Article Synopsis: *While using Real Time is the best option for moving sensitive client data between agents and carriers, independent agencies and carriers still must use email in certain circumstances and are in need of workflow friendly secure email solutions. Proprietary email solutions create inefficient agency workflows, require the retention of additional passwords, and require agents to go to the carrier Web site to retrieve email. Agencies and carriers are encouraged to implement a much more efficient and cost effective approach to secure email by enabling their email servers for TLS (Transport Layer Security) email encryption. This article explains how TLS works.*

Protect Your Clients with Secure Email Using TLS

By Jim Rogers, The Hartford

Email is now entrenched within business workflows and is how a significant amount of business is transacted between agents and carriers. The words shared between the parties are often critical to the business relationship and contain information of a sensitive nature that if lost or stolen could be harmful to either party.

Why Secure Email is Important

The use of Real Time rather than email is the best option for moving sensitive client data between the agent and carrier when available, because Real Time is highly efficient and transports the data directly between the agency and carrier systems in an encrypted form.

However, when email must be used to send communications with sensitive client information (such as that contained on some commercial lines applications), it is important for agents and carriers to start to use secure email. If the email is not secured, the contents of the email and any attachments can be intercepted and read as they travel across the Internet, in the same way an open postcard can be read when sent through the mail. If an unsecured email is intercepted, the agency would face a security breach creating a significant risk to the agency's reputation and potential E&O exposure.

The Inefficiency of Traditional Secure Email Applications

The traditional approaches to protecting email have included using tools to encrypt the document attachments, or services such as ZIX or Tumbleweed. Encryption of the document attachments suffers from difficulty in using the tools (which need to be purchased and learned) and remembering decryption passwords. Services such as ZIX or Tumbleweed insert themselves into the actual transmission process changing where the email is sent and how the recipient reads it, as well as adding additional costs due to usage or licensing fees.

There is no shortage of email protection products. Each vendor offers its own benefit package in what is typically a proprietary solution. While there are market leaders, customers looking for the best solution don't always follow this metric. As a result, Company A often cannot share encrypted email with Company B since they have implemented different proprietary solutions. This lack of convergence is troubling and can be expensive since multiple products and services must be implemented and used by one company to simply protect its email to other companies.

In a browser analogy, imagine if you needed to use a different browser for each of the web sites you visit. The web site owner would sell you the site browser and instruct you to use it whenever you visit. In this scenario you would have to maintain a list of the browsers to use with each site you like to visit.

Now consider having to go to each carrier's Web site to retrieve secure email, learning the different workflows and functionality of each carrier's email application, and remembering a whole new layer of passwords for each carrier's email. Sounds pretty ugly, doesn't it?

Enter TLS: a Better Alternative Built Upon an Open Standard

Enter into the world of standard designs, mechanisms and solutions. We see the benefits of standards all around us. Width of road surfaces, train tracks, and the vehicles that travel on them are good examples of where standards are crucial. It would severely impact travel if one road or track could not "connect" to another. The proprietary email encryption solutions mentioned above are good examples of a world without standards. One company's email safeguard may not be able to communicate with another's unless a solution such as TLS is used.

TLS (Transport Layer Security) provides an IETF-defined (Internet Engineering Task Force) industry standard protocol to protect emails sent over the Internet. It is built into most email gateways used today (MS Exchange/IBM Lotus Notes) and is simply "turned on" via a click of the mouse. TLS requires no changes to the end user (sender or receiver)—they simply benefit from the encryption it provides during transmission.

How TLS Works

Under the covers, TLS operates independently of the email user. When an email is sent from one domain (Agent or Carrier) to another (Agent or Carrier), the servers that control transmission negotiate to determine if TLS is enabled. If it is, then the servers transmit the email within an impervious TLS tunnel that protects all message content including attachments.

Carrier and agency email administrators can set the TLS option to send using TLS when sender and receiver are capable (opportunistic mode), send only if both parties are TLS capable (required mode), and send without protection if TLS is not supported by both.

It is highly important that the agency use an IT professional to set up TLS on its email servers for incoming and outgoing emails. Your IT professional can also tell pretty easily which of your carriers are enabled for TLS. It is also necessary for the agency's third party spam/anti-virus service to be configured to send and receive TLS encrypted email. Many third party hosted email applications do not appear to have incorporated TLS, but agents should inquire of their vendors.

TLS provides protection between the agency and carrier email servers. The agency's IT professional also must take care to employ the proper security safeguards to protect agency information, as well as emails, while within the agency's systems.

TLS also provides a practical way for an agency to provide a secure email pathway for communications to and from commercial clients that have the capability to TLS enable their email servers. This added measure of security will be appreciated by clients and will provide them with the capability to provide for more secure communications with their other trading partners which can enable TLS.

TLS is a security manager's dream solution—one that requires no work on the part of the end user yet protects email content. It uses an industry standard protocol that is freely available and implemented on most email platforms. For the agency, it is more cost effective than proprietary vendor email solutions and is already included on most email servers. The added cost for the agent involves the fee for the agency's IT professional to properly enable its email server for TLS and the cost of an email certificate (between $70 and $400 annually depending upon the email server's configuration). And for individual agency staff, does not require set up, training or having to remember and use a password to retrieve every email.

In this day and age of focus on security, all email gateways and servers should be configured to use TLS if it is available. Encourage your carriers to provide you the TLS option for secure email and explain to them how TLS is a far preferable alternative for agents than having to learn and then use each carrier's unique proprietary secure email system.

For more information on TLS, please see "Email Encryption via TLS; Frequently Asked Questions for Agents" at www.independentagent.com/act at the "Agency Security/Customer Privacy" link.

Jim Rogers (Jim.Rogers2@thehartford.com) is Director at The Hartford and is responsible for Distribution Technology Strategy. Jim also chairs the ACT TLS Email Encryption Work Group and produced this article for ACT (www.independentagent.com/act). *This article reflects the views of the author and should not be construed as an official statement by ACT.*