

Cyber Security Investigative Report

February 28, 2013

Prepared by

John E. Jorgensen
Senior Forensic Analyst
The Sylint Group
Suite 600
240 North Washington Blvd
Sarasota, Florida 34236

Re:

CASE INFORMATION

City of Sarasota Case # SARA-110439
City of Sarasota Case # SARA-120454

Table of Contents

Introduction	3
Case Background.....	4
Engagement RFQ #CAC 2012-01 of 11/8/2011.....	4
Engagement RFQ #CAC 2012-1 Expanded PO # PD-211318 Approved in City of Sarasota Commissioner’s Meeting of March 5, 2012.....	5
Investigation Tasks.....	6
Reference Materials and Evidence	7
Summary of Findings.....	8
Time Line of Events	8
Synopsis of Finding 1 – Deleted Emails.....	8
Synopsis of Finding 2 – Unauthorized Email Searches.....	10
Synopsis of Finding 3 – Best Business Practices and Cyber Security Threat Analysis.....	14
Support of Findings.....	17
Supporting Technical Information	17
Attached Documents	29
1. Network Diagram.....	29
2. Time Line of Events.....	29
Recommendations	30

Introduction

The Sylint Group, Inc. (Sylint) was engaged by the City of Sarasota on November 8, 2011, with the approval of the City Commissioners to conduct an audit/investigation into allegations by a private citizen that City Business related emails were potentially destroyed in the late 2011 time frame. During the course of this audit/investigation Sylint identified unusual activity and significant issues regarding the management of the City of Sarasota Information Technology (IT) department operations and the potential misuse of access to City of Sarasota email data and potential exposure of Personal Identifiable Information (PII) and Personal Health Information (PHI). A second audit/investigation was begun to resolve these issues. Because of the nature of the issues and potential violation of the Cyber Fraud and Abuse Act and violations of the Florida Sunshine Law Statutes Sylint proposed to the City Commissioners that Law Enforcement be notified. Law Enforcement reviewed the information collected by Sylint and subsequently opened an investigation which included investigators from Housing and Urban Development (HUD), Federal Bureau of Investigation (FBI) and the Florida Department of Law Enforcement (FDLE). The Sylint report does not address the status of the Law Enforcement investigations.

Simultaneous with the Sylint audit/investigation another audit firm, SUNERA, was asked to perform a COBIT audit/assessment of the City of Sarasota Information Technology (IT) Department. The associated report was issued in January 2012. The independent SUNERA report mirrors Sylint's reported findings concerning the IT Department cyber security, Best Business Practices and operational management problems.

Sylint's evaluation and SUNERA's report were used by Sylint to develop a plan for correcting both cyber security and operational management deficiencies with the City of Sarasota IT Department and providing recommendations for IT management changes and IT's interface with their client departments. SUNERA's report contained numerous and significant cyber security issues and therefore over one third of the report was redacted. Although Sylint, together with the City of Sarasota IT department and the Audit and Clerk's Office have addressed and resolved a majority of the cyber security issues identified there remains problems that continue to be addressed. The SUNERA report will continue to remain redacted until all issues are resolved. Likewise, Sylint is not publicizing further cyber security issues that we have identified because of security concerns. Sylint interfaces with and addresses cyber security attacks to public entities, to include Law Enforcement, City Municipalities, and School Districts, in detecting, remediating and criminally prosecuting the offending parties and is acutely aware of the potential vulnerability of protected information and infrastructure. There are significant legal and litigation issues associated with these attacks and the unauthorized disclosure of Protected and Personal information which places our clients at high risk. Maintaining the security of the data, services and infrastructure of the City of Sarasota is of primary importance.

Case Background

Engagement RFQ #CAC 2012-01 of 11/8/2011

The Sylint Group, Inc. (Sylint) was engaged by the City of Sarasota, with approval by the Commissioners through the Auditor and Clerks Office, to investigate an anonymous allegation that City of Sarasota emails may have been deleted from the City's email system by City employees during the September 2011 time frame.

In order to determine if emails had been deleted Sylint forensically imaged a number of computers to include the City Manager, the Deputy City Manager and Heather Essa (Auditor and Clerk's Office). A number of emails were found permanently deleted from the City Manager's and Deputy City Manager's computers. No emails were found permanently deleted from Heather Essa's computer (which includes the archive backups).

In order to determine if the emails were irrevocably deleted from the City of Sarasota's email Microsoft Exchange System it was required of Sylint to review the Exchange System email , capture, retention and backup processes. During the review of the City's Exchange email system and the attempt to recover the missing emails from the City Manager's and Deputy City Manager's email accounts a number of problems were encountered and other network and operational issues were discovered. The problems encountered and the issues discovered were recognized as two separate but related events. The first event involved the potential deletion of emails from the City of Sarasota Exchange Email System. The second event was the discovery of extensive Cyber Security issues which exposed the City network to breach.

The problems discovered were both technical and managerial and included: 1) a lack of personal knowledge in the Information Technology department to accurately and completely document and describe the Exchange email system and how it functioned; 2) the fact that Operating Software "patches," "updates" and "revisions" had not been installed, in some cases, for more than three to four years; 3) the backup of data servers , data bases and systems was failing and could provide for the inability to recover data; 4) various department requirements were not being met because of legacy and outdated software; and 5) various security, event and operational system logs were not being collected or maintained.

Other issues that became apparent including 100's of email searches, open ended, including EXEMPT data, were run, collected and burned to CD's and flash memory devices by certain members of the IT department, and importantly were not instigated by the Public Records Request process. The email searches were run on certain senior people of the Audit and Clerk's Office, certain Commissioners and other individuals associated with ongoing or potential

investigations or high profile matters. The email searches included EXEMPT data that contained Personal Identifiable Information and Personal Health Information.

It was also determined that “dummy” System Administrator Access Accounts had been set up which allowed access to the City Network without proper User account identification tracking capability. Access to the City Police Department email system was through the City email access process and therefore experienced the same security problems that existed on the City email system. The network and email system security problems had potential criminal ramifications and as a precaution, to allow for formal interviews of those people involved and to prevent the possible compromise of evidence, Sylint recommended that the Commissioners consider asking Law Enforcement to open and investigation. The Commissioners subsequently voted to ask Law Enforcement to evaluate the possibility of Criminal Behavior. Law Enforcement made that evaluation and decided to proceed with a formal investigation.

Simultaneous with the work that Sylint was conducting, another national Cyber Evaluation firm SUNERA, at the behest of the City of Sarasota Auditor and Clerk, was conducting a COBIT Audit of the City IT department. The findings of Sylint and SUNERA coincided in their evaluation of operational and security problems within the City of Sarasota IT department. The Sylint evaluation by nature of the investigation was more in-depth. It became obvious that the serious security and operational problems identified by both firms needed to be addressed immediately in order to prevent the City of Sarasota network from operational failure and potentially a serious security breach.

As a result of Sylint’s findings Sylint has divided its report into three separate but related areas. These three areas are addressed in the order of resolution necessary to determine the original issues of deleted emails and potential misuse of the City Network and data. The three areas are: 1) Investigation of Deleted Emails and Potential Misuse of the City Network and Resources; 2) IT Operational Problems; 3) Cyber Security and Business Continuity Problems.

Engagement RFQ #CAC 2012-1 Expanded PO # PD-211318 Approved in City of Sarasota Commissioner’s Meeting of March 5, 2012

The expanded PO # PD-211318 provided for investigation, identification and recommended resolution of the IT Operational Problems, Cyber Security Problems to include Business Continuity Problems. The expanded tasks included providing IT management guidance and assistance in finding a new IT director.

Investigation Tasks

Initial Investigative Tasks (PO#PD-211318)

At the request of the City of Sarasota a computer / digital data forensic investigation was initiated with the following purpose:

1. Secure all evidentiary materials received.
2. Create forensic images of computers / devices belonging to the following individuals:
 - a. City Manager
 - b. Deputy City Manager
 - c. City Auditor
 - d. City of Sarasota Email Server data as required
3. Perform forensic analysis on the data from the above identified devices and determine if emails were irretrievably deleted.
4. Provide written reports of all findings and recommendations as required.

Expanded Investigative Tasks (PO#PD-211318)

1. Investigation, identification and recommended resolution of the IT Operational Problems
2. Investigation, identification and recommended resolution of City of Sarasota Cyber Security Business Continuity Problems.
3. Provide IT management guidance and assistance in resolving IT management problems,
4. Assist the City of Sarasota Clerk and Audit Office in finding a new IT director.

