

Reducing the Risk from E-mail within Microsoft Exchange / Outlook

Protecting the organization, system and individual

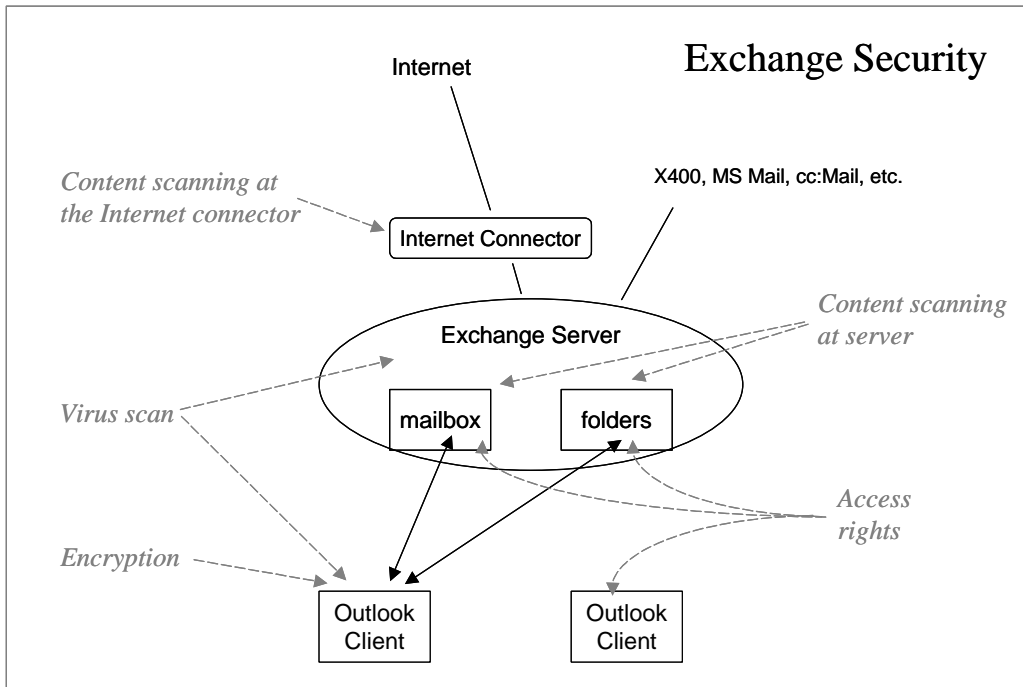
C2C Systems July 2002

In this paper we take a look at some of the actions that companies can undertake to minimize corporate risk associated with the messaging system. Microsoft Exchange Server is a well-constructed application offering not just e-mail, but a range of other related applications that are seen as the basis of the modern groupware platform. A Risk Control Strategy directly translates into security and related systems administration activities, and needs to be in place as part of a coherent Exchange strategy.

Although Microsoft has developed Exchange to be a securable system, the architect responsible for the system design is still responsible for ensuring the security of the messaging system, the individual user and the corporate entity.

This paper identifies six common themes of Risk, Security and Exchange, and moves on to look at three of them in more depth, as the first three are widely understood and implemented. This paper does not examine security related to Exchange Server Administration access nor the architecture established by your design team, but looks at the risk factors we see as affecting the integrity of the *user* and *corporation*. These being:

- 1 Virus control
- 2 Encryption
- 3 Content control at the Gateway
- 4 Content control of the Information Store
- 5 Mailbox and folder security
- 6 Governmental and Regulatory security requirements



1. Virus control

The problems are well understood and today the vast majority of organizations have this under control with Exchange and/or desktop scanning capabilities in place. Systems remain open to infection during the first few hours' life of a new virus. Administrators can use content tools (both gateway and information store) to search by subject, attachment, etc. to find and remove offending e-mails in advance of the real solution.

2. Encryption

Again this is a well-understood subject. This is primarily for protecting corporate information from prying eyes and usually implemented for a selected set of individuals in the organisation. There are a number of products available for use with Exchange.

3. Content control at the Gateway

This has been a hot subject in the last couple of years, with a variety of products available to monitor content passing between Exchange and the Internet. The prime need has been the potentially litigious issues of sexual and racial content,



but more recently companies have become more aware of the damage caused by competitive and/or company confidential information passing to the Internet. Scanning of mail takes place at the entry point to the Internet. There are a number of products around to fulfil this task. In general security takes precedence, even if performance is degraded. By its nature, scanning is in real-time only and not retrospective to mails that passed through in the last week, month or year.

Remember a gateway/connector is not always only to the Internet. Most content scanners only work on the Internet connector, so you may have other access points to your system.

