Barracuda

A Barracuda Company

How PST Discovery and Deletion Helps Public Entities

Mitigate Risk, Remain Compliant and Reduce Operational Costs

White Paper

Overview

Email drives the business of public entities much the same way it does within the private sector. Employees communicate via internal email, often in preference to the telephone, and enquiries and support concerns are increasingly handled via email.

This creates a complicated balancing act for public entities, as they are bound by a variety of overlapping laws, acts, and regulations which both force them to preserve and classify email and to produce them to outside parties, virtually on demand.

Systems which simply backup email stores cannot handle the tasks of demonstrating that proper preservation and classification policies were followed, that laws and regulations were not violated, and that the entity can provide information to the public when requested. This is why the majority of these organisations have already deployed information management and email archiving systems. However, the issue with legacy PST files is something frequently overlooked and the hidden threat that PSTs present needs to be considered either as part of a comprehensive email management system or as a standalone PST location, migration and elimination project.

The Dangers of PST Files

There are two major dangers to PST files. The more serious of these is corporate risk and governance.

The other problem is in IT operations, where PST files take up a lot of time as they corrupt easily, are often misplaced and rarely (if ever) backed up.

PST Files and Corporate Risk

Since mail can be found in places other than a user's mailbox, PST files (also known as personal archives) severely jeopardise best practice and compliance presenting an enormous challenge in an environment where laws and regulations regarding preservation, classification and protection are stricter, not only to the key security classification principles but since the UK classification system operates within the framework of domestic law, they are also subject to the following:

Official Secrets Act 1989

Damage assessment is a critical element of the OSA, in which most of the offences require there to have been a damaging disclosure of information relating to security or intelligence, defence, international relations, crime or special investigation powers, or of confidential information received from a foreign State or an international organisation. With respect to each type of information, the OSA describes the type of damage which has, or would be likely, to flow from an unauthorised disclosure. The OSA also specifies who is capable of committing offences under it. Different offences apply to: members of the security and intelligence services; persons notified under section 1 of the OSA; Crown servants; government contractors; and any person.

Data Protection Act 1998

The handling of personal data must be in compliance with the DPA. The DPA, however, contains a number of exemptions to some or all of the data protection principles and to other provisions of the DPA such as the right of access to personal data. For example, section 28 provides an exemption from the data protection principles and a number of other provisions of the DPA if it is required for the purpose of national security. But note that, although the exemption is widely drawn, it is only available to the extent that it is required for the purpose of national security. Thus departments and agencies will still be required to assess whether it is possible to address national security concerns and comply with the DPA. Other exemptions,

such as section 29 (crime and taxation) are more narrowly drawn. Whilst the presence or absence of a classification marking is not in itself a deciding factor as to whether an exemption is engaged, it may be a helpful indicator that one applies. Departments and agencies should also have regard to the DPA, including any relevant exemptions, when sharing personal data with other departments and agencies or pursuant to international agreements.

Freedom of Information Act 2000

Classification markings can assist in assessing whether exemptions to the Freedom of Information Act 2000 (FOIA) may apply. However, it must be noted that each FOI request must be considered on its own merits and the classification in itself is not a justifiable reason for exemption. It is therefore important that staff (including contractors) who handle, or are likely to handle sensitive assets, understand fully the impact of such legislation and how it relates to their role.

The UK Public Sector accounts for the bulk of data breach fines. Between March 2011 and February 2012, the total of ICO fines imposed on the public sector was £790,000.

Between 2012 and 2013 ICO fines issued to public entities had increased to over £2 million.

Key Principles

PRINCIPLE ONE

ALL *information that HMG needs to collect, store, process, generate or share to deliver services and conduct government business has intrinsic value and requires an appropriate degree of protection.*

PRINCIPLE TWO

EVERYONE *who works with government (including staff, contractors and service providers) has a duty of confidentiality and a responsibility to safeguard any HMG information or data that they access, irrespective of whether it is marked or not, and must be provided with appropriate training.*

PRINCIPLE THREE

Access to ***SENSITIVE*** *information must ONLY be granted on the basis of a genuine "need to know" and an appropriate personnel security control.*

PRINCIPLE FOUR

Assets received from or exchanged with external partners ***MUST*** *be protected in accordance with any relevant legislative or regulatory requirements, including any international agreements and obligations.*

Public Records Act 1967.

