyone still to be convinced.

The Law Council of Australia is one of many bodies, together with the federal government, that has been promoting the need for businesses to take action on cybersecurity. Cyber Precedent[1] is an information campaign by the Law Council of Australia to assist the legal profession in defending itself against cyber threats. When launched by the then Law Council of Australia President Stuart Clark AM, he said it was now a core priority of the Law Council of Australia to ensure Australian lawyers understand, and are prepared for, cyber threats.

If taking action on cybersecurity is a given, the challenge for many law firms is to know where to start. One area in particular should be a primary area of focus for all law firms — information security, or more specifically the security of electronic documents. For the purposes of clarity, any reference to documents in this article should be interpreted as meaning electronic documents, including email.

This article explains what document security is, why it is important and the options available to implement document security.

Takeaways:

- Recent events have highlighted the need for law firms to take action to improve their cybersecurity.
- The information handled by law firms is crucial to their operation and potentially their survival.
- Every law firm should be taking steps to understand the information they collect, process, transmit and store, and importantly understand how to protect this information.
- It is time for every law firm and the people who work in them to get serious about protecting information.

What is document security?

The essence of a law firm is the information it holds, whether it is client information, third party information or internal information. This information comes from many sources — provided by clients and other law firms, created by lawyers and staff, and/or obtained from third parties. The information is typically stored in a range of systems — email, files storage and/or practice management systems. Finally, a subset of this information is passed onto other parties — clients, other law firms and/or third parties. The day-to-day activities of most people who work in law firms involve working with and processing this information in the form of documents.

Document security is the practice of:

- preventing documents from being obtained, accessed or used by anyone not appropriately authorised; and
- maintaining the integrity of documents. In other words, stopping documents from being corrupted, modified, destroyed or lost.

Why should law firms care about document security?

The implications of not having adequate document security can range from annoying to catastrophic. Some potential consequences are:

- inability to deliver services due to lost or missing information;
- loss of clients as a result of appearing unprofessional or even being considered incompetent;
- loss of reputation as a result of a data breach; and/or
- actions by the Australian Information Commissioner as a result of a data breach. With the imminent introduction of the data breach laws, this could involve legal action if a law firm has revenues of more than $3 million.

At the extreme end of the spectrum there is the potential to bring an organisation to its knees or even put it out of business altogether. Any law firm ignoring document security is potentially putting their future at risk.

Identify and understand

How an organisation collects, processes, transmits and stores information should be the foundation of any cybersecurity program. The starting point is to identify and understand the different types of information you are dealing with.

The only effective way to get a complete and comprehensive understanding of the information within an organisation is to conduct a data inventory, sometimes referred to as a data map. A data inventory is a very structured process to identify all of the information collected, processed, stored and transmitted by an organisation. Although this is highly recommended, it is a non-trivial exercise, both in terms of time and money. There are references at the end of this article for further information about a data inventory.[2]

In the absence of a data inventory, a law firm needs to carry out some form of assessment to at least identify the main types of information that it handles. This assessment should consider the information across three areas:

- information that comes into a law firm via documents;
- information generated internally, and possibly circulated internally; and
- information contained in the documents sent to external parties.

Classify

Once there is an understanding of the various types of information involved, it then needs to be classified. The classification of information then determines what level of protection should be applied to documents containing a particular type of information.

There are many ways by which information can be classified, and how any particular organisation does it is a matter of what works for them. A typical classification could look something like this:

- *unrestricted* — information that can be made public (eg, a marketing brochure);
- *matter-restricted* — information that can be sent outside the organisation, but only to parties associated with a particular matter (eg, a client or another law firm);
- *internal* — information that is not to be sent outside the organisation (eg, a policy document);
- *business confidential* — intellectual property and sensitive business information (eg, financial records);
- *personal information* — as defined under the Privacy Act 1988 (Cth); and
- *sensitive information* — as defined under the Privacy Act.

Label

Once a law firm has identified the types of information it handles and has established a basis for classification, it is then necessary to have some way of assigning classifications to documents. Typically this is carried out by assigning labels to documents.

The simplest arrangement for implementing the labelling of documents is to rely on a policy and some complementary procedures. The policy would outline the intent of the classification process, and the procedures would detail how staff should go about labelling the documents.

There are a number of third-party software add-ons for Microsoft Office that aid in assigning labels to documents such as Office Classifier, Egress Switch Email and Document Classifier.[3] These solutions provide functionality that allows a user to easily apply classification labels to emails and Microsoft Word, Excel and PowerPoint documents.

A more sophisticated way to manage document classification is to use an information rights management solution, sometimes called document rights management or enterprise digital rights management. There is a section later in this article that will discuss information rights management in more detail.

An organisation that understands the types of information it handles and has formal guidelines for the classification and labelling of documents now can appropriately protect documents.

Protect email

Email is taken for granted but it is one of the least secure ways of communicating. Once you send an email, the process involved in sending it to the recipient is hidden with no practical way to control it. The delivery process can involve many steps, traversing a number of systems along the way. The security of the email delivery process has not kept pace with the rate of cyber threats, and as a result there are many ways email can be compromised. The bottom line is that sending any sort of confidential information via normal email is unsafe, because messages can be intercepted, redirected and viewed by unauthorised individuals.

