

## Email Archiving

### Introduction

In the last decade email has become one of the most important medium for communicating within and outside an organisation. Therefore mailboxes are one of the major sources of important company information and documentation – ranging from contract negotiations and agreements through to cancellation notifications and invoice information. Often those email communications – sent or received - are the only records that a company has about certain transactions.

For example would you be able to find an email on a customer's payment details, to which an ex employee agreed to on your behalf from three years ago? You will need to if this particular customer refuses to pay and you need to prove your case in court.

Considering the importance of company data stored in email boxes, this paper will firstly concentrate on the reasons why your company should employ an email archiving solution. Secondly, it will look at the advantages and disadvantages of in-house and hosted archiving solutions and the steps needed to successfully implement an archiving solution in your company.

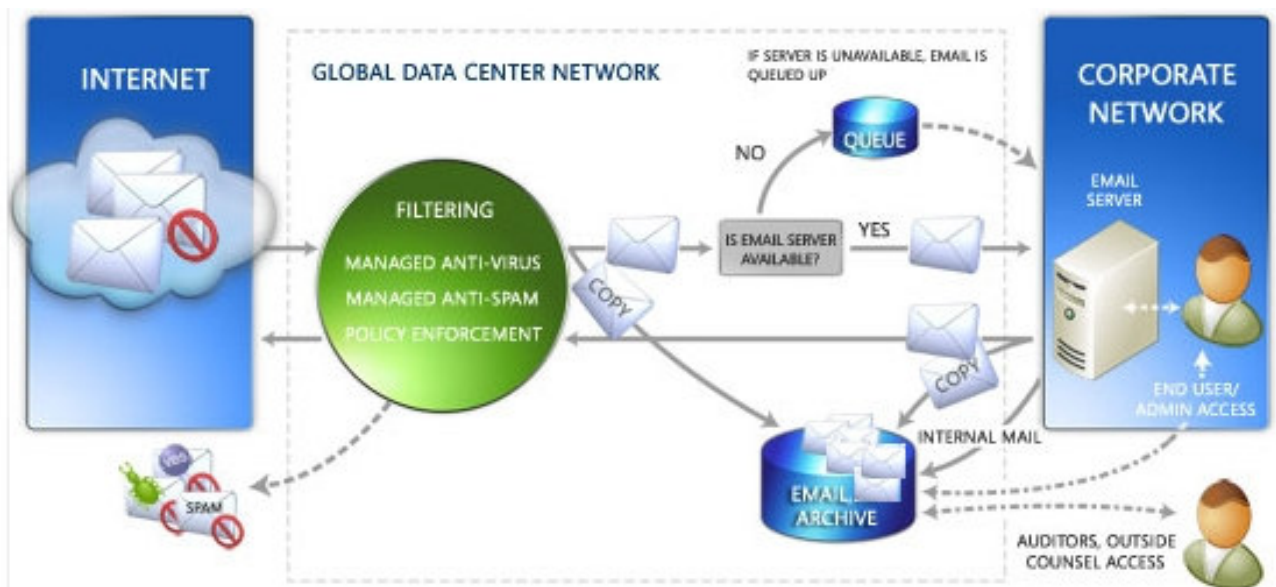
### What is Archiving – is it just backing up the data?

No! Archiving can be defined as:-

“a systematic approach to saving and protecting the data contained in e-mail messages so it can be accessed quickly at a later date” (SearchStorage.com, 2008).