Records selected for preservation may be retained under Section 3(4) of the 1958 Act or closed under an exemption provided by the Freedom of Information Act 2000. Decisions over retention or closure are driven by perception of residual sensitivities at the time that release is being contemplated.

Potential Consequences of Unmanaged PSTs

This tangled web of overlapping regulations all speak to preservation of email. Not knowing the contents, location or indeed the owner of a PST file can put the organisation's data at substantial security risk and leave them wide open to legal sanctions, regulatory fines or other consequences.

Under each of these Acts, the provision for retention varies and there are different consequences for organisations who do not comply. The Freedom of Information Act includes a penalty scheme for non-compliance, whilst the Data Protection Act is more severe.

In addition to fines, which can range from relatively trivial to substantial, there is the consequence of loss of confidence. When this happens to a commercial concern, the ramifications are typically reduced turnover and other negative business consequences. When this occurs to a public entity, the situation is a bit different. Because such entities are not competitive – the consequences of loss of confidence may include staff changes, either by vote or fiat, and even reduced funding.

Do PST Files affect Protective Marking?

From April 2014, the Government Protective Marking Scheme was replaced by the Government Security Classification scheme which is far easier and assumes all information pertaining to public entities is by default, Official. But does all legacy information need to be reclassified and does previously unclassified information now need to be reclassified as Official? The good news is that the answer is in most cases, no.

The **'Working with OFFICIAL Information v1.2 – April 2013'** document explains… *As a rule, organisations are not required to retrospectively remark legacy information or data that uses the old protective markings. Nor does information or data need to be remarked where it is in continued use within an organisation, provided that users / recipients understand how it is to be handled in line with the new Classification Policy.*

However, where legacy information or data bearing a former protective marking is to be shared or exchanged between organisations, or with external partners, the originator should consider remarking with the appropriate security classification. At the very least, meaningful guidance should be provided about how the asset should be protected in line with the new approach.

Many workers favour PSTs as a way to organise/keep older emails particularly if restricted by mailbox quota limits but they don't understand the risks.

This is why many public sector IT departments are prioritising PST elimination as a critical IT project.

For example, The National Archives, HM Passport Office and other public sector institutions have already issued guidelines about the use of PSTs, and instructions for users to not use .pst file formats to capture emails outside of Outlook.

So, whilst PSTs don't specifically create an issue for previously classified or unclassified information, when it comes to key principles, they still present a significant risk. PSTs can fly under the radar of central IT, fall outside of any compliance or retention policies and are easily corrupted or lost so they still present a risk to any organisation. Public entities who are subject to more stringent data protection and regulation guidelines, cannot afford to ignore them.

Operational Reasons to Eliminate PST Files

PST files also present a number of issues for the IT department: location, access, ownership, volume of storage, content and age of data all of which effect cost, risk and resource.

PST files are difficult to locate

PSTs can be located almost anywhere. Older versions of Outlook create them by default on a user's desktop or laptop, however that does not stop them being located on corporate servers, removable media such as USB and flash drives etc., or even home PCs. This makes it very difficult for IT departments to manage and control information centrally.

PSTs are neither secure nor reliable

Highly portable; PSTs can be disconnected from Outlook and copied or moved with ease. They can be seen as a great way of moving email data between people and/or organisations quickly. They can be password protected, although a simple search on the internet will find any number of programs that can crack these passwords.

Notoriously unreliable, PSTs were never designed to hold the amount of data they do today. Users pour more emails into them blissfully unaware of the risk posed to their data.

10-15% of an IT departments daily helpdesk calls can be taken up with looking after corrupt or lost PST files.

PSTs are not always available

Outlook must have access to the location where the PST file is stored. This is fine for office-based users who have the same access to either local or network storage, however if the user has the ability to work from different desktops or locations they may not be able to gain access to the PSTs. Also, if the user uses Outlook Web App (OWA) then they cannot gain access to the files. As more and more organisations embrace BYOD and mobile workforces, the risk is exacerbated.

Secondly PST files can be disconnected by users from Outlook profiles either inadvertently via a failure such as a power outage or PC crash or by the user 'closing' them. For most users, once the PST is 'closed', it is either forgotten about or they cannot find it again, which creates an 'orphaned' PST. Orphaned PST files can still contain valuable business information that may need to be preserved or discovered.