4. Content control of the Information Store

This is the ability to scan the Information Store for the same security breaches as we may be looking for at the Gateway. Recent high profile stories associated with e-mail content have resulted in costly litigation and PR related crises for some major corporations:

Smoking gun e-mail has become so common in workplace lawsuits that almost 10% of US companies have been ordered by courts to produce employee e-mail, and 8.3% have battled sexual harassment and/or sexual discrimination claims stemming from employee e-mail and/or Internet use. 2001 survey www.epolicyinstitute.com

High profile cases include:

The New York Times Company fired nearly two dozen employees and reprimanded another 20 workers for sending and/or receiving eMails that included sexual images and offensive jokes.*

Chevron Corp. in 1995 was ordered to pay female employees \$2.2 million to settle a sexual harassment lawsuit stemming from inappropriate eMail circulated by male employees.*

*Source: www.epolicyinstitute.com

Norwich Union, a UK Insurance company was forced to pay \$450,000/ £700,000 damages, after it was found to have libelled Western Provident Association through employee comments on its internal e-mail system.

In such cases, information store content control allows a company to find the perpetrator(s), and/or trace all such records existing. It can establish exactly what was said in case further action is required.

Information Store scanning can also tell you a lot more about the use of your e-mail system and what your users are storing in it. Most of this is outside the obvious scope of security, but it can demonstrate weaknesses of ePolicy.

Scanning enables an administrator to find, for instance,

- the number of AVI files being sent around in a company
- who the main distributors of such files are



- the number of large documents stored in the system, or even specific document names
- new viruses which may have entered the e-mail system prior to virus detection software being updated

The major benefit of Information Store scanning is that it can look at all messages passing within the organisation – messages sent or deleted¹ or any item still held in the information store, whether sent this week or last year. It can also scan content in a highly confidential fashion, so that even the Exchange or security administrator need not actually read the questioned content. The e-mail may simply be flagged as ‘outside ePolicy’ and sent or displayed only to the appropriate company executive who can then take action as necessary.

Implementation is straightforward as it is server based. Scanning large information stores may appear to be slow but this is directly related to the volume of messages held within these stores. A well-structured scanning rule that searches according to well defined criteria will reduce the time implication.

C2C’s Active Folders Content Manager is capable of providing content control of the information store as part of an E-mail Risk Control strategy.

5. Mailbox and folder security

Who is reading your e-mail?

This theme has been ignored by many organizations up until now, who have concentrated on securing their external boundaries. However, there are now real business imperatives driving companies to ensure that their confidential internal data cannot be compromised. Public listed companies need to keep their information proprietary until they publish their results. With the majority of company executives relying on Outlook as their main data store, security of access has to be an issue.

The thought that e-mail access could be compromised is probably far from the minds of most company officers, but these people are the most likely targets of mailbox hackers.

Finance and Human Resources executives are most likely to be targeted.

In your company a hacker can be anybody who

- feels they’ve been mistreated
- seeks insider trading information
- wants the inside story on their colleagues to benefit their career path.
- is merely curious.

¹ This refers to the ability to scan the Exchange Dumpster, if it is configured. A rogue user may have send and deleted mails, thinking they are safe from detection, but unaware Exchange may be holding this data for another 30 days (this period of time is defined when enabling the dumpster).



The consequences of their actions can be devastating. C2C has heard of employees finding they have access to a department's public folders, and changing permissions or even deleting whole trees of content, impacting months or even years of work.

So how real is the threat to mailbox or public folder permissions?

In reality, and particularly in medium to large organisations it's not uncommon to find errors in permissions granted at set-up or more likely during routine administration.

Also, system and department configurations tend to change over time, so users may be inadvertently granted access when these alter, or users may carry historical permissions with them into different departments.

In reality, where C2C has had reason to talk to or work with customers in the area of e-mail permissions, we have not seen one multi-server Exchange system where the permissions were as per the administrator's expectation.

Of course mistakes in permissions are usually unintentional, and the user is often unaware they have the access rights. Additionally, mailbox access should be password protected, but many companies have open mailbox access once user security had been verified. Even when passwords are enforced, how many people have their partners name, football team, pet's name or nickname as their password? A little knowledge can go a long way to getting a password right.

According to a recent British study, passwords are often based on something obvious. Around 50 percent of computer users base them on the name of a family member, partner or a pet. Thirty percent look to a pop idol or sporting hero.
<http://www.cnn.com/2002/TECH/ptech/03/13/dangerous.passwords/?related>

In order to establish permission set-ups and provide an easy correction method where breaches were found, C2C has developed software to verify and where required modify Exchange permissions. The approach offers both the ability to check permissions on a mailbox or folder, and conversely the permissions assigned to a user. In this way, we can see

- who has access to a given folder or mailbox – for example, has a manager just granted rights to a secretary
- permissions granted to a user – for example, which managers' mailboxes does the secretary have delegate rights to.

Two main corporate groups can make use of this solution.

- Security advisors can run periodic permissions audits according to ePolicy. Frequency of audits may change with the seniority of the target mailbox user.
- Exchange Administrators also use the software on an ongoing basis to better maintain security. eg The ability to check permissions associated with a user is necessary when someone leaves the company. A quick



check would ensure their mailbox was deleted, but also the entire public information store could be searched for folder access rights granted to this user².

