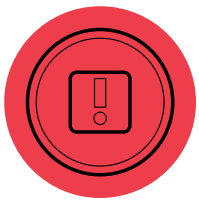
How Law Firms can use Secure Messaging to Win More Clients

As clients are demanding greater protection of their information, law firms must incorporate email encryption into their processes. This white paper will describe how email encryption has evolved into a tool that law firms can use to differentiate themselves from the competition and drive business development opportunities.

Background

Law firms have not been at the forefront of using email encryption despite having the responsibility for protecting highly confidential client information. Traditional email encryption solutions have not been easy to adopt because they are complicated to use and deploy, and can cause frustrating client communications. However, with growing frequency of security incidents impacting their clients, law firms must adapt because clients are demanding, and expecting, greater security of sensitive information. This white paper will detail how email encryption has evolved into a tool that law firms can use to differentiate themselves from the competition and drive new business.

cirius
Secure Messaging



The risk

Lawyers instinctively understand that they have responsibility to protect the confidentiality and privacy of their client's information. It's the foundation of the Attorney-Client Privilege. According to an amendment (Comment 16) to the the American Bar Association (ABA) Model Rule 1.6:

"A lawyer must act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision."

Despite this known responsibility, the legal profession as a whole has done a poor job of making information security a priority. Jody R. Westby, CEO of Global Cyber Risk explains:

"Law firms have never been very good with technology, and now they are struggling, as breaches in firms have made headlines and clients increasingly are asking questions about their security programs. The FBI has issued warnings to firms and held a meeting in early 2012 with about 200 firms in New York to discuss the risk of breaches and theft of client data. Around the same time, Alan Paller, director of research for the SANS Institute, a cyber training organization, revealed an amazing conversation that he had with partners from a New York firm who had been told—and shown—by the FBI that all their client files had been stolen." *(Source: American Bar Association)*

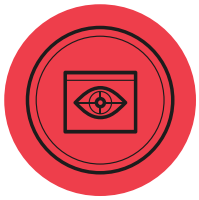
Mandiant, a security consulting firm, has estimated recently that 80 percent of the 100 largest American law firms have had some malicious computer breach. Law firms are an attractive target for hackers because they have access to a treasure trove of business strategies, intellectual property and pending deals. Case in point is the high profile case of the Canadian law firms that had data stolen by Chinese hackers looking to derail a $40 billion acquisition. *(Source: Bloomberg)* Sophisticated hackers have discovered that it is easier to steal information from a law firm than from a corporation because law firms have been slow to employ advanced security technologies.

Client security problems

You can't turn on the news without hearing about a major security breach. ebay, Adobe, SnapChat, Target... the list is constantly growing. Heartbleed and Snowden are now parts of the public lexicon. The ramification for firms is that as corporations are now being forced to invest more heavily in security, they expect their legal partners to do the same. Enterprise information security is now a prerequisite in order to conduct business with many organizations. Some companies are even asking firms to complete 60-page questionnaires detailing their cybersecurity measures, while others conduct on-site inspections.

"It is forcing the law firms to clean up their acts," said Daniel B. Garrie, executive managing partner with Law & Forensics, a computer security consulting firm that specializes in working with law firms. "When people say, 'We won't pay you money because your security stinks,' that carries weight." *(Source: DealBook)*

Firms that continue to trail behind may increasingly lose new business opportunities to more proactive competitors. Should a firm be the cause of a breach, Federal (e.g., HIPAA and GLBA) and State regulations (e.g., state Bar Associations) can be enacted to assess financial penalties, malpractice claims and potentially disciplinary action. In today's environment, organizations in every industry, including legal, must have a security program that meets internationally accepted best practices and standards.



How Email encryption has evolved

To be fair, one can almost understand why law firms have been slow to adopt legacy encryption solutions. Traditional encryption solutions have a well earned reputation for being difficult-to-use and deploy, can cause frustrating customer communications while still leaving firms exposed to security risk and unprepared for e-discovery and potential litigation. Who would want to spend IT budget and dedicate resources to receive that? Organizations in other industries have felt the same pain; however, they are now rapidly adopting next-generation email encryption solutions that have evolved in the following ways.

Its about more than just email encryption
Secure messaging protects and impacts much more than email. It encompasses secure mobile and tablet messaging, legally binding secure e-signatures, secure large file sharing, secure e-campaigns, policy-based encryption, secure web forms and the automated delivery of secure e-statements. It's an integrated strategy for secure communication from any device and any location that replaces a disjointed set of ad-hoc tools that are riddled with security gaps.

Multi-layered security
AES-256 encryption is only the starting point. Organizations need greater control over messages and attachments, and most importantly, tools to remediate inevitable user error. Secure messaging can provide additional controls such as preventing messages from being forwarded or replied to, password protection of the message and attachments, message recall even after a message has been read, and content filtering to stop mistakes before they happen.

Productivity and security
In addition to security, secure messaging can help bring tremendous value by accelerating processes. Real-time tracking in secure messaging enables staff and clients to know exactly when any action has been taken on a message and advance workflows. Being able to send an encrypted large file (e.g., 5 GB) with a secure message reduces the need to use inefficient mail and courier services. You and your clients will be able to send secure messages from the office, at home using Gmail or Outlook.com, at the airport on an unsecure network or while on the move via a mobile or tablet. Workflows never have to slow down because of security, which means that you ultimately deliver faster for your clients.

