

Who Should Read This Brief?

If your company uses email to transmit any commercial information, regardless of size you may have a duty of care to ensure your emails and their attachments are retained in a tamper proof environment.

Equally as important is the cost associated with losing and reviving (or attempting to find) old emails. By reading this Brief you should have a clear understanding of the benefits associated with Active Email Archiving. This brief is suitable for business managers and IT staff.

Synopsis

Recent research⁽¹⁾ indicates that more than 70% a company's intellectual property may be contained in current and historical emails and their attachments. This white paper discusses how to ensure that this information is protected and secured for future revival.

Security comprises security of availability of email as a service, security of transmission, security of the archive file system and lastly security of the datacenter and its connectivity.

This paper look at the key issues associated with appropriate Online Email Archiving Security Strategies.

Background.

Like many forms of communication email has "crept up" on IT departments as a fundamental form of inter and intra business communication. Historically the most important form of communication was the POTS (Plain Old Telephone Systems). This was certainly supplemented but not replaced by in the short term the Telex machine and subsequently the fax machine. Importantly the fax machine formed the first foray into using hardware to send and receive legal documents. However since 2000 email, most would argue, has replaced the POTS as the primary form of communication. Interestingly, many companies are training graduates on the appropriate phone techniques rather than email, reflecting how new employees default to email to communicate.

Since emails are such a widely used form of legal correspondence between companies and employees it is critical to be able to access quickly a true and correct copy of emails, should staff not be able to locate them locally. Indeed, in some jurisdictions it is now a criminal offence not to take due care to ensure emails are securely archived and more importantly quickly "discovered" from a tamperproof source.

Different Deployment Types: Online Versus Offline

In seeking to identify key security considerations two basic ways of deploying Email archiving are used. Whilst this paper focuses on Online, for completeness some comments are offered on the appliance market.

⁽¹⁾ ITNews March 2007

Appliance Based Archiving

Offline Archiving (Appliance based) is typically used where there are more than 500 users whose emails should be archived. All incoming and outgoing email whether internal or customer facing is transparently copied to a stand alone internally located hardware appliance.

Typically these appliances employ a hard disc sub-system for accessing more recent emails and a tape subsystem for archiving permanently the WORM (Write Once Read Many) tapes. It is important to note the tape library needs to be consistently rotated and stored with minimum pricings typically starting at around \$8,000.

Clearly key considerations are the physical security of the appliance and tape. Typically all traffic between the Email server such as the Microsoft Exchange Server and the appliance is encrypted.

Online Email Archiving Services

A relatively new addition to the Email Archiving industry is the addition of online Email archiving services. These transparently intercept and duplicate all incoming and out going emails. Clearly a benefit for security is that all archive data is maintained off site in a tamper proof environment.

Online Archiving Security Considerations

A clear advantage of online archiving is it ensures off-site tamper proof storage and retrieval for all incoming and out going emails.

For remote storage the key security aspects are:

- Email transmission encryption
- Data Center physical security and connectivity security
- File System Security
- Data Encryption

Email and Exchange Sync Transmission Encryption

All emails between the end user and the data center are encrypted using the standard based best of breed encryption technique of SSL.

The TLS protocol(s) allow applications to communicate across a network in a way designed to prevent eavesdropping, tampering, and message forgery. TLS provides endpoint authentication and communications privacy over the Internet using cryptography.

Typically, only the server is authenticated (i.e., its identity is ensured) while the client remains unauthenticated; this means that the end user (be that a person, or an application such as a web browser), can be sure with whom they are "talking".

The next level of security—in which both ends of the "conversation" are sure with whom they are "talking"—is known as mutual authentication. Mutual authentication requires public key infrastructure (PKI) deployment to clients.

TLS involves three basic phases:

- Peer negotiation for algorithm support
- Public key encryption -based key exchange and certificate-based authentication
- Symmetric cipher -based traffic encryption

File System Encryption

Encryption is symmetric block cipher that can be used as a drop-in replacement for DES or IDEA. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for both domestic and exportable use.

All databases are unique and encrypted eliminating cross pollination of data.

Web Mail Browser Encryption

When end users wish to use the web browser for either discovery, remote or emergency access to the remote online email archiving all data transmission is archived using SLL as with Email Transmission.

About MailRevive™

MailRevive™ is a managed application service that operates in conjunction with your existing IT network to ensure the protection, preservation and continuous operation of email communication for your business, while providing on-demand access for users anywhere and anytime. For any size business MailRevive™ will ensure that email data is automatically filtered and preserved, can be intelligently discovered, easily recovered and that continuous access is available at all times.