BULLET BACKGROUND PAPER

ON

<ORG> SHARED (Y:) DRIVE DATA

INTRODUCTION

The explosive growth and use of technology over the last 10 years within the <ORG> has resulted in a 600GB data landfill of loosely structured, unmanaged data on the shared (Y:) drive with various read/write permissions applied. Periodic clean-up initiatives have failed and have not addressed the root cause of the problem: a lack of true content management.

CAUSE

- Consistent access to an abundance amount of data storage has resulted in a perception that the shared network drive provides inexpensive and safe file storage.

- There are no data limits imposed.

- Data is not organized by unit even though Paragraph 1.7.4.1.,<ORG>FWI 33-115 indicates that each unit is responsible for monitoring and maintaining unit directories.

- There is no verbiage directing who is responsible to appoint the drive monitor; the appointment authority is difficult to define since the current folder names do not follow typical command structure.

- There is no schedule indicating how often monitoring must take place and when maintenance must be accomplished.

- There are haphazard read/write permissions granted to groups and individuals at various levels within the current structure.

  -- Per paragraph 1.7.4., <ORG>FWI 33-115, the shared directory is for sharing information between units and/or sections.

  --- Over the last 10 years permissions have strayed away from the initial permissions which were read/write permissions to the specific security group associated with the folder and read only permissions granted to the remaining domain users.

  ---- Placement of privacy act data subsequently discovered as being accessible to all resulted in additional permission restrictions being applied at various folder levels to protect data.

  ---- Group membership is not kept up-to-date as personnel transfer within organizations.

MSgt Houston/111CF/SCXK/1305/gmh/26 Oct 10

DEFICIENCY

- Generally not considered when evaluating the total cost of the shared network drive is the amount of time required to sort through folders identified by cryptic naming conventions, folders containing thousands of files, and identifying the latest version of a document.

- A small percentage of existing data constitutes “Official Records” which must be preserved.

- Much of the data falls into a non-record or convenience copy category.

  -- There is a subset of this data that is subject to the Privacy Act of 1974 which must be protected and tightly managed.

    --- The Base Privacy Manager receives a minimum of one notification monthly regarding unprotected Privacy Act data on the shared drive.

      ---- The <ORG> has a continuing affirmative responsibility to safeguard personally identifiable information (PII) in its possession and to prevent its theft, loss, or compromise.

      ---- The Privacy Breach Reporting Process is a tedious and time-consuming process.

IMPACT

- Without structure, identifying documents that should be official records or that require privacy act protection is virtually impossible and can leave our organization legally exposed and liable.

- Wasted man-hours searching for data

- Duplicate files wasting space

CORRECTIVE ACTION RECOMMENDATIONS

- Phase 1: ASSESS: Commanders responsible for data as determined by the top-level function name are directed to appoint two individuals to oversee the content assessment review.

  -- The shared drive must be limited to Read Only permissions.

  -- A temporary drive with storage limits can be created for current files needing to be shared between organizations during the assessment period.

  -- Appointees are given one month to review all shared drive content and identify files for deletion, records retention or shared requirements.

--- Records custodians must evaluate information their office has stored on the shared drive and move official records to the proper ERM folder on the X: drive.

- Phase 2: TRANSITION: Based on the information discovered during the Assessment Phase, appointees are given one month to address:

  -- Non-records (e-trash) that can be deleted.

  -- Applications and databases that should be stored on a dedicated server (K: drive) as opposed to a shared content repository.

  -- Application of records management rules and principles to identify official organization records for movement to the ERM drive (X: drive) to facilitate the <ORG> achieving greater records management compliance.

  -- Identifying remaining shared content.

  -- Create a back-up image of read only Y: drive and keep for one year following transition to facilitate replacement of erroneously deleted data

- Phase 3: IMPLEMENTATION: Re-write <ORG>FWI 33-115 to establish naming conventions, standards, data storage limits and governance.

  -- Include file size and type restrictions and impose data storage limits

  --- Prohibit placement of executable files on all but the Application (K:) drive.

  --- Impose size limitations for audio, video, and imagery files.

  -- Create two separate drives to address past permissions issues.

  --- The R: drive, a Restricted Office drive provided to share office-specific information. Membership is limited to members of the office user group. Offices may use the R: drive to maintain information not accessible outside of the office. Data such as recall rosters, leave, TDY schedules and internal office procedures may reside on the R: Restricted drive.

  ---- Protect PA data by limiting access to those with an official need to know

  ---- Prohibit storage of official records on the R: drive.

  ---- If storage limits are exceeded, files that have not been accessed for 1 year will be purged. Purged files are saved to back-up for a period of 90 days before deletion to provide end users with a method of retrieval.

  --- The S: drive, an open Shared drive provided to share information among the wing. Anyone may use the S: drive to maintain information to be shared.

Information such as training presentations and event files may reside on the S: Shared drive.

---- Prohibit storage of official records on the S: drive.

---- Once a task or event has been completed, the information owner will remove the files from the S: drive and properly file it in the official records (X:) drive, Restricted office (R:) drive or Personal drive (L:) for personal reference as appropriate.

---- If storage limits are exceeded, files that have not been accessed for 1 year can be purged. Purged files are saved to back-up for a period of 90 days before deletion to provide end users with a method of retrieval.

- Phase 4: SUSTAIN: Develop a plan/program to identify content which can be deleted to ensure that our organizational shared drive continues to adhere to the newly established guidelines which will be outlined in the re-write <ORG>FWI 33-115.

PREVENTATIVE MAINTENANCE

-- Establish a wing "Cyber Down Day" in which all users will clean files from electronic network drives such as L, M, O, and R . (Files on the X: drive are purged by the Records Custodian at the end of each FY and CY).

-- The NCC must identify and remove files that haven't been accessed in more than one year.

-- The NCC must identify files that contain PII (keyword searches such as "alpha", structure searches such as ###-##-### for SSN or ###-###-#### for phone).

-- The NCC must identify and remove duplicate files.

SUMMARY

- The case for performing legacy cleanup is clear – current infrastructure costs, manual clean-up costs, and PII breach risks all point to a revised content management approach to manage an ever increasing volume of information.