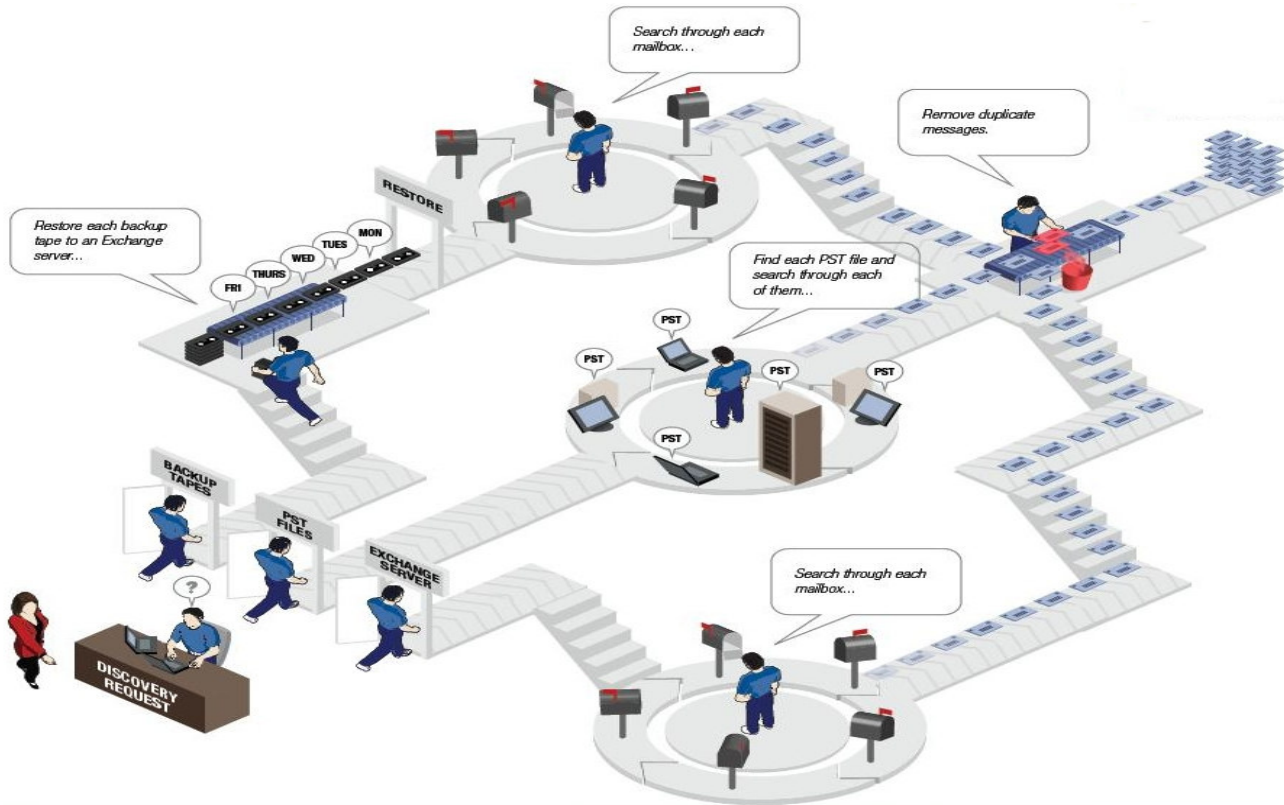
Thus professional archiving solutions split off and copy each message – both sent and received - before it reaches the email server used. It is therefore ensured that emails cannot be changed, deleted or tampered with by any staff member and regulatory compliance is therefore adhered to. Emails can even be accessed if the original has been deleted in the user's mailbox. Archived emails can usually be accessed and managed via a web-interface or within the email client. Figure 1 shows how email archiving systems deal with incoming and outgoing emails and the red circle indicates that archived emails can be directly accessed.

Figure 1: How email archiving works (Adapted from Microsoft, 2009)



On the other hand, back-ups represent a point-in-time snapshot of a particular mailbox and are not an effective way to archive due to ongoing deletion of messages by the user. Companies relying on only back-ups might risk losing large amounts of money for recovery-from-back-up solutions in litigation processes. Figure 2 indicates which steps would be involved if specific information needs to be extracted from a company's email and back-up system.

Figure 2: Message recovery using a company's back-ups (Adapted from Proofpoint, 2008)



### So, in summary, some of the reasons for archiving are:-

According to GFI (2008) an email archiving solution will help:

- your IT department to deal more easily with storage issues,
- your legal department to set up an appropriate discovery response strategy in a legal case,
- your compliance team to be ensured that all emails are preserved in a safe place in case they are needed at a later stage, and
- your employees to be more productive as they can access their email from anywhere in the world – even if it is a year old and has been deleted from their own mailbox.