Reference Materials and Evidence

Sylint entered into evidence four computers, a mass storage device, and storage media assigned to the individuals in this case, as noted in the following table:

Evidence Item #	Serial Number	Description
Sara-110439-1	Service Tag# D4705Q1	Dell Laptop Computer (Marlon Brown)
Sara-110439-1.1	WXB1A11E7106	Dell Laptop Hard Drive (Marlon Brown)
Sara-110439-2	Service Tag# 8R7SJH1	Dell Laptop PC (Robert Bartolotta)
Sara-110439-2.1	5NJ1GMZX	Dell Laptop Hard Drive (Robert Bartolotta)
Sara-110439-3	Service Tag# FSCB2C1	Dell Laptop PC (Heather Essa)
Sara-110439-3.1	X6HTTE71T	Dell Laptop Hard Drive (Heather Essa)
Sara-110439-4	C86FXAR6DM73	Apple Time Capsule - (Heather Essa)
Sara-110439-4.1	YMG0GHRA	Apple Time Capsule Hard Drive (Heather Essa)
Sara-110439-6	2GE6F1KT	External Hard drive with Mailboxes from Journal
Sara-110439-7	N/A	CD with Heather Essa Mailbox 12-06-2011
Sara-110439-8	N/A	CD with AM Logs/Documents
Sara-110439-9	N/A	CD with AM Logs/Documents
Sara-110439-10	N/A	CD with AM Logs/Documents
Sara-110439-11	N/A	CD with AM Logs/Documents
Sara-110439-12	110920 110-1247880	TAPE with Backup
Sara-110439-13	N/A	CD with Public Records Work Orders export list
Sara-110439-14	Service Tag# F35RKQ1	Dell Laptop (Sandra Coleman)
Sara-110439-14.1	5VH6G7DB	Dell Laptop Hard Drive (Sandra Coleman)

In addition to that material taken into evidence by Sylint the following information was used in this investigation:

1. Network diagrams
2. Operating System Event and Security Logs
3. Exchange Email System Logs, Journal Information, Event Logs, Archive Manager and Archive Manager 2 event logs, email data base.
4. Active Directory Logs

5. Firewall Logs
6. Public Records Request Logs
7. Event Logs for data searches on the Archive Manager and Archive Manager 2.
8. Backup data and Logs for the Exchange Email System
9. The SUNERA Report

Summary of Findings

Time Line of Events

The following is a chronological overview of key events associated with the computer information forensic examination, analysis and other responsibilities for this case:

1. Forensic imaging of computers and devices
2. Collection of associated data
3. Forensic analysis of data
4. Attempted recovery of relevant emails
5. Documentation of City of Sarasota Exchange Email System
6. Interviews with City of Sarasota IT Department
7. Identification of Cyber Security Risks
8. Identification of potentially compromising events associated with exempt emails
9. Review of SUNERA report
10. Initial Report to City of Sarasota Audit and Clerks Office and City Counsel
11. Expanded Investigation authorized
12. Contact Law Enforcement for potential Computer Fraud and Abuse Act violations
13. Provide Law Enforcement with documentation and data for evaluation
14. IT Management placed on administrative leave
15. Remediation of Cyber Security Threats
16. Address various City Department software development problems
17. Correct various software issues within Department clients
18. Provide recommendations for Applications and Control software
19. Documentation of City of Sarasota Email System and Network
20. Provide City of Sarasota IT Department management oversight
21. Recommendations of restructuring the City of Sarasota IT Department to effect necessary operational and network changes
22. Assistance in finding and qualifying new IT Director
23. Briefing new IT Director on events and status of City of Sarasota Network
24. Provide City of Sarasota City Counsel Commissioners with an Interim Report
25. Assist in transition to new IT Department Management
26. Conclude investigation and provide a Final Report

Synopsis of Finding 1 - Deleted Emails

TASK: Determine if emails had been irretrievably deleted from the City of Sarasota email Exchange System and who was responsible for the deletion. The computers and other data memory media provided for this investigation were: 1) City Manager, 2) Deputy City Manager and 3) City Auditor. Access to the City of Sarasota Email Exchange System and Network was provided.

1. City Manager's Computer

The City Manager's computer was forensically examined and analyzed. The forensic analysis indicated that approximately 11,000 emails were deleted from the email storage on the computer. The deleted or "Orphan" emails were recovered forensically and emails were recovered from the City of Sarasota Exchange Email system and email system backups that were valid and usable. Approximately 103 emails were unrecoverable even though all possible means of recovery were exhausted.

Deputy City Manager's Computer

The Deputy City Manager's computer was forensically examined and analyzed and there were 747 emails that were deleted and required further attempts at recovery. The computer used by the Deputy City Manager was newly placed into service. The deleted emails may have been on the Deputy City Manager's old computer however the Information Technology Department could not definitively state where the computer was and did not have the appropriate disposition records. Emails were recovered from the City of Sarasota Email system and cross referenced to Group mail addresses. Therefore, of the 747 emails that were deleted it could not be conclusively determined what emails were recoverable.

2. City Auditor's Computer

The City Auditor's computer was forensically examined and analyzed. The City Auditor also provided Compact Disks (CD) and a mass storage device. The City Auditor email was either active on the computer or present within an archive email file that was maintained by the Auditor and provided to Sylint by the City Auditor. There were no unaccounted for emails relative to the City Auditor. However, there were emails on the City Auditor's email archive that could not be found on the City of Sarasota email system when searched.

3. City of Sarasota Email Exchange System

The City of Sarasota Exchange Email System was analyzed and mapped. The City of Sarasota IT department could not provide a network diagram or explanation of how the Exchange Email System was setup and functioning. In fact, the Email System was not

functioning properly with various capabilities and processes either failing or executing improperly. In particular Archive Manager and Archive Manager 2 were not functioning properly, the Journal function failed, backups were failing and the Software and Security Updates to Exchange were, in some cases, 3 years out of date. These serious problems were noted by both Sylint and within the SUNERA COBIT Audit Report.

FINDINGS:

1. The City Manager and Deputy City Manager emails deleted from their respective computers by the User cannot be recovered from the computers using forensic means or from the City of Sarasota Exchange Email system because of the following reasons:
 - a. A well-defined email deletion and retention policy, given the state of the Exchange Email System, was not in place. Such a policy would require the Users to retain all emails on their individual computers with direction for the proper archiving of the emails periodically. The Auditor stated in interview with Sylint that she had misgivings about the Exchange Email system and took it upon herself to archive her emails periodically. The email personal archive process was followed successfully by the City of Sarasota Auditor and resulted in no loss of emails. The importance of this process is exemplified by the fact that there were emails in the Auditor's email archive that could not be found on the City of Sarasota Exchange Email System.
 - b. The issuing of new computers by the IT Department and reuse of the "retired" computer without proper data retention, record keeping or email and data archiving caused emails on those computers that might normally be recoverable to be overwritten through continued use, reformatting or IT processes in reissuing of the computers.
 - c. The failure of Exchange Email data backups, improper verification procedures, improper storage and retention of backups, the improper rotation of backups and a failure to correct and resolve known data backup failure issues.
 - d. To properly upgrade software, install software updates, and upgrade and document server and system configuration for the Exchange Email system. This lack of attention to the proper maintenance of the Exchange Email system caused various failures in both day-to-day operations and longer term data retention.

Synopsis of Finding 2 – Unauthorized Email Searches

TASK: Resolve potential issues of unauthorized email searches of non-EXEMPT and EXEMPT emails for Direct Reports to Commissioners and Commissioners themselves. Sylint addressed with City Counsel and outside Counsel before the Commissioner's the implications of exposed Personal Identifiable Information (PII) and Personal Health Information (PHI) caused by unauthorized email searches without "EXEMPT" restrictions. The unauthorized email searches,

which circumvented the Public Records Request process, and contained EXEMPT information on ongoing City Audit investigations were conducted using IT resources by the City Manager and the Deputy City Manager. The results of these unauthorized email searches containing EXEMPT emails were found on the City Manager's and Deputy City Manager's City laptop computers.