The only secure option for sending any confidential information by email is to use end-to-end email encryption. This form of email encryption protects the content from being read by entities other than the intended recipients. With end-to-end email encryption, the data is encrypted on the sender's system, and only the intended recipient will be able to decrypt and read it.

There are lots of acronyms you are likely to see relating to email security — Secure Sockets Layer (SSL), Transport Layer Security (TLS), STARTTLS,[4] Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) and Domain-based Message Authentication, Reporting and Conformance (DMARC), to name a few. Although these all play a role in email security, they will not keep email content secure from access by anyone other than the intended recipient in the way that end-to-end email encryption does.

End-to-end email encryption requires both sender and recipient to have a pair of cryptographic keys. There is one private key and one public key. The sender encrypts the message locally on their device using the recipient's public key. The receiver decrypts it on their device using their private key. It's all very complicated, and in the past, using it was just as complicated. It is only recently that end-to-end email encryption has been made available in a way that is simple and easy to use.

Today there are end-to-end email encryption options that are practical for anyone to use. With these solutions, the exchange of the cryptographic keys is taken care of in the background. The most common ways to get end-to-end email encryption are:

- add-on functionality to an existing email service, such as Office 365 Message Encryption;[5] and/or
- a third-party service that is used in conjunction with an existing email service, such as Enlocked or Sendinc.[6]

It should be noted that Google's G Suite does offer email encryption, but this feature is only available with G Suite Enterprise. G Suite uses a protocol called Secure/Multipurpose Internet Mail Extensions (S/MIME) and getting the encryption functionality set-up is not simple. Among other things, there is a requirement to obtain your own S/MIME certificate and then it has to be uploaded to Google, along with your private encryption key.[7] The fact that Google holds the private encryption keys means this cannot be truly classified as end-to-end email encryption.

Gmail does not provide any end-to-end email encryption capability. Even worse, Google scans Gmail email content looking for keywords to aid in their targeted advertising. Google did announce in late June 2017 that as of "later this year" it will stop scanning the content of emails sent by Gmail, but there is no confirmed timing for when this change will take effect.[8]

Protect documents

Instead of sending confidential information in an email, an alternative is to send the information in an attached document that is protected from unauthorised access. With this approach, a protected document can be transferred securely, even though the email itself may not be secure.

The most common way to secure a document that is to be emailed to someone is to use encryption in conjunction with a password. The following are some of the ways to protect a document using encryption and password protection:

- Microsoft Office provides this ability with Word, Excel and PowerPoint documents. Note that this capability extends to PDF documents in later versions of Microsoft Office;[9]
- PDF documents can be protected in this way with Adobe Acrobat (not the free Adobe Reader); and
- there are also utilities like WinZip that enable a file or a package of files to be protected.

Beware of cloud options

Many individuals and law firms use cloud-based file storage and sharing solutions, such as Dropbox, as an alternative to email for transferring information. With this arrangement, documents containing the information are stored in the cloud. Access to a document can then be provided to a third party by sending them a link to the document.

As detailed in a recent article by the Law Society in UK, the consumer or free versions of cloud-based systems like Dropbox or Google Drive are not too appropriate for communicating information with clients or receiving confidential information.[10]

The business versions of Dropbox and other cloud solutions with similar levels of security are safe to store documents. Nevertheless there are risks with document sharing. Sending a link to someone external so they can access a document leaves open the possibility that someone unauthorised could also use the link to access the document. With Dropbox Business, it is recommended to use the password and expiration features to increase the level of security.

There are other risks with using cloud-based systems. Cloud-based systems do not have the additional layer of security that a computer has when it is connected to a local network and protected by a firewall. The only thing stopping a cyber-criminal from getting access to a cloud system is by not having the username and password. Two-factor authentication adds another layer of security that significantly reduces the risk associated with cloud systems.[11]

Two-factor authentication is a form of access control that requires two different types of evidence to verify the user's identity — typically, what the user knows (password), and a one-time passcode generated by something held by the user (security token or mobile phone app). An everyday example of a multi-factor authentication is in using a credit card where you swipe the card and also have to enter a PIN.

Two-factor authentication is rapidly becoming a standard offering with cloud solutions. The “Two Factor Auth List” website lists the most popular cloud services and identifies whether a cloud service supports two-factor authentication.[12]

Another thing to be wary of with cloud-based solutions is that you may be exposed to geographical risks in relation to data sovereignty. Your information could be stored outside Australia and be subject to different legal regimes. This can also lead to regulatory issues, such as then being in breach of your Privacy Act obligations or inadvertently breaching the data obligations of those different legal regimes.

