

Microsoft® Exchange Server 2010

A simplified approach to information protection and compliance



Contents

Foreword	01
Information Protection and Compliance (IPC)	01
Archiving, retention and discovery	01
Information protection and control	02
Information Rights Management (IRM)	02
Mailtips	02
Moderation	03
Enhanced transport rules	03
IPC is the way forward	03

In recent times, a succession of major events has heightened the focus on organisational data protection and information compliance. Accounting scandals, the rise of shareholder activism, greater accountability from boards of directors, information leakage and data growth have all contributed to the need for more stringent compliance in organisations.

In response to the myriad of regulatory and legislative requirements around organisational data and information, organisations around the world have invested heavily in compliance. Yet the challenge grows daily as more electronic data is created and trends such as unified communications and virtualisation set about transforming the technology landscape forever.

Fortunately, technology has risen to the occasion. Microsoft® Exchange Server 2010, the world's most pervasive e-mail platform, is a case in point. This release brings with it a host of new and sophisticated tools designed to make the control and management of e-mail data more palatable.

Most data leakages require little technical sophistication and typically **involved exploitation of business rules or organisational policies** and in 87% of cases simple, **legitimate user commands were used**.

Information Protection and Compliance (IPC)

Recent research into information protection and compliance reveals some sobering statistics. Most data leakages require little technical sophistication and typically involved exploitation of business rules or organisational policies and in 87% of cases simple, legitimate user commands were used¹.

Today, it's not uncommon for lawsuits to involve demands for the discovery of important information contained in e-mail and acts pertaining to access to information heap additional accountability on organisations to ensure that they can quickly locate and access messages. Legislation can impose hefty fines and even jail terms for non-compliance, making it critical to have a robust IPC strategy.

An effective IPC strategy needs to provide for the monitoring of all messages flowing in and out of the organisation in terms of both content and recipients; facilitate retention, archiving and discovery; and control and protect all data according to granular policies and 'soft to hard' controls.

Exchange Server 2010 has built-in IPC functionality and tools designed to help organisations comply with legislative demands while maintaining the flexibility required to meet the needs of the business.

Archiving, retention and discovery

A 2009 study found that an average of 247 billion e-mail messages are sent everyday². In most organisations, the sheer volume of e-mail creates a major burden on storage and backup resources. Historically, IT administrators have placed quotas on users to maintain a manageable level of e-mail storage. Archiving has traditionally been done to .pst files, which heightens the demand for network storage, increases the risk of data corruption and limits search efficiency.

Exchange Server 2010 breaks this cycle by allowing for the use of low cost Serial Advanced Technology Attachment drives for storage and support of large gigabyte-sized mailboxes. Its archiving capabilities eliminate the need for .pst files by centralising all archived e-mail, making it more manageable. Let's explore these features in more detail:

Personal archive

Exchange Server 2010 provides a personal archive for every user, through what can be described as a secondary mailbox that operates alongside the main mailbox. This feature separates the .pst file from the desktop but retains the functionality of Microsoft® Outlook®, allowing access to e-mail across the web, the option to set quotas if required, access to full views in the archive as well as in the main mailbox as well as more sophisticated search functions.

Message retention policies

Exchange Server 2010 offers two retention policies. The first is a 'move' policy that automatically relocates messages from the mailbox to the archive on a user-selectable 6-month, 1, 2 or 5-year or 'never' basis. The second is a 'delete' policy which deletes or moves messages to an archive according to criteria such as mailbox quota, message category (on a per item basis) or expiration date.

1. Echowoxx, E-mail Data Loss- Case Study of Recent E-mail Leaks

Legal hold

In the event of mailbox data being required for discovery in a legal matter, Exchange Server 2010's 'legal hold' prevents users from changing, tampering with or deleting information contained in the message.

Multi-mailbox search

The administration rules in Exchange Server 2010 have been extended to include role-based access control. For example, a human resources or compliance officer can be assigned a search role without the need for administrator privileges. In addition, an e-discovery mailbox allows for automatic collection of the results of all searches, further lessening the administrative burden on the organisation.

Information Protection and Control (IPC)

Information is the lifeblood of any organisation and leaks can have serious legal, regulatory and financial impact, resulting in lawsuits or fines in the event of non-compliance. In addition, the damage to corporate reputation, customer loyalty and loss of competitive advantage can cripple the organisation.

Enhanced control and protection functionality introduced in Exchange Server 2010 has 'soft' and 'hard' controls. The concept of 'soft' and 'hard' controls affords organisation greater flexibility when applying rules to message types. For example, soft controls include a simple alert that allows a message to be delivered but adds a warning, classification, message modification or disclaimer. A middle-weight control would ideally allow delivery but prevent forwarding. Hard controls would avert delivery until the message has been moderated, redirected or, if appropriate, the message would not be delivered at all.

Exchange Server 2010 takes a proactive role in protecting information through information rights management, MailTips, moderation and enhanced transport rules.

