Results from the Deployment of A Targeted Security Testing Framework for the Testing of Email Systems in Local Government in Western Australia

Sunsern Limwiriyakul and Craig Valli

***Abstract*—This paper investigated Information Technology (IT) security on the email systems at three selected Western Australian (WA) local government councils. The study's testing and analysis was used and based on several industries and national benchmarking standards for investigated the email system security at all three selected councils. The scope of the analysis included the email threats, architecture, the infrastructure devices, port scanning and vulnerabilities on the email server, email spoofing and email vendor auditing. There were some common problems in all three selected councils that maybe applied in other contexts. In addition, the study aims to provide an email security framework which can be easily adopted and is flexible enough for use in any city councils or other organizations.**

***Index Terms*—Email System, Implementation Framework, IT security.**

I. Introduction

Electronic mail (email) is a common and widely used Internet related technology throughout individuals, industry and government organizations such as WA's local government councils. Other Internet related technologies that are being used in these councils, are Voice over Internet Protocol (VoIP), Geographic Information System (GIS), Global Position System (GPS) and online services systems. These technologies are used to provide both data and voice services to the councils, communities and their residents. Specialist online services such as web information, library, Customer Relationship Management (CRM) and payment systems are also being provided by the WA's councils to its residents and the public.

A major concern of all the selected WA's councils in the provision of these Internet services is the Information and Communications Technology (ICT) security system. The ICT security imperative includes both confidentiality and privacy of users' information over the Internet especially in relation to the online payments, online library and email systems.

This paper aims to investigate the IT security of the email system which is currently deployed at the selected WA councils, in order to investigate whether the system has been implemented securely in a way that meets national and international security standards. A proposed email security framework was deployed in incorporated with several security auditing tools, standards for the testing and analysis purposes.

Three WA local government councils were selected based on their willingness to provide sufficient and relevant data for testing and analysis. Reciprocally, this study provided feedback and security enhancement recommendations to the selected councils. The tests were collected on a real-time basis for all three selected councils. In addition, the testing analysis and implementation framework, results findings and discussions were also included as report submissions to the individual councils for which the study was undertaken.

Manuscript received June 25, 2011.

The authors are with Security Research Centre, Edith Cowan University Perth, Western Australia.

II. Methodology

This section is divided into two subsections which are email vulnerabilities and implementation framework.

A. Email vulnerabilities

The majority of email users are unaware of and resistant to the use of email encryption or security tools to secure their email messages [1]. This can leave email vulnerable to preventable malicious attacks. There are also some common threats and attack techniques associated with the email system which are frequently used by intruders as summarized in Table 1.

TABLE I: Common attack techniques to the email system

Attacking techniques	Description of the techniques
Email bomber	Massive emails generated which can be the same or different messages from an individual sender or a group of senders.
Email spamming	Any unwanted advertisements for services or products which were included in an email message.
Email sniffing and spoofing	A way of intercepting email traffic using a network sniffer tool which allows the attacker to capture all the email contents.
Email scam	Fraud or unwanted email that usually claims the prospect of a bargain or something for nothing.
Email phishing	Emails which were created to collect (phish) personal information (identity theft) such as usernames, passwords, credit card and bank account.
Email borne viruses	Emails that have an attached virus, worm or Trojan.
Buffer overflows	By sending a long HELO command or long email names in MAIL or RCPT commands to the target email server can create a buffer overflow and possibly interrupt the email system [2].
DoS	This attack may crash or destabilize the target email server by attempting to open multiple connections to the server (Simple Mail Transfer Protocol (SMTP) flooding).
Third-party mail relay	Or open relay is a target email server which receives email from an unknown sender. Then sending it on to recipient(s) which are not users of the email system [3].

B. Implementation framework

The implementation framework was based on the level of security of the council's email system. There were various testing techniques which were adapted for use as components within this framework. The testing techniques included were Section C of Open Source Security Testing Methodology (OSSTMM) 2.2 [4], the Center for Internet Security (CIS) Benchmark for Exchange 2007 for Windows Server 2003 Version 1.0 [5], Information Systems Security Assessment Framework (ISSAF) version 0.2.1 [6], National Institute of Standards and Technology (NIST) and other related testing information from various sources such as World Wide Web (WWW), journal, books and personal interviews.