Client communication
One of the most interesting ways that secure messaging has evolved is that it has the potential to improve how you communicate with clients. Real-time tracking of messages activity gives clients unique transparency so they always know what's happening in a workflow. You can give your clients large file sharing capability, so they can easily bypass frustrating corporate email size restrictions. You can also give clients access to the same email plugins, mobile apps, browser extensions and desktop clients that internal employees can use. Gone are the days when clients have to be driven to an external portal to read and reply to a message. They can have a secure message decrypted right into their customary inbox or mobile device, which makes secure messaging as easy and familiar as traditional email.

E-discovery and archiving
Legacy solutions have struggled to archive encrypted data and also typically force organizations to create separate mail stores. These limitations have left organizations woefully unprepared for e-discovery and at risk for compliance fines due to improper record retention. Secure messaging can now create a single mail store as well as automatically decrypt messages into any archiving solution so that organizations can properly retain and retrieve secure messages in the event of litigation or an audit.

In the cloud
Cloud-based solutions have become the defacto deployment model for email encryption because the large majority of organizations prefer a faster, easier deployment with no hardware infrastructure that interferes with their current network architecture. Cloud deployments also do not strain limited IT resources and are much easier to scale and upgrade in multiple global data jurisdictions. Organizations in heavily regulated industries such as healthcare and financial services are turning to cloud-based email encryption because of the value compared to on-premise solutions.

How to use secure messaging to differentiate and win new business

While email encryption will soon be required by all of your existing and potential new clients, keep in mind that not email encryption is the same. There are vast differences in functionality and end user experience that impact clients. Using a solution like Secure Messaging that has a unique array of patented features enables firms to differentiate themselves as a potential legal partner. Real-time tracking gives unique transparency, enhanced security options provide greater control and privacy, large file transfer, mobile apps and integrations allow clients to decrypt messages and attachments of any size directly into whatever email program they use without having to use a portal. The ability to brand the solution for each firm and attorney creates unique business development opportunities as clients see with each message that you value their privacy. It's email encryption that's easy, more secure, more flexible and more transparent for clients that ultimately accelerates the completion of projects.

Below is a checklist of features that you can use to demonstrate superior secure messaging compared to another firm using a standard solution. There may be some solutions that contend they have a couple of these features, but no one will be able to offer all of them.

	Checklist of Differentiated Features	**You Using Secure Messaging**	**Competing Law Firm**
1	Real-time tracking for internal and external users on any device.	✓	✗
2	Request or provide legally valid e-signatures in seconds right from your email.	✓	✗
3	Password protect messages and attachments for use with delegated inboxes and shared machines.	✓	✗
4	Large file capability (e.g., 5 GB) for internal and external users on any device.	✓	✗
5	Internal and external users have access to plugins, webapps and extensions for use with Outlook, Office 365, Gmail, Yahoo! Mail and more.	✓	✗
6	Internal and external users have access to mobile and tablet apps for Android, iOS, Blackberry 10, and Windows Phone 10.	✓	✗
7	Prevent message and attachment forwards and replies and recall a meesage even after it has been read.	✓	✗
8	Decrypt messages into any archiving solution.	✓	✗
9	Single mail store.	✓	✗
10	Secure web forms and e-statements.	✓	✗

How to choose an email encryption provider

Once you are ready to evaluate secure messaging solutions, here are a few key criteria and considerations to keep in mind.

1

Simple deployment

- Deployment should be fast and even possible in a matter of minutes. If the solution needs more than a few days to deploy then there is the risk of complexity running up high implementation fees and causing delays.
- No hardware to install and no architecture changes makes your life a lot easier. Having to install hardware that affects your network usually requires painstaking internal scrutiny and an approvals process that can take many months by itself. Even data loss prevention features (i.e., content filtering/policy-based encryption) should not require any hardware to install.

2

Ease of use and access

- If a solution is easy to use, user training should not be necessary.
- A secure web portal should be accessible from any browser without the need of a VPN.
- Internal and external users should also be able to send and receive secure messages and attachments from their customary inbox without navigating to a separate browser. Integrations with the following should be available:
    - MS Outlook, Office 365 and Outlook Web Access
    - Gmail, Yahoo! Mail and Outlook.com
    - Android, iOS, Windows and Blackberry devices
    - Windows and Mac desktop

3

Multi-layered security

- AES-256 encryption.
- Options to block message forwards and replies.
- Optional password protection for messages and attachments - ideal for use with delegated inboxes and shared machines.
- True message and attachment recall even after they have been read that doesn't require recipient's permission.
- Content filtering and policy-based encryption.

4

Productivity features

- Real-time, time-stamped tracking of all message activity available in the user interface for internal and external users.
- Secure e-signature provisioning without requiring additional software or third-party intermediaries.
- Secure large file sharing for internal and external users.
- Mobile and tablet apps for internal and external users.
- Secure web forms and e-statements to replace paper documents that need to be mailed.

5

E-discovery and archiving

- Options to store decrypted messages within MS Outlook or Office 365 to create a single mail store.
- Ability to auto decrypt secure messages and attachments into any third-party archiving solution.
- Ability to support journaling of notifications.

Conclusion

It's time for the legal industry to shed its image as information security laggards. Proactive investment in security demonstrates that law firms are taking their responsibility to protect client information with new found resolve. Firms that utilize innovative email encryption can differentiate themselves in the battle to win new clients by delivering not only security and compliance, but also more efficient workflows and improved client communication.

cirius
Secure Messaging