FINDINGS:

- A. Email repository files (.pst) containing EXEMPT emails exclusively for both **Pamela Nadalini** and **Heather Essa** were discovered on Marlon Brown's laptop computer and a reference to a similar email repository file was found on Robert Bartolotta's laptop computer. There are NO official Public Records Request (PRR) associated with the unfiltered search and .pst production activity found on these computers.
 - a. **These .pst files (belonging to Nadalini and Essa) contain emails classified as "EXEMPT" and were not obtained under the Public Records Request (PRR) process.** "EXEMPT" emails contain information about ongoing investigations, Personal Identifiable Information, Personal Health Information or other information termed "Exempt" under the Florida Sunshine Law disclosure laws. "EXEMPT" emails are not normally produced under the Public Records Request.
 - b. **The .pst file (belonging to Nadalini and Essa) production circumvented authorized Public Records Request processes and therefore contained EXEMPT emails that were classified by the City Auditor and Clerk Office.**
 - c. **Neil Bailey's (a former City of Sarasota Information Technology contract employee) login credentials created the email search criteria and executed the unauthorized email search process and created the "Default.pst" file** through the City of Sarasota Exchange Archive Manager. It is unknown who issued the unauthorized instructions to Neil Bailey or if his credentials were used by another individual within the IT department.
 - d. The emails produced in the .pst "Default.pst" files were then further manipulated and sent to the "deleted" folder of the .pst after being viewed by the User "brownm-020" used by Marlon Brown.
 - e. A USB flash memory device with a **"Default.pst" (created through an "archivemanager" search) was attached to Robert Bartolotta's City of Sarasota laptop computer on 9/2/2011.** This is the same type of

“archivemanager” output “Default.pst” file that was found on Marlon Brown’s City of Sarasota laptop computer.

- B. There exist non-recoverable deleted emails associated with Robert Bartolotta’s City of Sarasota (CoS) Exchange email account.
- a. This finding indicates that either a continuing problem exists with the CoS email Exchange System or that emails have been deleted from the CoS email repository through access to the SQL (Structured Query Language) back end.
 - b. Neil Bailey has been described, in interviews with the CoS IT personnel, as a knowledgeable SQL user. Further investigation and interviews are required to determine access to the SQL Exchange Backend.
 - c. Over 100 emails cannot be resolved. The Orphaned version of the email indicates them to be SPAM, junk mail, personal email or advertising. However, the fact that the emails are not on the Archive Manager Server creates grave concern that email data has been manipulated or deleted and would require further forensic investigation to resolve.
 - d. Other deleted emails may exist beyond those recovered as Orphan files. Orphan email forensic discovery does not recover all deleted emails and can only be used as an indicator of the deletion of email process. Further forensic investigation would be required to resolve the extent of email deletion.
 - e. There are strong indications (from email traffic) that Robert Bartolotta’s iPhone is being used for City of Sarasota Business. The policy of allowing personally owned computer and communications equipment for City of Sarasota business should be carefully reviewed and a strong Policy and Procedures should be developed to address potential legal issues and Florida Sunshine Law violations.
- C. Although there were a number of deleted emails associated with M Brown’s laptop computer Outlook email account, all of the identified deleted emails may not have been recovered. M. Brown’s laptop computer, used for this investigation, was issued to Brown in May 2011. Brown’s previous laptop hard drive may have been overwritten by IT. The recovered deleted emails were found on the Exchange Archive server. Sylint requested that Brown’s previous City computer be provided for forensic analysis even though it may have been over-written and placed back in service. Resolution of the computer’s disposition has been successful.

- D. Heather Essa's Mass Storage device did not contain any deleted files. All files were accessible and readable. There was no break in the continuity of the file write structure or large blocks of contiguous zeros or other indicators of data wiping. Essa regularly backed-up the mass storage device to CD's. The CD back-ups were compared to the mass storage device and no discrepancies were found. Two of H. Essa's deleted emails were not found on the Archive Manager Server. The Orphan state of these emails indicates that the two emails were weekly Audit Status Reports from August of 2009 which were forwarded to other individuals and therefore are resident on the Exchange Archive Manager server in other folders. Therefore, through Essa's archive process there were essentially no deleted emails.
- E. **During the review of email search logs, unusual and possibly unauthorized (non-Public Records Request initiated EXEMPT email production) search and production activity (EXEMPT emails) of commissioners email boxes, Pamela Nadalini emails and Heather Riti emails were identified.** In particular on 8/11/2011 an IT department personnel performed a general search of "caragiulop-001" mail box at 8:19 AM and again at 8:51 AM. Other searches of email were conducted that do not have the normal format of a Public Records Request and include "EXEMPT" emails. In particular over a dozen searches of "Pamela.Nadalini" and "nadalini-042" were conducted between 8/25/2011 and 9/29/2011. Commissioners email boxes that were also searched and produced were: "turnert-001", Terry.Turner", including emails sent to nadalini-42 from Atwell, Caragiulo, Shaw, Snyder and Turner. The results of the unauthorized searches and production were provided to the City Manager and the Deputy City Manager (and possibly others) on Compact Disks or Flash Memory Devices.
- F. There were several serious lapses in the IT management of the Exchange email system. These issues could represent serious consequences to the City of Sarasota and were addressed or are currently being addressed by the new IT Director. Noted concerns were:
- a. Lack of knowledge by all levels of IT personnel (from managers to operators) of functional operation of email system and in particular the Archive Managers and Journal email capture and access.

- b. Lack of collection and review of enterprise system logs / access rights & privileges to prevent unauthorized system use and documentation for potential litigation action.
- c. Administrator rights & privileges provided to unauthorized individual(s).
- d. Unauthorized / abusive use of email search process with policies and procedures loosely controlled and monitored.
- e. Cyber Security issues including use of City of Sarasota computer systems for Web gaming on City of Sarasota Computers during and after work hours. The infection of enterprise network resources has been notoriously caused through web based gaming and downloading of inappropriate materials. Safeguarding the security integrity of the City of Sarasota enterprise network should be of high importance.
- f. Improper classification of emails of a personal nature as “EXEMPT” in order to avoid there disclosure during a normal Public Records Request process.

Synopsis of Finding 3 – Best Business Practices and Cyber Security Threat Analysis

TASK: Review the City of Sarasota Computer Network, the network Policies and Procedures, and Network Management to determine the potential Threat and Vulnerability for network Breach and Compromise and the Viability of the Network for Disaster Recovery.

FINDINGS: The Cyber Security Threat and Vulnerability for the City of Sarasota Enterprise Network was “high” to the point of being extremely vulnerable. The extent of the Network vulnerability was also discussed in the SUNERA COBIT Audit Report and also ranked as “high”. Immediate action was taken by Sylint to remediate as many Cyber Security faults identified by Sylint and SUNERA as possible. A number of the issues from Sylint and the SUNERA report are identified below. These issues have been addressed or sanitized as necessary in order to not disclose the ongoing vulnerability. Sylint’s remediation efforts are in blue italics:

Industry and Regulatory Compliance (Impact = High)

PCI Compliance

- *Ensure comprehensive PCI gap assessment is performed by a PCI Qualified Security Assessor (QSA) to identify all systems and business processes*

involved in the processing, transmission, or storage of cardholder data, as well as areas in which the City is not compliant with the standard.

Sylint is a QSA and PCI gap assessment investigator and has assisted The City of Sarasota IT department in correcting various deficiencies. However, an actual QSA assessment needs to be performed once that IT feels confident in its remedial actions.

IT Security (Impact = High)

Network Infrastructure Security

Network and Data Flow Diagrams

- Ensure all network diagrams are updated to reflect the current state of the network architecture, updated after any significant changes and reviewed at least annually.
- Ensure data flow diagrams, which overlay the network diagrams, are created to depict the flow of critical data across information system components.

Sylint has assisted IT in documenting the Network and diagrams should be currently up to date. Review of the diagrams should be part of a formal Cyber Security Audit.

Network Security Standards and Firewall Documentation

- Create configuration standards for network devices, including routers and firewalls, which prescribe specific security parameters and their required configuration values.

Sylint assisted IT with providing direction for reconfiguring network devices. However, this should be a subject of a Cyber Security Audit.

Network Device User Names and Passwords

- Ensure that any insecure administration protocols in place on network devices, such as HTTP and Telnet, are disabled

Sylint oversaw the initial changes made to protocols. However, a Cyber Security Audit is required to validate changes.

Vulnerability and Threat Assessment

- Implement the recommendations identified with the external vulnerability assessment report

Sylint's first assessment identified significant deficiencies. Many of these deficiencies have been corrected; however a Cyber Security Audit is required.