NT permissions also have implications for mailbox security breaches. These can be difficult to track, and allow the user to access a mailbox at a level lower than Exchange permissions.

Clearly it is not the permissions themselves that can cause the problems, but rather the users exploiting them (wittingly or unwittingly) that can have dire consequences.

C2C's security management software Exchange Security Risk Auditor (ESRA) therefore addresses the three major levels of security breaches on mailboxes and folders, being:

- Exchange permission settings,
- NT permissions related to Exchange
- Send-on-Behalf-of permissions (delegates).

ESRA can be run by a Security Manager or Auditor so they can view permissions and check with the system description. The ability to change Exchange permissions is given to the Exchange Administrator. The authority to change NT permissions usually resides elsewhere and cannot be changed by ESRA.

ESRA is an MMC Snap-In, which is intuitive and provides results in an easy to understand format. Where changes are possible, the window allows the changes to be reviewed and accepted or rejected before proceeding.

Scheduled use of the application to review access to mailboxes of senior executives, HR department, and all those who handle sensitive items is recommended. Beyond this processes should be set-up to check all permissions on a semi-annual or quarterly basis.

However, please do not take this out of context. Exchange is a well structured and securely designed information management solution. But however well the product is designed, if mistakes are made in daily operational life then system accesses will be exposed. It is up to you, the administrator, to ensure these breaches are found and closed.

² It is a well known problem in Exchange 5.5 (and Exchange 2000) that when a user is deleted the mailbox is removed, but any rights the user had over the Exchange system are not removed

Check list: Recommendations for improving and checking permissions security

- Check the procedures in place for setting up mailboxes.
- Check the procedures in place for deleting mailboxes when an employee leaves your company.
- Ensure system and mailbox passwords are different.
- Create rules to change passwords every 28 days (exclude any NT service account passwords).
- Discuss the implications of inadvertent/malicious access with your security team.
- Establish a list of those people who handle the most sensitive information.
- Work with Security and give them the power to run security checks for you.
- Run security checks on ALL mailboxes on a 90/180-day period.
- Run security checks on VPs and Directors mailboxes every 30 days.
- Construct a permissions matrix to validate the security check findings.
- Make it corporate knowledge that permissions are monitored to help discourage the casual hacking attempt.
- Remove global unrestricted Public Folder creation rights.
- Establish a list of the most sensitive folders.
- Run security checks on the most sensitive folders every 30 days.
- Ensure User departments that have control of their own folders, understand the implications of permissions security.
- Validate that Anonymous and Default permissions are managed correctly.

6. Governmental and Regulatory security requirements

The final area covered by this paper encompasses rules and regulations laid down by governments, trade and regulatory bodies that impose rules and laws about use and retention of e-mail.

The requirements here include rules mandated by Securities Exchange Commission, local stock exchanges, federal and state legislature and regulatory bodies of many industries including petro-chemicals, financial services and aircraft/airlines.

In these environments the administrator needs advice and guidance by legal, business and human resources departments on

- what information must be retained
- for how long
- whether and when it should be destroyed.



Once the requirements are determined a flexible application such as C2C's Archive One can be used to enforce the rules. The advantage is that the user is unaware that the data is being moved and retained, yet they can still maintain seamless access to it.

The challenge to the corporate entity is to ensure that the relevant rules/laws are adhered to. The Exchange administrator has the means at his control to ensure compliance. For multi-national companies, an administrator may need to be aware of rules that apply not just in their home territory but also in their overseas territories.

Summary

Under the first three themes of this paper, there are a number of suppliers, non-specific to Exchange who can help reduce these security threats.

- Virus control
- Encryption
- Content control at the Gateway

However, the last three themes are purely internal to the Exchange/Outlook system and require a strategic approach to E-mail Risk Control.

- Content Control of the Information Store
- Mailbox and folder Permissions Management
- Regulatory Security Requirements

A number of Risk elements have been described in this paper, which will affect the e-mail-dependent company to differing degrees. It is highly likely, however that the Risk elements will occur simultaneously and these can have major implications on the efficiency of Exchange, particularly if they are not recognised and pro-actively controlled.

C2C's E-mail Risk Control strategy provides the elements that allow the company to control the outside influences on its e-mail system.

For more information visit www.c2c.com

June 2002 Copyright C2C Systems

Disclaimer of liability: While every precaution has been taken in the preparation of this document, C2C Systems assumes no responsibility for errors or emissions, or for damages resulting from the use of the information contained herein.

C2C Systems Ltd.
6 Richfield Place, Richfield Ave
Reading, Berks
UK RG1 8EQ
T. +44 118 951 1211 F. +44 118 951 1111
info@c2c.com

C2C Systems Inc.
1 Federal Street
Springfield Enterprise Center
Springfield, MA 01105 USA
T: 413-739-8575 F: 413-739-4980
info@c2c.com

