**Why You Shouldn’t Email Sensitive Corporate Documents**

**By David Strom**

**(written for Intralinks, 2/12)**

Email may be the default way people share business information – but it remains a problematic way to share anything sensitive.

Email traverses the public Internet in plain text, and can be easily copied or intercepted. Just ask the Gmail users famously hacked in 2010 and again in 2011 or the U.S. Chamber of Commerce, which had at least six weeks worth of email data containing sensitive information stolen in a breach that was widely reported in December 2011.

Today, as the business requirements of the world’s economies drive increasing inter-enterprise collaboration, the use of email to share necessary collaborative information creates unacceptable risks in security, compliance and – particularly – document control. If you are collaborating over a confidential document or data, the last thing you want to do is email it back and forth over the Internet

“Yet that is exactly what most businesspeople do, because of email’s ease and familiarity. Secure email solutions intrude on that ease-of-use,” says Christopher Ford, Vice President, Product Management for IntraLinks, provider of the new Connect cloud-based platform for secure, compliant inter-enterprise content sharing and collaboration.

Nevertheless, there are ways employees can use email to share sensitive information with existing and new partners ad hoc, as the need arises, yet with a central point of governance that enables the enterprise to stay in control of information – even *after* a document has been shared.

This article explores several secure email solutions and some of the choices and trade-offs involved in sharing documents securely via the Internet.

**Consumer-Oriented File-Sharing Solutions**

Perhaps the most popular alternative to emailing documents is to use one of dozens of consumer-grade file-sharing solutions, such as yousendit, dropbox or box.net. With these services, you upload your document to their servers and email someone a link to it. Originally created as a way around email attachment file-size limits, these sites also became popular for synchronizing files between home and office computers and accessing files from smartphones.

But these services are risky for enterprise use. There are numerous examples of confidential information being inadvertently distributed, sometimes due to poor authentication protocols (dropbox’s authentication issues have been [well documented here](http://dereknewton.com/2011/04/dropbox-authentication-static-host-ids/)). The recent FBI raid on MegaUpload is an extreme example of one risk: even legitimate users of this file-sharing site have lost access to their content.1

In addition, as a kind of “Bring Your Own File-Sharing Tool,” these services are mostly invisible to the IT department. Even when IT is aware of their use, the services generally lack transaction logging, which makes document control problematic and impedes litigation preparedness.

**Secure Email Alternatives and Add-Ons**

Many alternatives are available that enhance email security to different degrees, and with varying levels of ease-of-use and deployment difficulty.

* **Fully encrypt the email** conversation between sender and recipient. Secure email has been around for more than a decade and ensures that the recipient is the only person who can read your message. Aside from the public key flaws reported in February 20122, most IT departments find encryption tools cumbersome to use and manage, and they create friction and intrusion into users’ daily email habits. Adds IntraLinks’ Ford: “This approach also doesn’t give you control over a document after the user has received it. You don’t get visibility into whether the person opened or forwarded the document, and you can’t revoke access.”
* **Secure file transfer protocols** (FTP) have also been in use for many years but are equally cumbersome to use. You have to set up the link ahead of time and make use of a specialized client to do the transfers. The FTP servers have to be maintained by IT and generally appeal to just IT-types.
* **Data leak protection** (DLP) products are great at identifying security breaches after the fact but don't do much to help keep your confidential information contained within your enterprise. They are mostly used for compliance and other regulatory reasons.
* **Secure Intranet/collaboration systems** take a great deal of effort to setup and maintain but generally don't get much user interest or adoption because they don't integrate with the email stream that most of people use in their daily communications. In addition, they must be extended in order to meet the needs of inter-enterprise collaboration.
* **Secure document delivery services** often offer the best combination of features, security and integration with email networks. Cloud-based services such as IntraLinks Courier leverage the security, control and digital rights management inherent in the company’s core inter-enterprise content sharing and collaboration platform, yet with integrated ease-of-use that can make the increased functionality virtually transparent to the user (depending on the user’s email client).

**Secure Document Sharing Issues**

As you evaluate any of the above kinds of services/solutions, consider the following issues concerning how you intend to share confidential information.

* **Do you need secure intra- or inter-enterprise collaboration?** Many secure email enhancements and add-ons aren't designed for easy external communications, but inter-enterprise collaboration is clearly on the rise as a core requirement.
* **Can you recall sent messages?** This is an important feature, especially in today's world of limited user attention spans and multitasking that can introduce mistakes into the workflow. “One of the biggest sources of data breaches is the ‘auto complete’ feature in the email ‘To’ field,” points out Ford. Document delivery services provide the ability to delete files past a certain date or prevent files from being forwarded or printed.
* **What happens when someone leaves your company?** How easy is it to "expire" his or her account so that the former employee doesn't have access to the secure communications path? This is a problem for the email encryption products that require careful crypto key management to ensure that a former employee's keys are turned off.
* **How does the service affect users’ existing email experience?** Many of the above services require difficult add-ons to your existing email networks, or require you to make changes to your networking infrastructure or applications. The less of these changes, and the higher the level of integration, the better. “For Microsoft Outlook, for example, there’s a plug-in that allows you to just push a button and use Courier to send your email. You’re still filling out an email and making an attachment, but on the back end we strip out the attachment and send it along in a separate secure channel,” explains Ford.
* **Can you authenticate recipients and thwart malware such as key-loggers?** These are necessary abilities for any service. Of note, a recent *New York Times* article describes extreme security measures taken by some international business travelers – measures that seem more appropriate to spy films. These include traveling with temporary smartphones and laptops that are wiped clean before departure and again on return home, copying passwords from a USB drive to thwart key-logging malware and removing phone batteries to prevent remote activation of the microphone during confidential meetings.3

**Conclusion: Integrate Document-Sharing Services With Your Email**

A full-fledged, cloud-based platform for secure, compliant inter-enterprise content sharing and collaboration is the ideal way for your enterprise to pursue the partnerships necessary to business success while maintaining security, compliance and control. But few organizations can prevent their users from emailing sensitive documents.

Services such as IntraLinks’ Courier enable the integration of such secure document-sharing platforms with email. “What we’re really doing is hosting and posting files for secure access; we’re not delivering files over email. But we’ve packaged it in a way that it looks like email so that the ramp-up for users is very low,” explains Ford.

Thanks to the familiar user experience services like Courier provide, their proven security, control and compliance features can make email document sharing safe, after all.

Sources:

1. Megaupload's Ripple Effect - WSJ.com, 25 January 2012
   1. <http://online.wsj.com/article/SB10001424052970203806504577181201072864644.html>
2. Researchers Allege Defect in RSA Public Keys, Findings Questioned, *ReadWrite Enterprise*, 15 February 2012
   1. <http://www.readwriteweb.com/enterprise/2012/02/researchers-allege-defect-in-r.php>
3. Traveling Light in a Time of Digital Thievery, *The New York Times*, 10 February 2012
   1. <http://www.nytimes.com/2012/02/11/technology/electronic-security-a-worry-in-an-age-of-digital-espionage.html>