The following reasons are therefore the main reasons that justify the costs of employing a professional email archiving solution:

#### Storage issues

With email storage growing at an average rate of 35% annually, IT departments constantly struggle with storing large amounts of messaging data. If server quotas cannot be increased, emails must be stored on local machines or a network share. This usually creates bigger problems as not all employees might store their data in the same way and it will become a nightmare if an IT specialist needs to search for information within those files. In addition, storage on messaging servers is usually more expensive than archival storage; thus migrating data from messaging servers to archival storage usually results in considerable cost savings and archived data is also easily accessible to everyone.

## Legal Compliance

In the UK the two main laws that are regulating archiving in the UK are the Data Protection Act 1998 (DPA) and the Freedom of Information Act 2006 (FOIA). These laws affect all private and public sector organisations in the UK that process personal data, are involved in court proceeding or are involved in Employment Tribunal claims (GFI, 2008).

In addition, UK subsidiaries of US companies as well as US companies themselves also need to conform to various US laws depending on the industry they are operating in. Generally all US companies and subsidiaries of US companies however have to comply with the Sarbanes-Oxley Act 2002 (SOX) and the Federal Rules of Civil Procedure (FRCP). Although these laws only apply to US companies and their subsidiaries all UK companies working with US companies are advised to implement an archiving solution that conforms to both UK and US law.

Table 1 gives a brief outline of key archiving laws in the UK and the US and the key implications for organisations regarding data that needs to be retrievable.

*Table 1: Key archiving laws UK and US*

<b>Key Regulatory Bodies/Statutes</b>	<b>Key contents/requirements</b>
<b>Data Protection Act 1998</b>	<ul style="list-style-type: none"> <li>• individuals have a right to obtain a copy of personal data held about them; companies have 40 calendar days to respond to such a request and cannot charge more than £10 per request</li> <li>• companies therefore need to be able to retrieve emails that include the individual quickly and at a low cost</li> <li>• personal data also needs to be stored in a way to prevent unauthorised or unlawful processing of personal data, and accidental loss or destruction</li> </ul>
<b>Freedom of Information Act 2000</b>	<ul style="list-style-type: none"> <li>• the public has the right of access to recorded information held by public authorities; email falls within the definition of "recorded information"</li> <li>• authorities have 20 working days to reply to a request</li> <li>• NB the FOIA is retrospective, thus emails generated before it came into force on 01/01/05 also need to be retrievable</li> </ul>
<b>Sarbanes-Oxley Act</b>	<ul style="list-style-type: none"> <li>• primarily regulates financial reporting of organisations; companies must have adequate internal controls over financial information and assets</li> <li>• organisations need to maintain, store, and secure data - including electronic messages - to be able to retrieve data when necessary and to prevent or detect any unauthorised transactions</li> </ul>
<b>Federal Rules of Civil Procedure</b>	<ul style="list-style-type: none"> <li>• amendments in 2006 now list emails and other electronic assets as business records that can be used as evidence in a legal case</li> <li>• organisations need to be able to produce electronic data in a timely and complete manner when necessary, e.g. during legal discovery proceedings</li> </ul>

In addition to these key laws there are compliance regulations that concern specific industries. The following list shows a few of the many additional industry specific regulations:

UK	US
<ul style="list-style-type: none"> <li>• Financial Services Authority (FSA)</li> <li>• Companies Act</li> <li>• Company Lay Reform Bill – Electronic Communications</li> <li>• Combined Code on Corporate Governance 2003</li> <li>• Human Rights Act</li> <li>• Anti-Terrorism, Crime and Security Act 2001</li> </ul>	<ul style="list-style-type: none"> <li>• Securities and Exchange Commission (SEC)</li> <li>• National Association of Securities Dealers (NASD)</li> <li>• Financial Industry Regulatory Authority (FINRA)</li> <li>• Health Insurance Portability and Accountability Act (HIPAA)</li> <li>• Medicare Conditions of Participation</li> <li>• General Records Schedules from the National Archives and Records Administration</li> <li>• Auto Industry Action Group (QS-9000)</li> </ul>