Cisco Firewall End-of-Life

- Procure and install a Cisco ASA 5520 firewall with an IPS feature set

Requires further review and action.

IDS/IPS

- Implement ASA 5520 firewall IPS feature set
- Ensure that an IPS is installed for the redundant Internet connection firewall
- IPS should be configured to generate automated alert notifications to network administration personnel

Requires a Cyber Security Audit to validate and verify changes.

Information System and Server Security (Impact = High)

Microsoft Exchange Security

- Upgrade to the latest service pack to ensure security vulnerabilities are mitigated

Service packs have been upgraded. A Cyber Security Audit is required for assurance.

Media Access to City E-mail

- Disable all Active Directory credentials provided to media outlets due to the security risk associated with providing "Domain User" accounts to non-employees.
- Consider options that would allow media access to e-mail without using Active Directory credentials or authentication

Requires changes to City of Sarasota Policies and Procedures.

Public Access to City E-mail

- Immediately remove the public's access to view e-mail using published internal Active Directory credentials
- Consider options that would allow media access to e-mail without using Active Directory credentials or authentication

Removed for Security Reason

Windows Administrator Account

- Modify name of “Administrator” account
- Discontinue sharing of “Administrator” account among IT administrators
- Modify super user passwords on a regular basis

Policies were put in place. However, a Cyber Security Audit is necessary to validate.

User Administration (Impact = Moderate)

Domain Administrator Access

- Group membership should be highly restricted to only those who require access based on job responsibility.

Implemented but requires Cyber Security Audit to validate.

Password Management (Impact = Moderate)

Password Minimum Age

- Enforce minimum password age of at least one to three days to better ensure that password history of four previously used passwords is enforced

IT Operations (Impact = Moderate)

Application Performance and Availability (Impact =Moderate)

Archive Manager Performance

- Update to the most current version of the Archive Manager software

Accomplished.

System and Data Backups (Impact = Moderate)

Exchange Hosted Services E-mail Retention

- Ensure compliance with public records retention statues and the ability to fulfill public records requests regarding e-mail messages, the City should implement and configure an e-mail solution that captures all messages to and from City personnel

Sylint assisted in developing an implementation plan and selecting the proper equipment and network design. Requires further review and implementation to ensure successful archiving and backup of information.

Support of Findings

Supporting Technical Information

FORENSIC FINDINGS

User Profiles on Each Computer

User Profiles for Marlon Brown's Laptop Computer

Name	Size	Created
Administrator	0.6 GB	06/12/2006 04:45:36 PM
administrator.SRQ	22.4 MB	05/03/2011 08:18:20 AM
All Users	0.7 GB	06/12/2006 03:40:35 PM
brownm-020	17.1 GB	05/03/2011 10:30:35 AM
Default User	1.2 MB	06/12/2006 03:40:35 PM
LocalService	0.7 MB	06/12/2006 04:30:53 PM
NetworkService	0.8 MB	06/12/2006 04:02:05 PM

User Profiles for Robert Batolotta's Laptop Computer

Name	Size	Created
Administrator	452 MB	06/12/2006 04:45:36 PM
administrator.SRQ	5.4 MB	10/20/2008 02:48:41 PM
All Users	2.0 GB	06/12/2006 03:40:35 PM
bartolottar-020	24.8 GB	10/17/2008 11:37:01 AM
colemans-045	5.4 MB	05/13/2009 08:59:14 AM

Default User	1.2 MB	06/12/2006 03:40:35 PM
LocalService	6.5 MB	06/12/2006 04:30:53 PM
NetworkService	6.4 MB	06/12/2006 04:02:05 PM
urbanskil-045	5.3 MB	10/20/2008 09:50:05 AM

User Profiles for Heather Riti Essa's Laptop Computer

Name	Size	Created
Administrator	229 MB	06/12/2006 05:45:36 PM
administrator.SRQ	14.2 MB	10/25/2007 02:01:15 PM
All Users	1.6 GB	06/12/2006 04:40:35 PM
Default User	1.0 MB	06/12/2006 04:40:35 PM
LocalService	23.6 MB	06/12/2006 05:30:53 PM
mallettw-042	5.7 MB	08/15/2011 04:34:13 PM
NetworkService	1.3 MB	06/12/2006 05:02:05 PM
public-042	143 MB	05/04/2009 12:59:36 PM
ritih-047	5.3 GB	05/02/2008 10:15:52 AM
urbanskil-045	7.7 MB	10/30/2007 04:15:10 PM

Email Containers on Each Computer

The following email containers were found on Marlon Brown's laptop computer:

Name	Size	Created	Accessed
Default.pst	1.0 GB	09/25/2011 09:07:37 PM	10/12/2011 11:41:21 AM
outlook.ost	8.3 GB	05/03/2011 02:15:23 PM	10/12/2011 11:41:23 AM
Personal Folders(1).pst	265 KB	09/25/2011 09:16:02 PM	10/12/2011 11:41:22 AM

Marlon Brown's email is contained within outlook.pst. Personal Folders (1).pst is empty and not in use. Default.pst resides on Marlon Brown's "desktop" screen and contains emails belonging to Pamela Nadalini and Heather Riti Essa.

This Default.pst was created from Archive Manager on 09/21/2011 by a User using Neil Bailey's account.

The screenshot shows the Quest Software Archive Manager Search Log interface. The search criteria are set for User: Neil Bailey, Search Date: Between 9/20/2011 and 9/21/2011, and Search All Users: All. The search results table is as follows:

User	Date	Search All	IP Address	Search Criteria
Neil Bailey	9/21/2011 4:34:12 PM	Yes	10.20.16.32	Search all emails where The Email was sent between 1/1/2011 and 9/21/2011 The Email was Sent To or From Marvellen,McGrath@sarasotaqov.com; mcarath_marvellen@yahoo.com
Neil Bailey	9/21/2011 4:32:49 PM	Yes	10.20.16.32	Search all emails where The Email was sent between 1/1/2011 and 9/21/2011 The Email was Sent To or From Marvellen,McGrath@sarasotaqov.com; mcarath_marvellen@yahoo.com
Neil Bailey	9/21/2011 11:43:02 AM	Yes	10.20.16.32	Search all emails where The Email was sent between 7/1/2011 and 9/21/2011 The Email was Sent To or From Pamela.Nadalini@sarasotaqov.com; Heather.Riti@sarasotaqov.com
Neil Bailey	9/21/2011 11:16:22 AM	Yes	10.20.16.32	Search all emails where The Email was sent between 7/1/2011 and 9/21/2011 The Email was Sent To or From Pamela.Nadalini@sarasotaqov.com; Heather.Riti@sarasotaqov.com

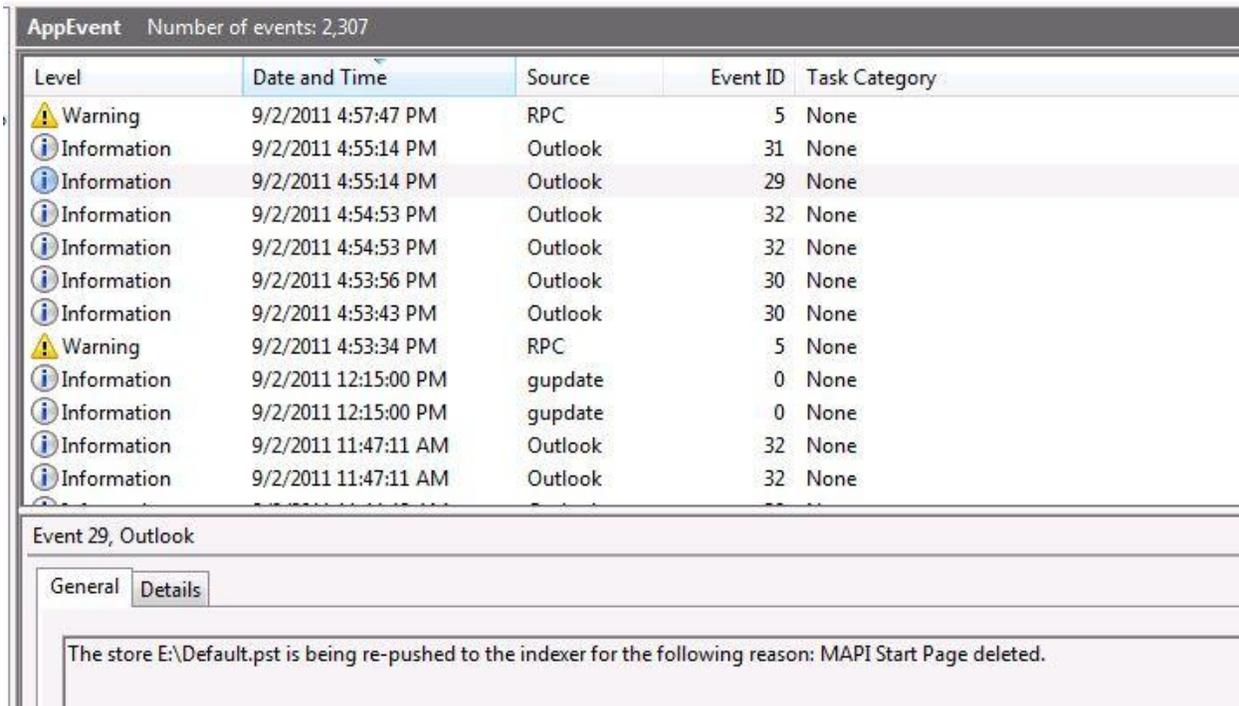
The following email containers were found on Robert Bartolotta’s laptop computer:

Name	Size	Created	Accessed
archive.pst	3.0 GB	10/31/2008 09:38:20 AM	10/12/2011 11:27:50 AM
outlook.ost	11.4 GB	10/17/2008 12:12:19 PM	10/12/2011 11:27:51 AM

Both email containers contain emails belonging to Bartolotta.

On 09/02/2011, a Default.pst was opened by Bartolotta from an “E:\” drive, an Ativa My 4GB USB Device. This file, Default.pst, does not exist on his laptop computer.

This Default.pst is not the same Default.pst that was found on Marlon Brown’s laptop computer. Sylint can determine file similarities or differences when given access to and reviewing the file located on the Ativa drive.



Level	Date and Time	Source	Event ID	Task Category
Warning	9/2/2011 4:57:47 PM	RPC	5	None
Information	9/2/2011 4:55:14 PM	Outlook	31	None
Information	9/2/2011 4:55:14 PM	Outlook	29	None
Information	9/2/2011 4:54:53 PM	Outlook	32	None
Information	9/2/2011 4:54:53 PM	Outlook	32	None
Information	9/2/2011 4:53:56 PM	Outlook	30	None
Information	9/2/2011 4:53:43 PM	Outlook	30	None
Warning	9/2/2011 4:53:34 PM	RPC	5	None
Information	9/2/2011 12:15:00 PM	gupdate	0	None
Information	9/2/2011 12:15:00 PM	gupdate	0	None
Information	9/2/2011 11:47:11 AM	Outlook	32	None
Information	9/2/2011 11:47:11 AM	Outlook	32	None

Event 29, Outlook

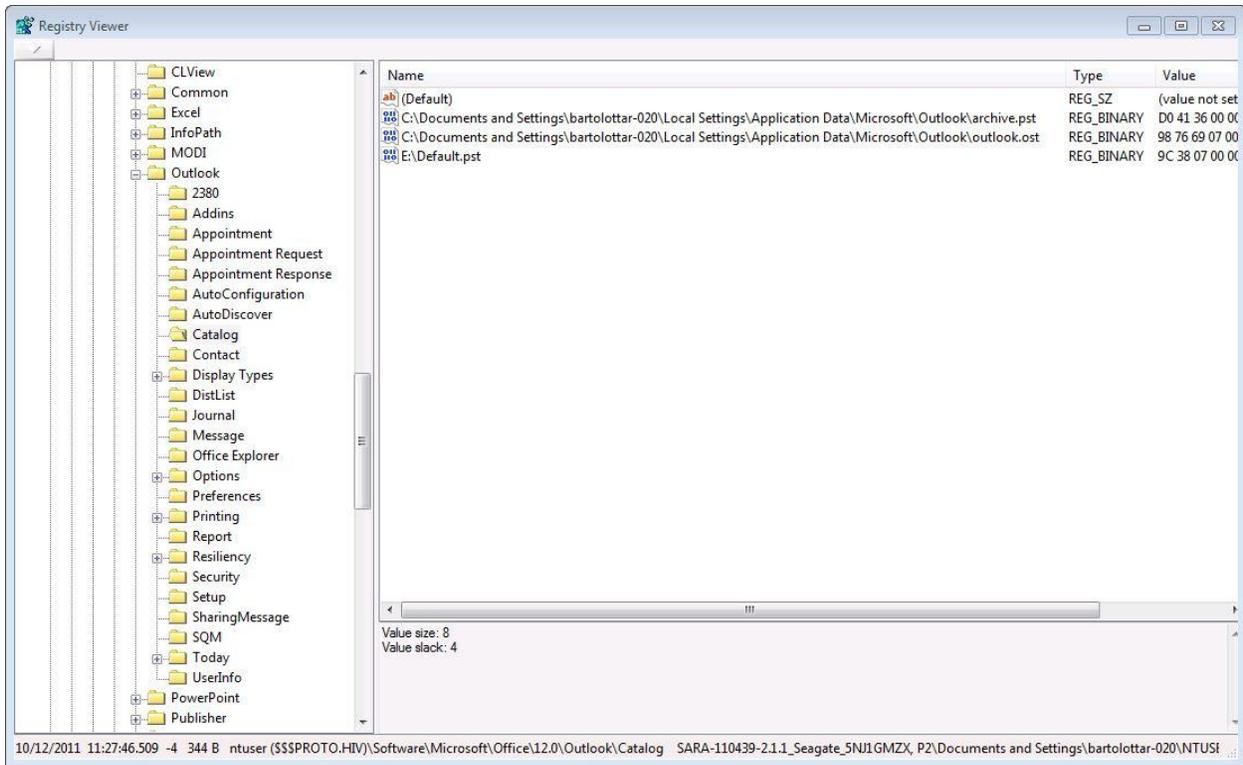
General Details

The store E:\Default.pst is being re-pushed to the indexer for the following reason: MAPI Start Page deleted.

AppEvent Number of events: 2,307					
Level	Date and Time	Source	Event ID	Task Category	
Warning	9/2/2011 4:57:47 PM	RPC	5	None	
Information	9/2/2011 4:55:14 PM	Outlook	31	None	
Information	9/2/2011 4:55:14 PM	Outlook	29	None	
Information	9/2/2011 4:54:53 PM	Outlook	32	None	
Information	9/2/2011 4:54:53 PM	Outlook	32	None	
Information	9/2/2011 4:53:56 PM	Outlook	30	None	
Information	9/2/2011 4:53:43 PM	Outlook	30	None	
Warning	9/2/2011 4:53:34 PM	RPC	5	None	
Information	9/2/2011 12:15:00 PM	gupdate	0	None	
Information	9/2/2011 12:15:00 PM	gupdate	0	None	
Information	9/2/2011 11:47:11 AM	Outlook	32	None	
Information	9/2/2011 11:47:11 AM	Outlook	32	None	

Event 31, Outlook	
General	Details
The store E:\Default.pst has detected a catalog rebuild.	

