THE COUNCIL of INSURANCE AGENTS & BROKERS

Buyer's Guide: Email Encryption Services

Prepared by Frank Sentner, Director of Technology at The Council
March 2010

This paper has been developed in response to Council members' requests for guidance on which email encryption service would best help them comply with heightened regulations regarding email encryption in certain circumstances. This paper will assume Council members have themselves, with counsel, identified which communications should be transmitted in encrypted form to comply with HIPAA regulations in the United States, FSA requirements in the United Kingdom, or other requirements that they may have identified.

Selection of Companies for this Analysis

For this analysis, The Council is only considering for its recommendation those solution providers that have developed and operate the technology, and not those firms that resell a technology solution from one of the companies listed below.

Assuming that Council members would prefer to implement technology that has proven sustainability in the marketplace, we have focused this analysis on only those providers who have been servicing commercial enterprise customers for more than 5 years. If members are considering purchase from a reseller rather than from the solution providers directly, we recommend that they insist on knowing what solution the reseller is offering, even if it is 'white-labeled' and offered under the resellers' brand, to use this analysis as a decision tool. Finally, these providers have been evaluated from the point of view that Council member firms will not want to require their email recipients to download software or pre-register for an account with a solution provider.

Solution Providers:

- RPost
- Voltage

} *These are referred to as **"Encrypted Delivery Direct"** to Inbox. The recipient receives the encrypted data right in their inbox.*

- Zixcorp
- Cisco Ironport
- Axway Tumbleweed

} *These are referred to as **"Store-and-Forward"** systems. Encrypted data is stored by provider or device, and forwarded to recipient after recipient clicks back to website, registers at the website, and downloads encrypted file.*

Service providers, such as Google/Postini, Symantec/Messagelabs, AppRiver, among others, private label or resell solutions from some of the above companies. Newer service providers are not evaluated here due to a risk of inexperience in being able to service enterprise customers and sustainability in the marketplace.

Council Recommendation: RPost® (www.rpost.com/secure)

The Council's top recommendation is RPost's recently upgraded SecuRmail™ service. RPost has demonstrated its ability to respond to market needs and has continuously enhanced its solutions accordingly. This service upgrade, in particular, has addressed key points of interest for our members: (1)

simplicity for senders, (2) a high response rate for recipients accessing encrypted email, (3) auditable proof of compliance, (4) ability for recipients to reply with encryption, (5) support for compliance with e-discovery, (6) ease of implementation, and (7) flexibility in cost models. For further details, we direct you to the following analysis.

Analysis

Understanding Underlying Purchase Drivers to Prioritize Evaluation Criteria

With heightened enforcement actions by regulators, the purchase driver of email encryption services is no longer whether or not the provider's solution was 'secure enough' but is now how well the provider's solution will protect from fines in the case of a data breach.

All of the vendors discussed in this guide have systems that are 'secure enough' to comply with security 'best practices' and regulator guidelines for encryption. Further, customer IT departments can select various methods of making these encryption services available to senders, with all of the vendors discussed having options for sending encrypted ad-hoc via a desktop plug-in or key word insert, or auto filtered by policy at the outbound gateway -- thereby making the sender experience equally simple across each of these discussed vendors. Therefore, these points are not the focus of our analysis. What we will focus on, as top level evaluation criteria, is **how well the solutions will protect from fines in the case of a data breach**.

When considering data breach, we are considering two points, a data breach when the data is (a) **within the sender's control** (i.e. where the email is sent from sender to recipient - "security of sender-controlled data"); and (b) **after the data leaves the sender's control** (i.e. if there is a data breach on the recipient's system or after the recipient forwards the information on to others - "downstream data breach").

Top Level Evaluation Criteria

SECURITY OF SENDER-CONTROLLED DATA

(1) Simplicity for sender, high response rate for recipients accessing encrypted email:

> Many email encryption systems are too cumbersome, resulting in less use and therefore, potentially more exposure to a data breach. Most of the systems (other than RPost and Voltage) are 'store-and-forward' email systems which require the recipient to take significant action for the recipient to retrieve the email – often clicking through to a website, setting up an account with the provider, installing software plug-ins on the recipients' computer, which typically is not allowed without the recipient having administrative rights (rare in corporate environments), and then downloading the message to their desktop. We have heard from insurance brokers that

these systems are rendered virtually useless due to the low response rate for clicking through to download the material. Some of these store-and-forward systems – like Zixcorp, Cisco's Ironport, and Axway's Tumbleweed – require recipient registration for a more seamless experience, but in reality, if there are hurdles to getting the information to the recipient, the fallback is unfortunately for the sender to re-send the email unencrypted. Therefore, we conclude that there is greater risk of a data breach or fines with these "store-and-forward" systems.

RPost and Voltage are the only providers that we evaluated that deliver the encrypted material right to the desktop, reducing risk as compared to the other providers.

PROTECTION FROM DOWNSTREAM DATA BREACH

(2) Auditable proof of compliance:

It seems that only RPost has a robust mechanism in place to provide an auditable record of precisely what message content (body text and attachments) was in fact sent and received in an encrypted manner to each intended recipient. This is important because, in the case where there is a data breach after the email has reached the recipient (in the recipient's environment, or after they have passed the information along to others), the sender will need to retain information to prove that the breach did not happen "on their watch" – that they in fact complied with the data security requirements and delivered the information in a compliant, encrypted manner.

RPost addresses this issue by having built its encrypted email service on top of its core Registered Email® service, which The Council endorsed in 2004 as the best way to prove email content, time, and delivery with court-admissible records. By doing this, RPost provides not only effective encryption, but also the most robust proof and record of compliance with the rules of regulators.