### *The Risks of Non-compliance*

Failure to comply with electronic archiving and recovery rules can be damaging to an organisation as they can result in fines, sanctions, executive liability, brand damage, etc. For instance according to FOIA 2000 “it is a criminal offence to alter, deface, erase, destroy or conceal any record, including and email, with the intention of preventing disclosure” (Desai, 2009). In accordance with that the Sarbanes-Oxley Act also states that “anyone who alters, falsifies, destroys or otherwise tampers with a document or record can be imprisoned for up to 10 years and/or fined” (Osterman Research, 2005). Courts are taking cases in which companies did not comply to archiving laws very seriously and research conducted by Osterman Research (2005) and Chudnow (2003) mentioned the following cases in which companies were punished by the court:

- Five Wall Street brokerage houses—Deutsche Bank, Goldman Sachs, Morgan Stanley, Salomon Smith Barney and U.S. Bancorp—were fined a total of more than \$8 million by the SEC in December 2002 because these firms did not retain certain emails for SEC-mandated retention periods and for other infractions of SEC rules. The SEC investigation that culminated in these fines arose as part of a larger investigation into potential conflicts of interest between the research and investment banking operations at various brokerage firms.
- In *Proctor & Gamble Company v. Haugen* (an independent distributor of Amway products), Proctor & Gamble was fined for destroying email-based records. Proctor & Gamble did not preserve or search for emails relevant to this case that were written by five individuals and was fined \$10,000 for their failure to do so.
- In *Applied Telematics, Inc. v. Sprint*, Sprint was charged with destroying evidence because it continued to recycle its backup tapes even after the legal proceeding brought by Applied Telematics had commenced. The data that Applied Telematics had asked Sprint to produce included routing plans that were housed in Sprint's internal databases. Although there was no allegation that Sprint had intentionally destroyed this data, the Court found that Sprint should have modified its normal backup procedures in order to preserve the data after Applied Telematics had requested it.
- In *Anti-Monopoly, Inc. v. Hasbro, Inc.*, the Court ruled that a defendant that is required to produce documents during the discovery phase of a legal action can also be compelled to bear the costs of designing a mechanism for extracting the information from its computer-based files.

- Related to the above case is *Zubulake v. UBS Warburg*, in which the judge in the case has ruled that a new standard should be established for evaluating whether the plaintiff or the defendant bears the cost of electronic discovery. The judge in this case has taken a decidedly pro-plaintiff approach, meaning that organizations may be more likely to be charged for the costs of electronic discovery where the plaintiff can demonstrate that this discovery would yield information of sufficient importance to a case.
- Prudential Life Insurance was involved in a class action suit and the court had ordered that it destroy no records during the proceedings. Unfortunately no one told the IT department, who happily went on deleting electronic records on its own retention schedule. A judge issued a \$1 million penalty against Prudential for destroying data that supported its opponent's case. Although Prudential had not deliberately destroyed relevant data it still lost huge sums of money over its inability to enforce a reasonable and consistent retention policy.

### Access to old/deleted emails

Although an email archiving solution is especially needed when a court has requested certain information to support a legal case, an archiving solution will also pay off when staff needs to find email communications with customers that are unlikely to end up in court but would still embarrass the company in front of the customer.

GFI (2008) mentioned an example of Quantum Marine Engineering when one of their "customers had asked in an email to them about the suitability of a component they were using to hook up a piece of equipment. Quantum's sales force and technicians both were adamant about having replied, saying that what they were proposing wasn't suitable; but no one could come up with the email". Having an archiving solution in place, Quantum's administrator found the email using a keyword search as well as the whole string and conversation within five minutes.