26479	09/02/2011 16:53:34.000 -4	09/02/2011 16:53:34.000 -4	5	Warning	0	RPC	WS1382	?	#0: "C:\Program Files\Microsoft Office\Office12\OUTLOOK.EXE" /recycle #1: 1632
26480	09/02/2011 16:53:43.000 -4	09/02/2011 16:53:43.000 -4	30	Information	0	Outlook	WS1382	?	#0: E:\Default.pst #1: The store was last opened on a different machine
26481	09/02/2011 16:53:56.000 -4	09/02/2011 16:53:56.000 -4	30	Information	0	Outlook	WS1382	?	#0: E:\Default.pst #1: The store was last opened on a different machine
26482	09/02/2011 16:54:53.000 -4	09/02/2011 16:54:53.000 -4	32	Information	0	Outlook	WS1382	?	#0: C:\Documents and Settings\bartolotta-020\Local Settings\Application Data\Microsoft\Outlook\archive.pst
26483	09/02/2011 16:54:53.000 -4	09/02/2011 16:54:53.000 -4	32	Information	0	Outlook	WS1382	?	#0: C:\Documents and Settings\bartolotta-020\Local Settings\Application Data\Microsoft\Outlook\outlook.pst
26484	09/02/2011 16:55:14.000 -4	09/02/2011 16:55:14.000 -4	31	Information	0	Outlook	WS1382	?	#0: E:\Default.pst
26485	09/02/2011 16:55:14.000 -4	09/02/2011 16:55:14.000 -4	29	Information	0	Outlook	WS1382	?	#0: E:\Default.pst #1: MAPI Start Page deleted
26486	09/02/2011 16:57:47.000 -4	09/02/2011 16:57:47.000 -4	5	Warning	0	RPC	WS1382	?	#0: "C:\Program Files\Microsoft Office\Office12\OUTLOOK.EXE" /recycle #1: 3704
26487	09/02/2011 16:59:30.000 -4	09/02/2011 16:59:30.000 -4	32	Information	0	Outlook	WS1382	?	#0: C:\Documents and Settings\bartolotta-020\Local Settings\Application Data\Microsoft\Outlook\archive.pst
26488	09/02/2011 16:59:30.000 -4	09/02/2011 16:59:30.000 -4	32	Information	0	Outlook	WS1382	?	#0: C:\Documents and Settings\bartolotta-020\Local Settings\Application Data\Microsoft\Outlook\outlook.pst
26489	09/02/2011 16:59:36.000 -4	09/02/2011 16:59:36.000 -4	32	Information	0	Outlook	WS1382	?	#0: C:\Documents and Settings\bartolotta-020\Local Settings\Application Data\Microsoft\Outlook\archive.pst
26490	09/02/2011 16:59:36.000 -4	09/02/2011 16:59:36.000 -4	32	Information	0	Outlook	WS1382	?	#0: C:\Documents and Settings\bartolotta-020\Local Settings\Application Data\Microsoft\Outlook\outlook.pst



Deleted Outlook Express .dbx files were found in the Recycler on Robert Bartolotta's laptop computer. These files do not contain any relevant emails within them, only the initial welcome email.

Name	Type	Type Status	Type descr.	Path	Sender	Recipients	Size	Created	Modified
INFO2	not in list		Recycle bin	\\RECYCLER\S-1-5-21-807563678-782510350-623648099-3721			34.4 KB	03/12/2009 11:38:10.586 -4	07/22/2011 07:21:18

Partition	File	Preview	Details	Gallery	Calendar	Legend	Raw	Sync	Size	Path
27									3.9 MB	C:\WINDOWS\Temp\vpremove.log
28									4.0 KB	C:\WINDOWS\Temp\WGAErrLog.txt
29									136 KB	C:\Documents and Settings\bartolotta-020\Desktop\MrBartolottaInfo.docx
30									7.2 MB	C:\Documents and Settings\bartolotta-020\Desktop\BLR
31									16.6 MB	C:\Installs\Hurrevac2000-Old
32									16.0 KB	C:\Documents and Settings\bartolotta-020\My Documents\memo to commission.docx
33									4.0 KB	C:\Documents and Settings\bartolotta-020\Favorites\Society of Former Special Agents of the FBI, Inc. - Home.url
34									4.0 KB	C:\Documents and Settings\bartolotta-020\Favorites\HartryLaw.com.url
35									4.0 KB	C:\Documents and Settings\bartolotta-020\Favorites\bartolotta-020\Favorites\Cherokee fund.url
36									4.0 KB	C:\Documents and Settings\bartolotta-020\Favorites\Gulf Coast Provider Network.url
37									4.0 KB	C:\Documents and Settings\bartolotta-020\Favorites\AMA DoctorFinder.url
38									4.0 KB	C:\Documents and Settings\bartolotta-020\Favorites\LEOAFFAIRS.COM - Welcome.url
39									4.0 KB	C:\Documents and Settings\bartolotta-020\Favorites\community alliance.url
40									4.0 KB	C:\Documents and Settings\bartolotta-020\Favorites\http--www.seattle.gov-climate-docs-ClimateActionHandbook.pdf.url
41									4.0 KB	C:\Documents and Settings\bartolotta-020\Favorites\Deep Water Horizon Oil Spill Live video link from the ROV monitoring the damaged riser.url
42									140 KB	C:\Documents and Settings\bartolotta-020\Local Settings\Application Data\Identities\{65986956-F9A1-43EF-9120-6A330FD5F5AF}\Microsoft\Outlook Express\Inbox.bak
43									12.0 KB	C:\Documents and Settings\bartolotta-020\Local Settings\Application Data\Identities\{65986956-F9A1-43EF-9120-6A330FD5F5AF}\Microsoft\Outlook Express\Offline.bak
44									76.0 KB	C:\Documents and Settings\bartolotta-020\Local Settings\Application Data\Identities\{65986956-F9A1-43EF-9120-6A330FD5F5AF}\Microsoft\Outlook Express\Folders.bak

The following email containers were found on Heather Riti Essa's laptop computer:

Name	Size	Created	Accessed
archive.pst	1.9 GB	05/21/2008 08:19:24 AM	10/12/2011 03:30:10 PM
Heather Riti.pst	70.3 MB	09/28/2009 10:13:11 AM	10/12/2011 11:24:47 AM
outlook.ost	0 B	05/02/2008 10:19:24 AM	05/02/2008 10:19:24 AM
outlook0.ost	46.5 MB	05/06/2008 08:40:38 AM	10/12/2011 03:51:42 PM
WO21446.pst	166 MB	09/02/2011 12:05:18 PM	09/14/2011 10:46:16 AM

Heather Essa's email is contained within archive.pst, Heather Riti.pst and outlook0.ost. outlook.ost is an empty email container that has never received email. WO21446.pst appears to contain emails relative to an audit and does not contain Heather Essa's email within.

An email comparison was done between the deleted email's resident on the laptop computer (archive.pst, Heather Riti.pst and outlook0.ost) and the City's Archive Manager Program. With the exception of two emails (Audit 09-12 Weekly Update 2- EXEMPT.eml and Audit 09-12 Weekly Update 3- EXEMPT.eml) all other deleted emails are contained within Archive Manager.

It is important to note that emails not directly addressed to Heather Riti Essa are not contained within her Archive Manager repository. For example, Heather has emails on her laptop computer that are not contained within Archive Manager. These particular emails are not addressed directly to Heather, but instead are addressed to recipients such as: EveryoneCityAuditor&Clerk@sarasotagov.com and CentralRecords@sarasotagov.com.

It is also important to note that Sylint only compared deleted items on the laptop computer to the Archive Manager repository. Sylint did not conduct an examination of ALL emails contained on the laptop. **A cursory look indicates that there are emails on the laptop, in an allocated state, that are not within Archive Manager and indicates that there may be a failing of the Archive Manager / Journal operational structure and causes emails to miss capture by the Exchange email system. This could cause a potential Public Records and litigation issue.**

Sample of Emails Not Found in Archive Manager

Name	Path	Sender	Recipients	Created	Modified
Audit 09-12 Weekly Update 2- EXEMPT eml	\\Documents and Settings\vtih-047\Local Settings\Application Data\Microsoft\Outlook\archive.pst\Path unknown	Heather Riti </o=City...		08/31/2009 08:41:47.000 -4	08/31/2009 08:42:14.000 -4
Audit 09-12 Weekly Update 2.eml (1)	\\Documents and Settings\vtih-047\Local Settings\Application Data\Microsoft\Outlook\archive.pst\2009 Audits\09-12 LBTR Internal Controls Review	Heather Riti </o=City... Beverly Spa...		08/31/2009 08:41:47.000 -4	11/03/2009 13:53:19.000 -5
Audit 09-12 Weekly Update 3- EXEMPT eml	\\Documents and Settings\vtih-047\Local Settings\Application Data\Microsoft\Outlook\archive.pst\Path unknown	Heather Riti </o=City...		09/08/2009 11:08:43.000 -4	09/08/2009 11:09:06.000 -4
Audit 09-12 Weekly Update 3.eml (1)	\\Documents and Settings\vtih-047\Local Settings\Application Data\Microsoft\Outlook\archive.pst\2009 Audits\09-12 LBTR Internal Controls Review	Heather Riti </o=City... Gretchen Sc...		09/08/2009 11:08:43.000 -4	11/03/2009 13:51:49.000 -5

From: Heather Riti </o=City of Sarasota/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=rith-047>
To: Beverly Spangler </o=City of Sarasota/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=spanglerb-033>, Gretchen Schneider </o=City of Sarasota/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=...>
Date: 31 Aug 2009 12:41:47 -0000
Subject: Audit 09-12 Weekly Update 2
Attachment: [1.3a 09-12 Weekly Status Update2.pdf](#)

Hi Ladies,

Attached is the weekly update for the week August 24-28th.