The implementation framework for the testing of the security of the email system consisted of five stages, which included (1) network surveying; (2) internetwork infrastructure review; (3) services and system identification, port scanning and vulnerability detection of the email system servers; (4) spoofing testing and vendor security benchmarking; and (5) email system security policy review. See Fig.1 for more details.

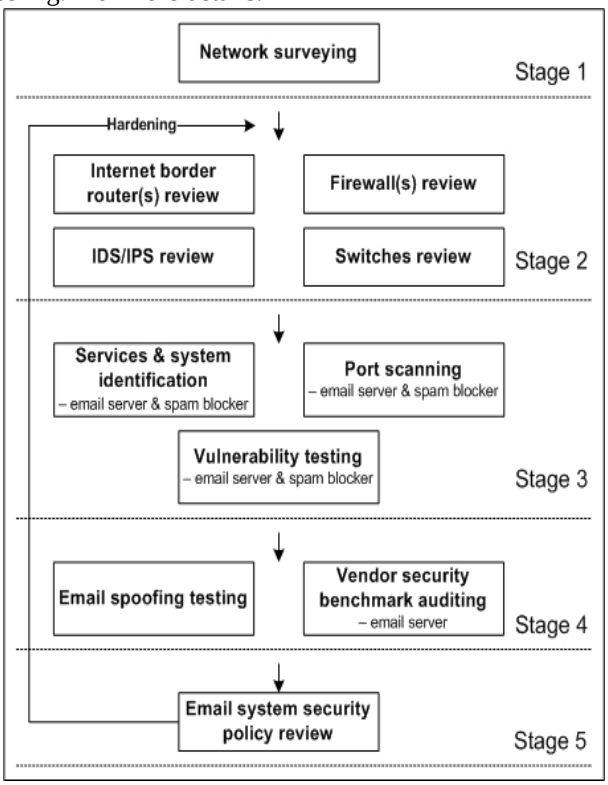

Fig. 1.An implementation framework.

Stage1: The network surveying stage was used to collect information on the council's email system through the use of the following two artifacts:

- Overall network diagram for the internetwork linkages,including the Demilitarized Zone (DMZ) infrastructure connectivity of the email system;and
- Configuration codes and device specifications of all internetworking devices such as the Internet border router, the Internet firewall(s) , the external /DMZ/ internal switch(s),the reverse proxy server and the related email system.

In addition, in this stage the overall email system architecture including its internetwork infrastructure was also reviewed.

Stage 2: The internetwork infrastructure devices review was used to review the related specification and configuration codes as part of the data collection of the internetwork infrastructure devices of the email system of the three selected councils. The internetwork infrastructure devices consisted of the Internet border router, the Intrusion Detection System/Intrusion Prevention System (IDS/IPS), the firewall(s), the DMZ switch(s) and the reverse proxy server (Council C only).

Stage 3: In this stage, both Network Mapper (NMAP) [7] and GFI LANguard [8] network scanning tools were used for scanning the council's email system (email server and in-house spam blocker(s)). NMAP with GUI standard (open source Zenmap version 5.0) for Windows XP version with slow comprehensive scan option, and GFI LANguard version 9.0 with the full scan option, were run for all three testing steps (services and system identification, port scanning and vulnerabilities testing), at all of the three selected councils.

Stage 4: This testing stage involved two steps which included the email spoofing testing and the email vendor security auditing as follows:

- Email spoofing testing which was adapted from the OSSTMM 2.2 email spoofing template as a guideline. The purpose of this testing was to test the email server against any spoofing attacks; and
- Email vendor security auditing which was specifically modified to suit the email application server system of each selected council. However, the CIS Benchmark for Exchange 2007 for Windows Server 2003 version 1.0 (recommended Security Setting for Exchange Controls template) was modified and used at all three selected councils. This was due to the fact that the Microsoft (MS) Exchange 2007 email server platform was being used in all three selected councils.