### **Understood. But what is better for us – an in-house or a hosted email archiving solution?**

Having discussed the reasons for deploying an email archiving solution it is worth reviewing the different options. The following section will therefore take a closer look at the pros and cons of in-house vs. hosted email archiving.

#### In-house email archiving

If your company decides to set up an in-house solution your company will have to buy all hardware and software required to run the archiving solution efficiently. Everything will be installed in the company's data centre and it will be managed by your IT specialists.

Some advantages of in-house solutions include:

- The control that your company has over the archiving system is higher than with hosted solutions.
- It ensures that all confidential data on your company is kept and managed in-house.
- The degree of possible customisation is usually higher than with hosted solutions. Your company can make decisions on the type of storage, employee access and/or security, etc.

Some disadvantages of in-house solutions include:

- High upfront costs for hardware and software that are required to set-up the service.
- Set-up usually takes longer and requires an IT consultant to ensure that regulatory or litigation requirements are met. In order to keep the system up and running new staff usually has to be hired as well to keep the standards up to date.
- Upgrades of software or hardware can be expensive. In order to implement the updates successfully your company's IT department might require large amounts of working hours in addition to the normal work load.

### Hosted email archiving

All emails of your company – sent or received – are sent to a service provider who accepts, indexes and stores all emails for later use. Thus all emails are stored using the service provider's hardware and software. The service provider usually charges a monthly or annual fee on a per user base or by the amount of storage used.

Some advantages of hosted solutions include:

- Initial costs are kept to a minimum as your company does not have to buy any equipment. Hosted solutions also have the advantage that you can simply cancel the services without having to worry about servers or software sitting unused on your premises.
- The set-up of the system can be done relatively fast and the hosting provider will do all the work to get the archiving solution up and running. Therefore your company's internal human resources are not used or only to a very small extent. The same counts for monitoring and managing the archiving solution.
- The scalability is very high since hosting companies run a large number of servers that can be dedicated to archiving solutions.
- You will always work with the latest versions of hardware and software since hosting companies strive to offer the latest products to their clients.
- If you decide that your email service itself is to be outsourced then hosting provides a total solution – mail servers and archiving – in one package.
- The data is not stored in your facilities and less vulnerable to alteration or deletion. Hosters also tend to have a high quality environment to store data because they use dedicated server centres well connected to the internet.

Some disadvantages of hosted solutions include:

- Some companies might feel uncomfortable with handing over sensitive data to an outside provider, thus having limited control over their data as it is stored outside the company's own data centres.
- There is sometimes the perception that outsourced solutions are slower in responding to requests.

### **Decided. What are the next steps and is it easy?**

It does not matter whether you decide to go ahead with an in-house solution or a hosted solution – in any case your company should develop an email retention policy with the help of experts to make the integration process of an archiving solution as easy as possible.

If you decide to employ an in-house solution you should probably consult an IT expert who will be able to specify your requirements and to help you set up the solution. An IT consultant will be able to recommend the hardware and software you require to run an effective email archiving solution. Nevertheless, well known archiving solutions – some were mentioned in an Osterman (2008) research paper – include: GFI, Sunbelt Exchange Archiver, Autonomy ZANTAS EAS, Barracuda Message Archiver, and EMC EmailXtender.

If you decide however to go for a hosted solution you will most likely search the internet or ask business partners and friends for possible hosting companies who also offer archiving solutions to their clients. Your company will simply subscribe to the services on a monthly or annual basis and charges usually depend either on the number of users or the amount of storage you consume. The hoster's archiving solution will be instantly available to you as it simply hooks into your company's email system. With some hosting providers you will also need to outsource your email system; many hosting companies offer advanced email solutions such as MS Exchange. Nevertheless considering that you are already outsourcing your archiving solution it is worth thinking about the option to outsource your email system altogether. You will then benefit from the advantages mentioned above since these also count for outsourced email solutions. Hosting companies that are offering archiving solutions include: ASP-one, cob-web, Intermedia, Simply Mail Solutions, and USA.net.

