



Compliance Archives Integrity

Permissions Vulnerabilities with
Compliance



Introduction

This paper considers the use of email archives for compliance. It will also review how archives are trusted and look at what has to be done to ensure that integrity is maintained throughout the chain of events that take place within an email archive environment.



Why do email compliance archives exist?

Email compliance archives provide a reliable record of internal and/or external communications and provide potential evidence or other critical records, quickly and cost effectively.

Email archives exist to help organizations of all types, all sizes and in all countries to meet the growing demands of government, industry and internally generated regulations that have grown into being during the post-Enron era. Although the scope and value of some of the new legislation is questioned, due to its impact on international trade, company ownership and national tax revenues, it appears that compliance-driven archiving is here to stay.

Archive technologies are becoming more cost effective every year as they prove to provide many obvious benefits to organizations. These include:

- Proof and accountability in instances of specific legal actions around compliance laws
- Tools for good business governance and ethical audits of business practices

Data sources that can enable an organization to leverage information flows and information records in new ways. For example, analysis can provide businesses with specific competitive advantages based on the actual actions of their staff in their daily activities.

Chain of trust

A compliance archive has to be a 'trusted' source of information about the organization, especially because of its potential legal uses. Normally, this archive is created directly from the source or main transport mechanism of the information, such as the email or calendar system. The archive process makes copies of all information, indexes it (for rapid search and retrieval at any later time) and places onto some form of storage.

The process of maintaining an email archive can be considered a 'chain':

- A new user is given an email identity
- The user writes an email and sends it via the email system
- This email is transported by the email system and copied by an archiving solution. (It is also placed into an email system mailbox to be read)
- The archive solution places a copy of the email on a storage device to provide a permanent record

So long as the archive holds a trusted copy of the original, the communication or other data the information from the archive has validity for internal audit, to meet best practice and legislative guidelines and as legal evidence.

For the email Archive to be valid, and trusted, all parts of the chain have to be trusted. The first links in the chain depends on the security settings of the email system itself. Other links, including in some cases the compliance archive itself, depend on exact rights and permissions settings for the email system.

The trust of the final link, the storage media itself, is often addressed by the use of WORM drive. These are devices from which data can be read many times but which cannot be altered hence the Write Once Read Many acronym (WORM).

The trust of the mail system depends on standard access controls for mail servers and administrators. For example, Microsoft Exchange has a set of permissions to control exactly who is able to have access to which email storage



areas and mailboxes. These are regularly reconfigured to help administrators cope with day-to-day events such as people moving departments or leaving the company.

At least 40% of mailbox permissions will change every year in a typical organization with a staff turnover of 15% and a 25% role change rate – an arduous task for administrators.

How could the email system break the chain?

The mail system itself is certainly susceptible to being configured incorrectly. Microsoft Exchange in particular is a flexible but complex system that has evolved over time. The security models that underlie Microsoft Exchange are built on many contradictions – some features are driven by the need to maintain high usability, while others try to focus on email integrity. What has grown through this evolutionary process are access controls and permissions.

Microsoft Exchange permissions are a complex set of rules that provide varying degrees of access to mailboxes, mailbox folders and public folder data. Permissions can be assigned by central administrators and end users and are dependent upon existing or newly granted authority.

Organizations need to proactively review and understand what is possible within Microsoft Exchange to administer permissions and check the resulting permissions profile. Without the application of security permissions analysis products actions such as auditing, best practice enforcement and central review of the permissions are practically impossible to achieve for Microsoft Exchange servers.

Below is a list of some of the areas where security can be compromised:

Zombie users

For legacy and mixed Exchange environments (non-native mode) inheritable or zombie¹ permissions are commonplace. Zombie permissions are a major security flaw that can easily be exploited.

Un-restricted mailbox access

For legacy implementations of Microsoft Exchange (version 5.5) it was common practice to assign the equivalent of Microsoft Exchange Service Account rights to administrators. This assignment would then allow full unrestricted access to all of the mailboxes hosted on that Microsoft Exchange server. End user checks do not highlight this security compromise of their mailboxes.

Inherited mailbox access

There are many software applications that perform legitimate activities within Microsoft Exchange, but are required to be granted Microsoft Exchange Store access permissions. Once these permissions are granted by using the associated account it is possible to gain access to other mailboxes then hosted within that Store. For example, a user who is responsible for managing Brick level backups carries out day to day tasks whilst logged in as the service account for the Brick level backup software. By using this service account, the operator could by using OWA or native Outlook gain unrestricted access to all mailboxes on the Microsoft Exchange server(s).

¹ Where the primary owner of a set of permissions no longer exists. The simple act of deleting a user from NT/AD can leave behind zombie attributes.



Public folder ownership permissions

Anyone with ownership permissions assigned to public folders can determine subsequent permissions granted to that folder. Indeed owner permissions enable the ability to modify and remove permissions that were granted to that folder (including any other users with Owner permission). A creator of a public folder is automatically granted owner permission status, and yet very few organizations provide any training to the appropriate use of Microsoft Exchange permissions.

