



Email Security in Law Firms

What you need to know and how you can
use secure email to win more clients

Introduction

As clients are demanding greater protection of their information, law firms must incorporate email encryption into their processes. This Whitepaper will describe how secure 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 utilizing 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 whitepaper will detail how secure email encryption has evolved into a tool that law firms can use to differentiate themselves from the competition and drive new business.

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 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.

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.

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 cyber security measures, while others conduct on-site inspections.

Firms that continue to trail behind with adopting a secure email service 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 secure email services with encryption solutions that have evolved in the following ways.

1. It's About More Than Just Email Encryption

[CipherPost Pro®](#) protects and impacts much more than email. It encompasses secure mobile and tablet messaging, secure large file transfer, 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.

2. 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. CipherPost Pro[®] 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.

3. Productivity and Security

In addition to security, CipherPost Pro® can help bring tremendous value by accelerating processes. Real-time tracking in CipherPost Pro™ 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.

4. Client Communication

One of the most interesting ways that [CipherPost Pro®](#) 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 transfer 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 CipherPost Pro® as easy and familiar as traditional email.

5. eDiscovery 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 eDiscovery and at risk for compliance fines due to improper record retention. CipherPost Pro™ 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.

6. 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-prem solutions.

How to Use CipherPost Pro[®] 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 all email encryption is the same. There are vast differences in functionality and end user experience that impact clients. Using a solution like CipherPost Pro® 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.





Next is a checklist of features that you can use to demonstrate CipherPost Pro[®] 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 CipherPost®	Competing Law Firm
	1 Real-time tracking for internal and external users on any device	●	●
	2 Message Recall even after a message or attachment has been read	●	●
	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, Web apps and extensions for use with MS Outlook, Office 365, Gmail, Yahoo and Outlook.com	●	●
	6 Internal and External users have access to mobile and tablet apps for Blackberry 10, Windows Phone 8, Android, iOS	●	●
	7 Prevent message and attachment forwards and replies	●	●
	8 Decrypted 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 email encryption 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 being connected to 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 and Outlook.com
- Blackberry, Android, iOS and Windows Phone
- Windows and Mac desktop



YAHOO!



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 large file transfer for internal and external users.
- Mobile and tablet apps for internal and external users.
- Secure web forms and e-statements that can replace paper documents that need to be mailed.

5. eDiscovery

- [eDiscovery](#) has 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

End-to-end encryption securing the confidential transmission of e-PHI demands an end-to-end solution to ensure that data remains confidential and secure between the message sender and the intended recipient, preventing unauthorized access or loss of e-PHI.

Archiving: An effective email archiving system will enable your organization to meet control objectives for auditing by capturing, preserving and making all email traffic easily searchable for compliance auditors to evaluate. When encrypted and backed-up, archiving provides additional protections for information against loss and unauthorized exposure.

Anti-spam and anti-virus: Protections from spam, phishing, and malware at the email gateway such as email filters and antivirus software will also demonstrate adequate protections against unanticipated threats to the integrity and security of e-PHI.

“It’s refreshing to work with a company like AppRiver that takes the time to understand the unique needs we face as a firm and provides services to match those needs. Even better, AppRiver makes its incredible support team available to help us night or day. If we do have a problem, we always have someone to help.”



James A. Holmes
Director of Information Systems



In 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.

CipherPost Pro®

- Email can travel a long way before it hits your inbox. With CipherPost Pro® from AppRiver, you'll avoid prying eyes along the way.
- Features and benefits:
 - Secure, fast and easy to use
 - Protects confidential information and helps ensure regulatory compliance
 - Provides delivery slip and registered mail options
 - Features centralized management and reporting
 - Enables large file attachment encryption and delivery
 - One-click encryption
 - Includes Outlook plug-in, Windows and Mac desktop agents, browser plug-ins
 - Full-featured functionality for mobile devices including iPhones, iPads, BlackBerry, Windows Phone, Android and more
 - Compatible with Office 365
 - Includes Phenomenal Care™ from our US-based team, 24 hours a day, every day

AppRiver's Phenomenal Sales advisors can provide information on which features are available with CipherPost Pro email encryption service. Contact sales@appriver.com for more information.



Learn more about **CipherPost Pro®**
at www.appriver.com

About CipherPost Pro®

The makers of CipherPost Pro™ believe that email security should complement your email, not complicate it. Our cloud-based solutions for secure file transfer and email encryption work seamlessly with any email to enable secure communication and collaboration anytime, anywhere.