PST files are rarely backed up

Although this depends on the location and how an IT department manages PSTs, if they are located on desktops and laptops there is a very high chance that they will fall outside the corporate backup strategy and therefore not be protected. If however, they are located on network shares, chances are they are being backed up, however this in itself brings a set of new challenges to the IT department …

The average size of a PST is 1.3 gigabytes (equivalent to more than 100,000 emails).

Many organisations average 3-4 PSTs per user.

Every time Outlook connects to a PST- or if one email is added to it, it marks the PST as requiring backup and backs up the entire PST file. But the size of individual PST files is not the biggest problem. Most enterprises have thousands of PSTs littered throughout their infrastructure going unseen and unprotected. So the scale of the problem with PSTs is significantly larger than most organisations realise.

How can we solve the issue of PSTs?

Project-based PST Management

One solution is to deploy a PST management tool. This will find all PSTs across the organisation's network and help determine their contents. Items which must be kept can be re-ingested into inboxes, or better still correctly classified and archived, and any items not subject to retention policies can be deleted.

The human factor is still the primary cause behind data and information breaches.

An automated solution that controls the location, retention and deletion of data can go some way to helping public entities mitigate risk, ensure compliance and respond quickly to discovery or disclosure requests

The benefit of a one-time project is that it enables IT to quickly understand the scale of the problem that PST files are causing, and to then take appropriate action to regain control over existing email stored within PST files. As it is a one-off exercise with no ongoing investment required, it can be easier to justify the overall cost of the project, but it doesn't of course address the original reasons why users have been creating PST files. Even if end users are prevented from creating new files, an alternative means may need to be provided for them to retain selected email for their future reference.

Information management and email archiving solution

A longer term and more comprehensive solution is a comprehensive email archiving solution which includes modules for policy, retention management, compliance, and discovery that include PST location, migration and elimination. An Information management solution archives emails based on adherence to rules-based policies, and automatically applies retention and disposition strategies. The users aren't required to do anything, nor are their preferred environments compromised.

These solutions can eliminate the need for PST files because they will proactively archive email yet provide users a direct way to access those stored emails, eliminating the need for any local storage. To alleviate the need for additional storage for archived email, these solutions include compaction routines which automatically compress emails for archiving and conversely decompress them when they are accessed.

The preferred information management solutions use a "manage in place" strategy, wherein policies and retention management will be applied regardless of where an email is found (live, stored locally, or archived). This ensures that IT has a consistent understanding of the landscape of stored emails.

Preferred information management solutions also offer search and discovery capabilities. Users naturally engage search engines to retrieve older, archived emails, and search must be part of the information management solution. More sophisticated search capabilities, under the requirements of discovery, must also be provided, wherein legal professionals can query email archives and mailboxes to locate and catalogue potentially-relevant emails in the face of litigation.

Finally, these solutions need to offer a preservation mechanism that permits authorised personnel to place such emails under legal hold, such that the email, any attachments, and all relevant metadata are preserved and secured from further editing or modification.

In Summary … What are the Benefits of Managing PST files?

Corporate Risk

Reduce Risk

- Mitigate risk association of unmanaged email data
- Protect against end user data loss and intellectual property data loss.
- Implement robust data retention and defensible deletion policies
- Help with compliance, Freedom of Information, Data Protection and other regulations.
- Support eDiscovery and eDisclosure requests

Operational Benefits

Reduce Costs

- Streamlined processes with centralised storage
- Reduce IT overheads
- Reduce the amount of data to back up and restore

Improve Performance

- Alleviate pressure on storage and back up windows
- Improve restore times of business-critical file servers
- Quicker retrieval of centrally stored information
- Reduce IT support requests
- Remove obstacles to hardware upgrade, BYOD, VDI or Office 365 migration projects

About Barracuda Networks, Ltd.

Protecting users, applications, and data for more than 150,000 organizations worldwide, Barracuda Networks has developed a global reputation as the go-to leader for powerful, easy-to-use, affordable IT solutions. The company's proven customer-centric business model focuses on delivering high-value, subscription-based IT solutions for security and data protection. For additional information, please visit **www.barracuda.com.**

A Barracuda Company

Barracuda

Barracuda Networks Ltd.
6 Richfield Place
Reading
Berkshire, RG1 8EQ
United Kingdom
t: *+44 (0)118 951 1211*
e: *emeainfo@barracuda.com*
w: *barracuda.com*