Information Rights Management (IRM)

IRM forms a core part of the Microsoft® Windows® platform information protection technology and enables administrators to safeguard information from unauthorised viewing, editing, copying, printing or forwarding of messages; limiting access to files and creating an audit trail that tracks the usage of protected files.

Armed with these enhanced capabilities, organisations are now able to protect data wherever it may go, better enforce organisational policies and enable authors to define how recipients can use the information. Exchange Server 2010 takes a content-based approach to information protection by analysing not only key words within the message but also taking into consideration its destination and destination. Other notable features include the following:

- Rights management can be applied to unified messaging environments enabling administrators to mark incoming voicemail as private or prevent forwarding and copying
- Rights management services are integrated into Microsoft® Outlook® Web Access to ensure that information is protected no matter where or how users access their e-mail
- Rights management services can be extended outside the organisation to key stakeholders. With Exchange Server 2010 your customers and partners can federate using Microsoft® Federation Gateway which provides a single access point opposed to individual trusts
- Senders are able to control third party access to data



MailTips

MailTips provide informative alerts to users as they compose messages. Exchange Server 2010 analyses the message, its content, attachments, size and recipients in search of potential issues and notifies the user thereof before the message is sent. MailTips will also inform the user of the potential implications of sending the message. While this feature does not enforce specific policies, it does provide a first line of defence.



Moderation

The moderated transport features in Exchange Server 2010 enable administrators to enforce moderation approval for messages sent to specific recipients. Moderated transport comprises the following features:

Categoriser

Initiates the approval process, re-routing the message to an Arbitration Mailbox if a moderated recipient is detected.

Store driver

Processes the message marked for moderation by the Categoriser. The original message is stored in the Arbitration Mailbox and an approval request is sent to the moderators. Once the moderator's response is received, the message is marked.

Information assistant

Monitors the Arbitration Mailbox, submitting any approved messages to the submission queue for delivery to the recipient or deleting any rejected messages. It also sends rejection notifications to the sender and manages the Arbitration Mailbox.

Arbitration mailbox

Stores messages due for moderation.

Enhanced transport rules

Introduced in Microsoft® Exchange Server 2007, Transport Rules have been further enhanced in Exchange Server 2010. Rather than merely scanning the file name of attachments, Exchange Server 2010 can scrutinise their contents too. It also allows administrators to create rules based on user aspects such as department, groups, manager, city, by means of example. These rules may be extended beyond the walls of the enterprise to users from business partners or customer organisations. Furthermore, disclaimers are now more flexible, allowing administrators to add properties to the disclaimer based on data pertaining to the user.

Now, your administrators are able to automatically define client-side rules in Outlook® based on predicates such as the sender's department and the recipient's identity or scope. These rules are automatically retrieved from Exchange using Autodiscover and Exchange Web Services.

Let's take a typical scenario to illustrate this capability: A user creates a new message and adds a distribution list to the 'To:' line. Should Outlook® detect that the distribution list is sensitive, it will automatically flag the message as confidential and apply the appropriate user rights.

IPC is the way forward

Thanks to the advanced IPC capabilities innate in Exchange Server 2010, organisations are better positioned to ensure compliance while maintaining complete control of the flow of messages into and out of the enterprise. Furthermore, by leveraging the product's flexible and automated controls, organisations can alleviate the burden on their administrators and compliance officers without compromising their ability to manage, search, archive and – most importantly – protect information.

Organisations around the globe that face an ongoing and uphill battle to protect and secure their business-critical data are quickly waking up to the role Exchange Server 2010 can play in making this a more proactive and less time – consuming endeavour. Shouldn't you be one of them?

MIDDLE EAST & AFRICA

ALGERIA • ANGOLA
BOTSWANA • CONGO
DEMOCRATIC REPUBLIC OF THE CONGO
GABON • GHANA • KENYA
MADAGASCAR • MALAWI
MAURITIUS • MOROCCO • NAMIBIA
NIGERIA • SAUDI ARABIA • SOUTH
AFRICA • TANZANIA • UGANDA
UNITED ARAB EMIRATES • ZAMBIA

ASIA

CHINA • HONG KONG
INDIA • INDONESIA • JAPAN
KOREA • MALAYSIA
NEW ZEALAND • PHILIPPINES
SINGAPORE • TAIWAN
THAILAND • VIETNAM

AUSTRALIA

AUSTRALIAN CAPITAL TERRITORY
NEW SOUTH WALES • QUEENSLAND
SOUTH AUSTRALIA • VICTORIA
WESTERN AUSTRALIA

EUROPE

BELGIUM • CZECH REPUBLIC
FRANCE • GERMANY
ITALY • LUXEMBOURG
NETHERLANDS • SPAIN
SWITZERLAND • UNITED KINGDOM

AMERICAS

BRAZIL • CANADA • CHILE
MEXICO • UNITED STATES