



Punchstock.com

Solutions for the MAILSTREAM

Ever since written communications began there has been a need to keep some of these communications more secure and private than others. Today, much of this written communication is exchanged through electronic mail, and yet email security still remains something of a blindspot for most organizations.

There are an increasing number of business scenarios now relying upon the

Companies must find a solution that protects the confidentiality of data sent via email, report Andrew Kellett and Richard Edwards

use of secure and reliable email, but we believe that only a fraction of these are being conducted in such a manner. There is undoubtedly a perception within the business community that messages sent using corporate email facilities are inherently secure. If only they knew! IT departments are fully aware of the vulnerabilities associated with email traversing the internet, and in some cases have implemented server-centric solutions to

address the problem, but unfortunately this covers only a tiny fraction of email traffic, and can hardly be considered an ideal, end-to-end solution.

Standards for secure email have been around for many years. Indeed, secure email using Public Key Infrastructure (PKI) was defined by an internet standards committee nearly a decade ago. Commonly referred to as S/MIME, the facility to send secure and digitally signed email messages is present in all mainstream email clients, and yet few organizations appear to make this feature available to their users.

Considering the many points of vulnerability that exist between sender and recipient, it is incredible how blasé we have become in our use of this particular communication method.

Despite the ubiquity of electronic distribution file types, such as Adobe's Portable Document Format (PDF), many organizations still use expensive courier services to hand-deliver important business documents. Why is this? The answer in part has a lot to do with the idea of "Registered Delivery." Again, email clients have the capability to request a "delivered receipt" and even a "read receipt," but these are often dismissed or ignored by the message's recipient.

If the business community is to rely on email as an alternative to courier services, then it must provide a truly reliable, secure, cost-effective and non-repudiable service which meets the requirements of industry and government regulators and compliance initiatives.

The following list represents the must-have elements of such an electronic, certified delivery service:

- No significant IT administrative overhead
- Scalable for use with large numbers of senders and recipients
- As ubiquitous as the most common internet technology
- No effective limit on document size
- No pre-established coordination requirements between sender and



In business circles, over 70 percent of security breaches emanate from within the confines of the organization.”

recipient

- No user training requirements
- Integration with internal and trusted partner email systems
- Message tracking and status reports to accommodate compliance requirements.

Sensitive email documents need to be protected both in transit and on arrival. Unprotected email, which probably represents more than 99 percent of all email communications, is easy to intercept and access, and if malicious intent is part of the equation, modify or pass on for other nefarious reasons.

In business circles, over 70 percent of corporate security breaches are reported to emanate from within the confines of the organization, and are being committed right now by a company's own employees. This fact alone makes a strong case for ensuring that important email messages can only be distributed and accessed by the intended sender and recipient, and that after they have been read they can be archived to a secure area retaining an appropriate level of security.

One other area that businesses should consider when thinking about securing sensitive company information is that of the legal consequences. The 1998 version of the *Data Protection Act* puts an emphasis on information owners to ensure that material of a sensitive nature

is properly protected.

The act implies that sending out unprotected email, under certain circumstances, is a dereliction of care. It contains eight data protection principles, covering areas such as ensuring that data is processed fairly, is lawfully obtained, and is only used for the purposes for which it was intended. The data must be accurate and where appropriate kept up-to-date, and should be stored for no longer than is necessary to preserve the rights of the individual users.

Providing protection facilities for important documents that need to be moved around between computer users, either internally or externally, makes common sense. Any encryption solution deployed needs to be flexible in its approach, and at the same time unrestricted in its operational use.

It must of course be highly secure when used, but it should not add layers of restrictive bureaucracy that would cause it to remain unused. There are some organizations that have a need to protect most of their communications, and for these a more formal approach to communications management is required. But for the rest, the best approach is to allow users to manage their own communications and have the protection facilities available for use whenever necessary.

Email travels across the internet in plain text, bouncing from router to router until it reaches the recipient's email server with levels of security probably less than that of a picture postcard traversing the postal system. Secure email is clearly a fundamental requirement for financial institutions, governments, healthcare and other organizations with a compelling need to protect confidential information; but it is also an issue for every other organization currently conducting business on the back of a digital postcard. ■

Andrew Kellett and Richard Edwards are research analysts at Europe-based Butler Group