As always, please let me know if there are any questions.

Heather Riti

Senior Internal Auditor

City Auditor and Clerk's Office

City of Sarasota, Florida

(941) 954-4135

Internal ext. 4239

Name	Path	Sender	Recipients	Created	Modified
Audit 09-12 Weekly Update 2- EXEMPT eml	\\Documents and Settings\vtih-047\Local Settings\Application Data\Microsoft\Outlook\archive.pst\Path unknown	Heather Riti </o=City...		08/31/2009 08:41:47.000 -4	08/31/2009 08:42:14.000 -4
Audit 09-12 Weekly Update 2.eml (1)	\\Documents and Settings\vtih-047\Local Settings\Application Data\Microsoft\Outlook\archive.pst\2009 Audits\09-12 LBTR Internal Controls Review	Heather Riti </o=City... Beverly Spa...		08/31/2009 08:41:47.000 -4	11/03/2009 13:53:19.000 -5
Audit 09-12 Weekly Update 3- EXEMPT eml	\\Documents and Settings\vtih-047\Local Settings\Application Data\Microsoft\Outlook\archive.pst\Path unknown	Heather Riti </o=City...		09/08/2009 11:08:43.000 -4	09/08/2009 11:09:06.000 -4
Audit 09-12 Weekly Update 3.eml (1)	\\Documents and Settings\vtih-047\Local Settings\Application Data\Microsoft\Outlook\archive.pst\2009 Audits\09-12 LBTR Internal Controls Review	Heather Riti </o=City... Gretchen Sc...		09/08/2009 11:08:43.000 -4	11/03/2009 13:51:49.000 -5

From: Heather Riti </o=City of Sarasota/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=rith-047>
To: Gretchen Schneider </o=City of Sarasota/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=schneiderg-033>, Beverly Spangler </o=City of Sarasota/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=...>
Date: 8 Sep 2009 15:08:43 -0000
Subject: Audit 09-12 Weekly Update 3
Attachment: [1.4a 09-12 Weekly Status Update3.pdf](#)

Hi Ladies,

Attached is the audit status report for August 31st - September 4th.

Please let me know if you have any questions.

Heather Riti

Senior Internal Auditor

City Auditor and Clerk's Office

City of Sarasota, Florida

(941) 954-4135

Internal ext. 4239

USB Devices Attached to Each Computer

USB Devices Attached to Marlon Brown's Laptop Computer

Description	First Attach	Last Attach
EPSON UD 100 USB Device	09/12/2011 06:00:00 PM	09/12/2011 10:00:22 PM
Novatel Mass Storage USB Device	08/29/2011 10:00:17 AM	08/29/2011 02:00:20 PM
Novatel Mass Storage USB Device	05/11/2011 12:24:42 PM	05/28/2011 06:39:11 PM
UM175AL CD-ROM USB Device	08/26/2009 10:32:43 AM	05/28/2011 06:39:11 PM
UM175AL CD-ROM USB Device	08/26/2009 10:39:23 AM	05/28/2011 06:39:11 PM
Novatel Mass Storage USB Device	05/11/2011 12:13:35 PM	05/28/2011 06:39:10 PM
Sony Storage Media USB Device	05/02/2011 11:56:50 AM	05/11/2011 04:04:37 PM
UFD USB Flash Drive USB Device	08/20/2009 04:33:34 PM	08/20/2009 08:33:37 PM
UFD USB Flash Drive USB Device	11/03/2008 01:21:52 PM	11/03/2008 06:21:58 PM
UFD USB Flash Drive USB Device	10/16/2008 01:46:36 PM	10/31/2008 07:39:29 PM

USB Devices Attached to Robert Bartolotta's Laptop Computer

Description	First Attach	Last Attach
Ativa My 4GB USB Device	09/02/2011 11:40:00 AM	09/04/2011 05:18:07 PM
CBM USB 2.0 USB Device	08/10/2011 10:19:38 AM	08/10/2011 02:19:41 PM
LEXAR JD FIREFLY USB Device	01/13/2010 02:34:51 PM	06/18/2010 02:14:28 PM
HP Officejet Pro L7 USB Device	11/19/2009 08:05:14 PM	11/20/2009 01:05:19 AM

Kingston DataTraveler 2.0 USB Device	11/19/2009 09:14:33 AM	11/19/2009 02:14:37 PM
LEXAR JD FIREFLY USB Device	07/06/2009 07:41:31 AM	07/20/2009 01:57:57 PM
SanDisk Cruzer Mini USB Device	04/10/2009 11:10:36 AM	04/10/2009 03:10:39 PM
NEC USB UF000x USB Device	03/12/2009 11:52:14 AM	03/12/2009 03:53:34 PM
TEAC FD-05PUB USB Device	10/17/2008 12:08:01 PM	10/17/2008 04:08:04 PM
UFD USB Flash Drive USB Device	10/14/2008 01:40:11 PM	10/14/2008 05:40:15 PM

USB Devices Attached to Heather Riti Essa's Laptop Computer

Description	First Attach	Last Attach
PNY USB 2.0 FD USB Device	07/15/2011 09:13:16 AM	10/12/2011 03:37:01 PM
Verbatim STORE N GO USB Device	09/10/2010 08:10:47 PM	10/12/2011 03:27:15 PM
Verbatim STORE N GO USB Device	12/30/2010 04:15:25 PM	10/11/2011 03:01:44 PM
I-Stick2 IntelligentStick USB Device	01/13/2010 08:11:35 PM	10/04/2011 08:21:14 PM
Imation USB Flash Drive USB Device	09/12/2011 08:20:10 AM	09/12/2011 12:20:35 PM
hp USB Flash Drive USB Device	08/29/2011 04:48:24 PM	09/01/2011 07:23:34 PM
hp USB Flash Drive USB Device	07/25/2011 10:13:42 AM	08/23/2011 06:51:24 PM
PNY USB 2.0 FD USB Device	05/05/2011 06:07:03 PM	05/05/2011 06:07:08 PM
Kingston DataTraveler 2.0 USB Device	04/22/2011 08:54:27 PM	04/22/2011 08:54:34 PM
Verbatim STORE N GO USB Device	03/25/2011 01:19:46 PM	03/25/2011 01:19:50 PM
Verbatim STORE N GO USB Device	03/25/2011 01:11:10 PM	03/25/2011 01:11:20 PM

*Only devices used in 2011 are shown for Heather.