User housekeeping of permissions....or lack of

All users of Outlook have the ability to set permission access to their mailbox folders. This process is quite cumbersome and requires a minimum of 7 mouse clicks per folder. Typically, calendars are granted extended access permissions but often additional folders have permission updates applied. Once more end user training is often not provided to ensure appropriate permission provision and worse, users rarely check the permissions that have been applied to ensure accuracy (e.g. change of user roles, people who leave the organization, access no longer appropriate etc.). End users are seldom trained on the implications of these permission settings.

Each of these security weaknesses in the email system may have an impact into an email archive store. A simple flaw could result in a major embarrassment to the organization or in a worst case scenario, could open it up to litigation. Despite the costly consequences of errors in this area there is no consolidated view within Microsoft Exchange that can provide authorized officers with a complete understanding of the security risks associated with their Microsoft Exchange servers. Only through the use of products like Archive One Access Security Manager is it possible to highlight and understand the risks and, where appropriate, take direct action to remove the security pitfalls.

Archive One Access Security Manager enables administrators and audit officers to centrally report and analyze the Microsoft Exchange security profile, retain historical information and, where appropriate, apply changes to prevent inappropriate data access.

Specific issues about 'Send as' permissions

Microsoft Exchange has a very specific permission called 'Send as'. This is very powerful and has deep implications in the context of message integrity and chains of trust.

It is particularly dangerous if you consider the legal implications of someone pretending to be someone else or obtaining information on a pretext. There is the potential for the organization to be sued for email pretexting since the archive will state the false 'Send as' usage as if it were correct.

Pretexting

A pretext is a false motive put forth to hide a real one. "Pretexting", pretending you are someone else to obtain information, is at the centre of the boardroom scandal at the Silicon Valley computer company, Hewlett-Packard. The company has admitted that it hired a private investigator who obtained the phone records of the HP board by using a contractor. The contractor also used pretexting methods to obtain the phone records and other confidential data of targeted journalist.



Email pretexting

This specific form of pretexting involves masquerading as another email user in order to obtain financial, confidential or other information. There are a number of ways to do this – many of which are used by spammers and can be caught in anti-spam traps. They include setting up false spam addresses which don't match the actual email sender's domain. Buying a web identity that is very similar, in spelling, to the organization that you want to appear to belong to and sending a message from there or gaining access to a mail system 'send as' feature in order to totally impersonate that real email user.

In 1999, Congress passed the Gramm-Leach-Bliley Act, outlawing the use of pretexting to obtain financial data from customers or institutions. The Federal Trade Commission has investigated businesses that advertise pretexting services. However the law's boundaries are fuzzy. Even though its language is limited to financial data, lawyers have disagreed on whether it could be used to prosecute pretexters who have obtained non-financial data. Also, some private investigators maintain that no laws have been broken if the pretexted data is not used illegally. In the HP case, the California attorney general said on one day that he was unsure if laws had been broken. On the next day, he said he was certain they had.

As for email pretexting: the same yardstick applies. If it is used to obtain financial information it is going to be more likely to lead to a prosecution than if there is no financial data involved.

A compliance archive solution still leaves an organization open to pretexting, indeed it can even re-enforce the credibility of the fraudster in the future if a seemingly legitimate pretext email can be retrieved from the archive. However products like Archive One Access Security Manager which focus on permissions such as the 'Send as' permission make it far more difficult for fraudsters to take advantage of other peoples email identities.

How can it be prevented?

In the case of the Microsoft Exchange 'Send as' rights, Archive One Access Security Manager is able to carry out a complete audit of the permission. Allowing the system administrator or security office to make sure that users are not getting themselves into a position from which they could do email pretexting, and so, perhaps tarnish the reputation of the individual whose email identity they could borrow, or the reputation of the whole organization.

What does this all mean for compliance?

The implications of installing an email archive are far reaching. Questions arise about the exact controls that provide security and integrity for the email system itself. It is advisable to monitor these controls carefully in order to get the full value out of your archive solution.

Current events further highlight the potential ramifications of placing false or misleading information into an archive system.

For an email archive system to run smoothly and with validity, administrators and security officers must make sure that the email system itself is checked constantly to ensure that powerful permissions settings are maintained correctly and are up to date.



About C2C

C2C offers automated data archiving and management for email, files and SharePoint content. With over 15 years experience delivering solutions for capacity, e-policy enforcement, compliance and e-discovery, C2C optimizes performance, reduces storage management costs and minimizes risks associated with email - helping you to control your data before it controls you.

The Company, a Microsoft Gold Certified Partner, supports organizations in the government, manufacturing, finance, education and healthcare industries, including Fortune 1000 companies. Established in 1992, C2C is a privately held company with offices in Springfield and Westborough, Mass. and Reading in the UK.

Disclaimer of Liability

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

Trademarks

All trademarks, trade names, service marks and logos referenced herein belong to their respective companies.

Where can I find out more?

For more information and free evaluation software, visit www.c2c.com or email info@c2c.com.

C2C Systems, Inc.
1 Federal Street
Bldg. 101-R
Springfield
MA 01105-1199
USA

T: +1 413-739-8575
F: +1 413-739-4980

C2C Systems Ltd
6 Richfield Place, Richfield Ave
Reading
Berkshire
RG1 8EQ
UK

T: +44 (0) 118 951 1211
F: +44 (0) 118 951 1111