### **Conclusion**

Having an effective archiving solution can have various important benefits for your companies independent of its size. A correctly deployed solution for instance, saves your IT department time and resources which can be re-deployed to more strategic tasks, supports your company in legal compliance issues and ensures an effective knowledge management. At the end of the day it is your own decision whether you want to deploy your own server for your archiving solution or whether you think it worth outsourcing your archiving solution together with your email solution. Outsourced solutions however tend to lower your total ownership costs and provide you with guaranteed service levels.

*References:*

Centerbeam (2009) "Email Compliance Services" [online] Available from:

<http://www.centerbeam.com/index.php?page=hosted-compliance-suite-2#archive> (Accessed: 21/04/09)

Desai, J (2009) "Email Archiving: UK law, regulations and implications for business" [online] Available from:

<http://www.message-labs.co.uk/registered/Download.aspx?id=24248&verify=Y3YAL%2f5hiUSnGkYrX9Aj2ZjKNzOaOG%2fPks%2bTcj6TPo%3d&&ml=53O%2bTyvN2rR7Y3fQ4%2feUwk1UwatLv779ey4PyXhBXI59IKBf4MYmePieWe%2f1pLoAAzagQpxtRMT7GkqHXF3YIA%3d%3d>

(Accessed: 17/03/09)

GFI (2008) "The Business Case For Email Archiving" [online] Available from: [http://](http://whitepapers.securityfocus.com/whitepaper3366/)

[whitepapers.securityfocus.com/whitepaper3366/](http://whitepapers.securityfocus.com/whitepaper3366/) (Accessed:26/03/09)

Microsoft Technet (2009) "Exchange Server Tech Centre" [online] Available from: [http://](http://technet.microsoft.com/en-us/library/cc164320.aspx)

[technet.microsoft.com/en-us/library/cc164320.aspx](http://technet.microsoft.com/en-us/library/cc164320.aspx) (Accessed: 21/04/09)

Osterman Research (2005) "The Impact of Regulations on Email Archiving Requirements" [online]

Available from: [http://www.techlineinc.com/librarypdf/alchemy/3497al\\_ostermanwhitepaper\\_0405.pdf](http://www.techlineinc.com/librarypdf/alchemy/3497al_ostermanwhitepaper_0405.pdf)

(Accessed: 24/03/09)

Osterman Research (2008) "Customer Satisfaction with Email Archiving Systems" [online] Available

from: <http://i.zdnet.com/whitepapers/>

[Sunbelt Software SEA Customer Satisfaction With Email Archiving Systems.pdf](http://i.zdnet.com/whitepapers/Sunbelt_Software_SEA_Customer_Satisfaction_With_Email_Archiving_Systems.pdf) (Accessed:

16/03/09)

Proofpoint (2008) "Email Archiving: A Proactive Approach to e-Discovery" [online] Available from: [http://](http://viewer.bitpipe.com/viewer/viewDocument.do?accessId=9414798)

[viewer.bitpipe.com/viewer/viewDocument.do?accessId=9414798](http://viewer.bitpipe.com/viewer/viewDocument.do?accessId=9414798) (Accessed: 24/03/09)

SearchStorage.com (2008) "SearchStorage.com Definitions: e-mail archiving" [online] Available from:

[http://searchstorage.techtarget.com/sDefinition/0,,sid5\\_qci1123554,00.html](http://searchstorage.techtarget.com/sDefinition/0,,sid5_qci1123554,00.html) (Accessed: 22/03/09)

Taylor Chudnow, C (2003) "Business dilemma: email retention policy; new SEC regulations to address storing and restoring" [online] Available from: [http://findarticles.com/p/articles/mi\\_m0BRZ/is\\_1\\_23/](http://findarticles.com/p/articles/mi_m0BRZ/is_1_23/ai_99811009/)

[ai\\_99811009/](http://findarticles.com/p/articles/mi_m0BRZ/is_1_23/ai_99811009/) (Accessed: 26/03/09)