Voltage, while having the benefit of encrypted delivery direct to the recipients' inbox – like RPost -- does not provide any mechanism to prove what email content was sent and received encrypted. Voltage support confirms that there is no proof record and suggests that this is an 'infrastructure' issue and not part of their encryption system.

Zix recently added a point in their data sheet claiming that their system's "time-stamping and authentication provide irrefutable proof of delivery and receipt." However, when asked to describe this certified receipt and how it may be authenticated, Zix admits to a simple text-based 'open' receipt – a text receipt that can be easily altered with a few clicks, tells nothing of the message content sent and received, and relies on the recipient accessing its website to download the encrypted information to generate such a receipt. This has very little evidentiary value and falls short of auditable proof of compliance as well.

Axway's Tumbleweed and Cisco's Ironport do not address this issue in their materials, and due to their short storage period of data in the store-and-forward process, a breach investigation soon after the send time would be even more difficult to trace. An offering of a longer-term message archive would likely not solve this issue either as there would remain challenges of associating the message content with the records of encrypted delivery, in a manner that could be easily ported to regulators and then authenticated, in the case of a data breach.

We believe this is an important (and often overlooked) evaluation criterion, especially considering that Council members have placed a high value on encrypted email services fulfilling the need to **protect them from fines in the case of a data breach. RPost is the only provider evaluated that fulfils this requirement.**

Secondary Criteria

The following four points are important but secondary to the points previously discussed. Of these points, RPost presents some clear advantages over the others noted.

(1) Ability for recipient to reply encrypted: This is a clear requirement and all of the providers evaluated fulfill this requirement.

(2) Support for compliance with e-discovery: RPost has the most robust record for e-discovery purposes, along with a simple mechanism for an administrator to decrypt such records as needed. These records are embedded within RPost's court-admissible Registered Receipt™ transaction record.

(3) Ease of implementation: RPost has been reported as the simplest to implement for Council member firms – either by way of an Outlook, Lotus, Groupwise, Zimbra or other plug-in; through certain managed email service providers; or as an embedded application within certain appliances. We have been informed that RPost will be releasing a Blackberry plug-in in the April-May timeframe.

(4) Flexibility in cost models: Again, RPost seems to have the most flexibility here, in terms of pricing and plans. They have opted to provide services either on a pay-per-use basis with pricing published on their website (with all software, start-up, service, support, training cost fully loaded into a cost equivalent to a postage stamp per use), or unpublished per user monthly or annual licenses. Further, RPost includes its Registered Email® legal delivery proof and eSignOff® electronic signature services at no extra cost. Others require up-front commitments, appliances, and generally far less pricing flexibility. We have also negotiated a special Council-member discount with RPost – simply mention during the sales process that you would like "CIAB special pricing".

With these secondary evaluation criteria, RPost remains favored as compared to the other service providers analyzed. Further, RPost has shown an ability to continuously innovate and update its services, which reduces risk of obsolescence and demonstrates technology leadership.

Comparison Chart

FEATURE	*RPost*	*Store-and-Forward*	RPOST BENEFIT
End-to-end encryption delivered directly to recipient inbox with no 3rd party storage of emails or attachments.	Yes. - No links for receiver to click - No accounts to create - No software to download	No. - Recipient must click on link, complete registration or download software to view message	Highly secure, practical, and user friendly as compared to an average open rate with store-and-forward systems reported to be less than 50%.
Auto-email giving awareness to receiver with decryption password (optional).	Yes. - User friendly, low complexity - Receiver is aware - No need to contact recipient	No. - User must click on link and create account or sender must pre-arrange password	Recipient does not need to contact sender for decryption password. Password email gives notice to recipient that an encrypted email is coming.
Proof records of delivery, content, and time; regardless of whether the receiver chooses to open the message. Proof that remains verifiable at a later time in case of a security audit.	Yes. RPost's Registered Receipt email provides a verifiable forensic analysis of the message giving proof of encrypted content sent and received, with a timestamp, regardless of recipient action.	No. - If message is not opened the sender does not have a record that the email was delivered to recipient, and even if a record is provided, there is no easy way to authenticate the record for proof of compliance with encrypted content delivery requirements.	RPost has legal delivery proof regardless of any recipient actions, fulfilling requirement to send message and proving compliance with encryption requirements in case of a downstream data breach.
E-discovery and records management module: Auto-delivery of master password spreadsheet to company manager or help desk.	Yes. - Company protected from future disputes involving content or email timing - Able to prove content in a future dispute - Prove compliance with encryption requirements	No. - Future proof of content not available after message is deleted from provider's system - No proof of content	Permits the sending organization to decrypt message records using the Registered Receipt email if message is subject to litigation or e-discovery requests in the future.
One-click optional encrypted replies back to the sender.	Yes.	Yes.	Creates a secure, encrypted communications loop between sender and receiver.
No software or hardware needed. No setup costs or hidden fees. Flexible pricing.	Yes. - Offered as service with pay-per-use or pay-per user plans. -Optional filtering by policy with appliance or message filtering partners - No hardware - Outlook/Lotus desktop installation options	No. - Generally require hardware or appliance - Require software on server or redirect of outbound mail to service provider	Companies can get started in minutes, as easily as downloading and installing an Outlook plug-in, which provides all capabilities.

Disclaimer: This analysis has been provided for information only. The Council does not provide legal advice and disclaims any liability due to any party's reliance on this analysis for selection of any particular software. For recommendations to your specific circumstances, please consult your own legal and technical consultants. Trademarks referenced in this document are property of their respective owners and are used here to reference their owners' commercially available products and services.