There are more details about the benefits and risks of cloud solutions in the recently published Law Institute of Victoria’s “Cloud computing essentials”.[13]

Information rights management

Using end-to-end email encryption, securing documents using password-protected encryption, or using cloud-based file sharing are all only partial solutions to the problem of protecting information. Information rights management, sometimes referred to as document rights management or enterprise digital rights management, is a more holistic approach which enables the management and protection of documents over their entire life cycle, from creation to destruction.[14]

Information rights management enables a document to be classified, labelled and encrypted at the time it is created. Protection policies are then applied in accordance with the classification, and the policy then controls what actions can be carried out on the document and who is allowed to access it. The classification and the policy are attributes of the actual document and these attributes remain with it regardless of where it is moved or sent.

Because the protection policy applied to a document is embedded *in* the document, information rights management solutions provide the ability to control documents wherever they go. Documents can be monitored and tracked, enabling visibility of who has accessed a document, where it was accessed and when. It also enables the protection policy to be changed so that access can be revoked. A document retention policy can also be enforced by including a defined retention period as part of the document policy.

Information rights management is available as an add-on to Office 365, referred to as Azure Information Protection.[15] There are also a number of third-party solutions such as Vera, Vitrium and Seclore.[16]

Conclusion

Information is the life blood of a law firm, having the ability to sustain and support growth, but if it is not properly secured, it also has the ability to seriously damage or even cripple a law firm.

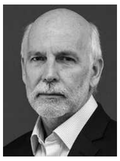
With the imminent implementation of the data breach laws, protecting information will become a compliance requirement for many law firms. The level of security in place to protect information will no longer be at their discretion, and the only acceptable minimum will be to be compliant.

Law firms must take steps to understand the information they are responsible for, and implement arrangements to ensure that information is appropriately protected, both inside their organisation and also when it is communicated externally.

Whether you are a large law firm or a sole practitioner, email is unsafe for communicating confidential information, and using end-to-end email encryption is essential. Documents containing confidential information have to be protected, and the responsibility for protecting the information in documents cannot be abrogated just because the document is passed onto an external entity.

Information rights management can provide an effective way to protect information, but it’s not appropriate for all organisations and it is not a silver bullet. As with most technology, you have to understand the scope of the problem you are trying to solve, assess the available options, and be able to make an informed decision about what will best suit your particular needs.

One thing is certain, with a cyber threat landscape getting even more complex and presenting an increasing risk, along with a regulatory framework imposing greater compliance obligations, business as usual is not an option.



Ian Bloomfield
Managing Director
Ignite Systems
www.ignite.com.au

Footnotes

[1] See the Law Council of Australia Cyber Precedent website at www.cyberprecedent.com.au.

[2] For data inventory references, see: D Manek, B Radke and M Waters “Data inventory: the critical 1st step in data security” (28 April 2017) www.law360.com/articles/918460/data-inventory-the-critical-1st-step-in-data-security; and B Cave “How to conduct a data inventory” (18 January 2016) www.lexology.com/library/detail.aspx?g=c40ee415-c2bf-4a3f-a2b5-8bff79a93a82.

[3] Document labelling software: Office Classifier: www.boldonjames.com/products/office-classifier; and Egress Switch Email and Document Classifier: www.egress.com/what-we-offer/classification.

4. See www.fastmail.com/help/technical/ssltlsstarttls.html.
5. See Office 365 Message Encryption at https://technet.microsoft.com/en-us/library/mt661609.aspx.
6. Third party email encryption services: Enlocked: www.enlocked.com; and Sendinc: www.sendinc.com.
7. See how to enable S/MIME message security: https://support.google.com/a/answer/6374496?hl=en.
8. D Greene "As G Suite gains traction in the enterprise, G Suite's Gmail and consumer Gmail to more closely align" (23 June 2017) www.blog.google/products/gmail/g-suite-gains-traction-in-the-enterprise-g-suites-gmail-and-consumer-gmail-to-more-closely-align.
9. A Da Costa "How to password protect and encrypt Office 2016 Documents" (3 October 2016) www.groovypost.com/howto/password-protect-encrypt-office-2016-documents-excel-word-powerpoint-o365.
10. P Wright "Beware of the phish — how to stay ahead of the scammers" (3 May 2017) www.lawsociety.org.uk/news/blog/beware-of-the-phish-how-to-stay-ahead-of-scammers.
11. L Constantin "5 things you need to know about two-factor authentication" (31 March 2016) www.pcworld.com/article/3050358/security/5-things-you-should-know-about-two-factor-authentication.html.
12. See www.twofactorauth.org.
13. Law Institute of Victoria "Cloud computing essentials" (February 2017) www.liv.asn.au/getattachment/Professional-Practice/Areas-of-Law/Technology-and-the-Law/Resources/20170223_LP_LawTechEssentials_CloudComputing_V02.pdf.aspx.
14. M Branscombe "Why you need DRM for your documents" (3 May 2016) www.cio.com/article/3065036/security/why-you-need-drm-for-your-documents.html.
15. Microsoft "What is Azure Information Protection?" (last updated 12 July 2017) https://docs.microsoft.com/en-us/information-protection/understand-explore/what-is-information-protection.
16. Third party information rights management solutions: Vera: www.vera.com; Vitrium: www.vitrium.com/editions/enterprise; and Seclore: www.seclore.com.