Attached Documents

1. Network Diagram
2. Time Line of Events

Recommendations

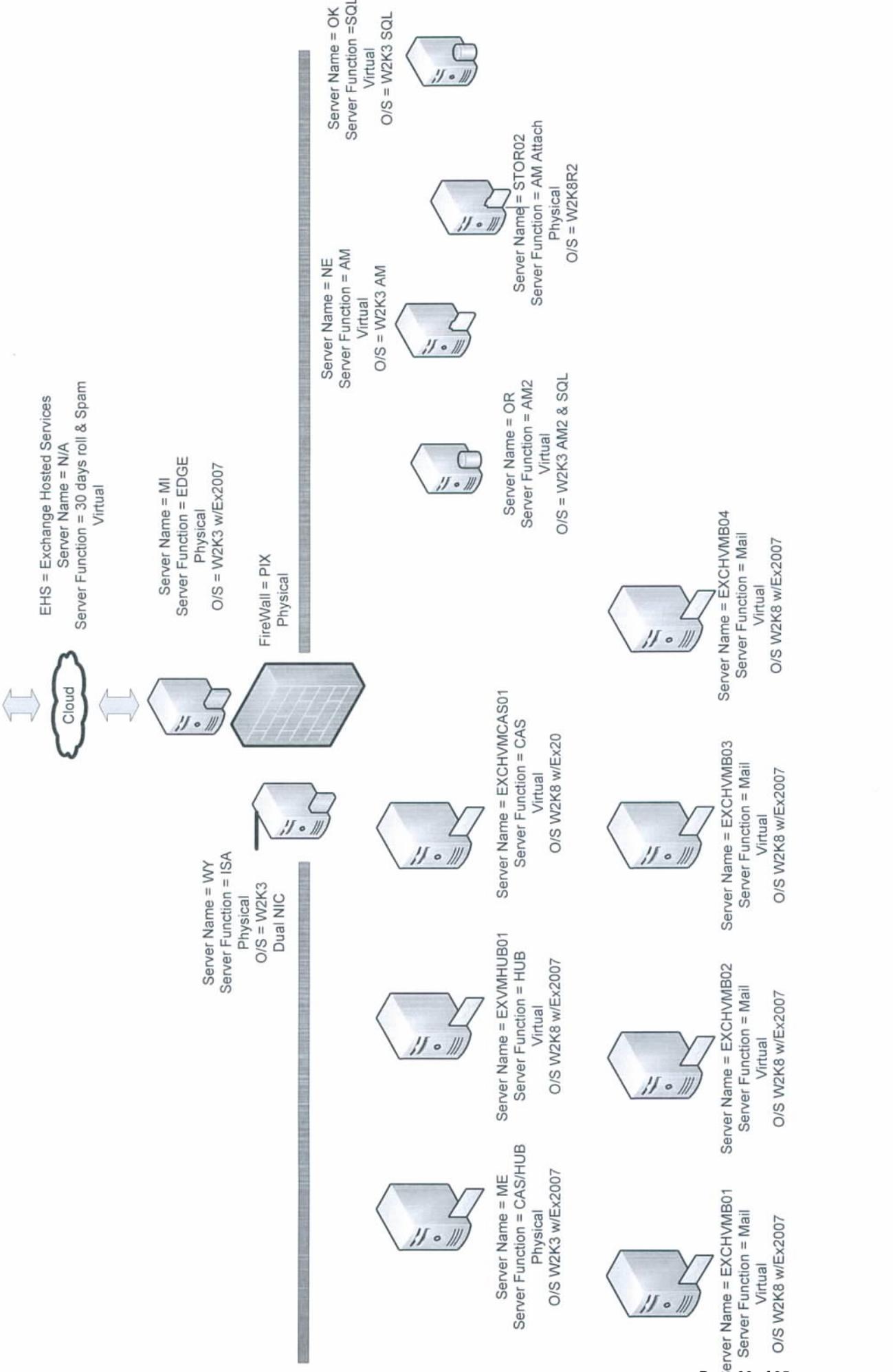
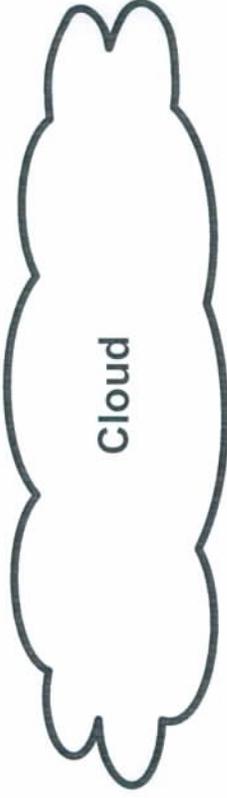
Email Policy

- A. Establish Public Records Request and email search and production Policies and Procedures to avoid potential Computer Fraud and Abuse Act violations caused by the unauthorized searches and potential public disclosure of EXEMPT information to include:
 - a. Personal Identifiable Information
 - b. Personal Health Information
 - c. Ongoing investigation compromise
- B. Establish City of Sarasota email “Use” Policies and Procedures to avoid potential Florida Sunshine Law Violations. The Policies and Procedures should address the following:
 - a. Proper use of the “EXEMPT” email classification.
 - b. Establish Policies and Procedures for fulfilling Public Records Requests that will properly record the request and the fulfillment of the request.
 - c. Ensure that emails are being properly captured and backed up.
 - d. Establish City of Sarasota email access (EXEMPT and non-EXEMPT) Policies and Procedures to include:
 - i. Smart Phones
 - ii. Personal Computers, phones and portable computing devices
 - iii. Remote Access to City of Sarasota emails
 - iv. iPads or other portable devices
 - v. Use of storage media to store City of Sarasota emails
- C. Resolve continuing operational problems with the City of Sarasota email system to prevent Florida Sunshine Law violations, Public Records Request Violations or other potential legal issues.
- D. Continue to resolve City of Sarasota enterprise system logging and documentation problems for purposes of data movement tracking and Cyber Security Incident Response or Breach capabilities.
- E. Resolve City of Sarasota IT Department Policies and Procedures weaknesses and deficiencies for Operating Systems maintenance.
- F. Use of personal computers and smart phones for City Business should be restricted if not entirely eliminated. Guidance and Policies and Procedures are required for the use of both City of Sarasota assets and the use of personal assets such as: smart phones, computers,

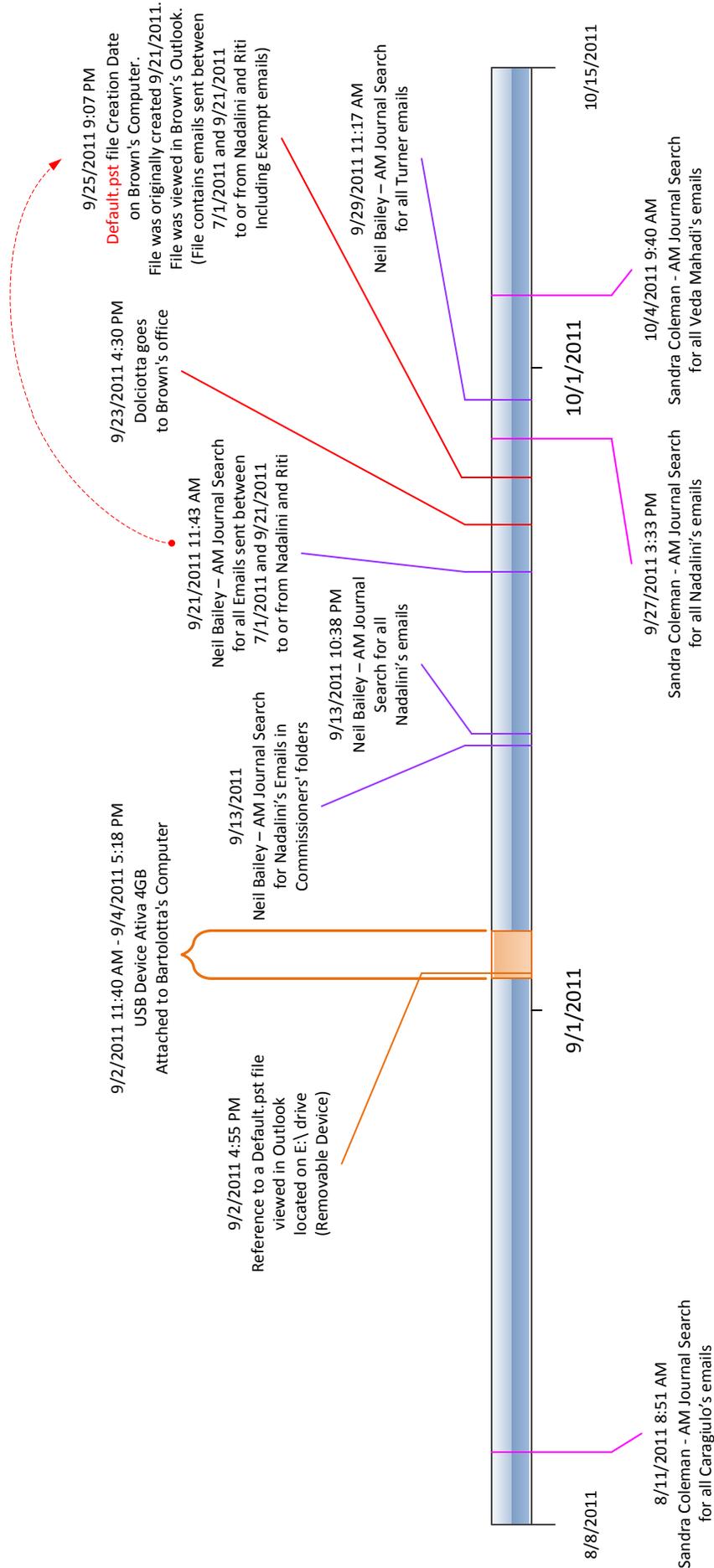
tablets, data memory storage devices, etc. and the use of Remote Access to the City of Sarasota network and data repositories.

- G. Establish IT Policies and Procedures for handling and tracking City of Sarasota sensitive, confidential or EXEMPT information.
- H. Conduct a Cyber Security audit of the City of Sarasota Enterprise Network to determine if security breaches have occurred or if the City of Sarasota enterprise network has been used in an unauthorized manor beyond the scope of this report.

City of Sarasota Network Diagram



EventTime Line



DRAFT - CONFIDENTIAL