Stage 5: The email system security policy review; the intention of this stage was to review the IT security policy in relation to the email system which covered the internetwork architecture and its devices, the email server(s), the authorization, the authentication and the accounting of the email system in each of the selected councils.

III. Current Email System Architecture and Email Protocols

A. Council A

Council A's email system has one MS Exchange 2007 email server which was located in the council's internal network and one appliance Symantec Mail Security Suite 5.0 spam blocker server which was located in the council's DMZ network. Typically, MS Exchange 2007 has five server roles which are Edge Transport, Hub Transport, Mailbox, Client Access and Unified Messaging. The council's MS Exchange 2007 email server was configured as a MS Exchange 2007 simple-server architecture which includes only Hub Transport, Mailbox and Client Access server roles.

In addition, the council's spam blocker serves as a MS

Exchange 2007 Edge Transport server. The spam blocker appliance has two network interfaces (A.B.C.y2 and A.B.C.y3). The interface A.B.C.y2 provides sending and receiving email traffics between the outside and the DMZ networks. The interface A.B.C.y3 serves email traffics between the inside and DMZ networks. Having two network interfaces allows the spam blocker appliance to be better in control, performance as well as filter both incoming and outgoing email traffics against threats such as virus, worm, malware, spyware and spam emails.

The internetwork infrastructure consists of a Cisco 2811 Internet border router, one Cisco ASA (5520) firewall and three Cisco Catalyst 3650SM switches. The Intrusion Detection System (IDS) feature on the Internet border router has been disabled. Furthermore, the IPS features on the firewall was also disabled due to past bad experiences in using the IPS. Staff relayed to the researchers that the IPS failed continuously when activated and was difficult to manage given the resources they had. The firewall also performs Network Address Translation (NAT) as well as Port Address Translation (PAT). Each of the three switches provides the internetwork, DMZ and internal network connectivity respectively. See Fig. 2 for more details.

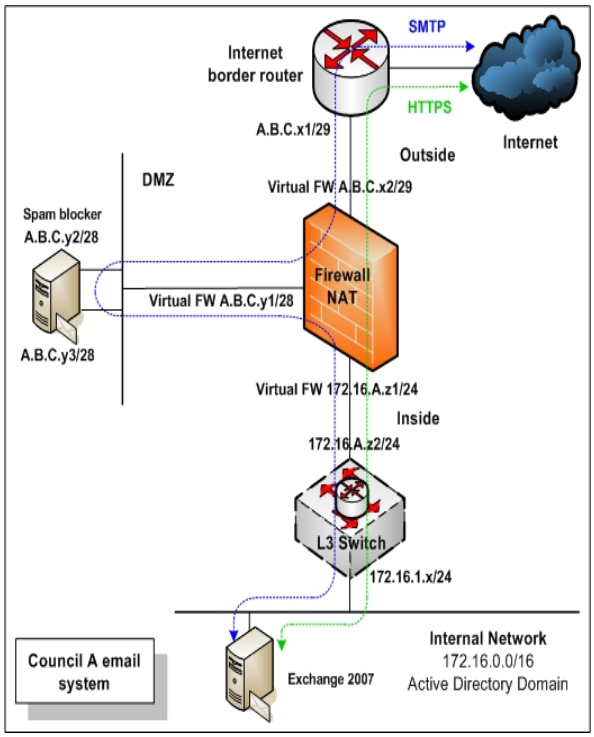

Fig. 2. Council A's current email network diagram.

B. Council B

Council B's email system consists of one MS Exchange 2007 email server, and two Cisco IronPort C150 spam blocker servers. The email server was located in the council's internal network while the two spam blockers were in the DMZ area. Council B's email server was also configured its email application software as a simple-architecture similar to Council A. Additionally, each of the two spam blocker appliances has two network interfaces for splitting between incoming and outgoing email traffics. The two spam blocker appliances run concurrently as part of a redundancy strategy (active and standby modes).

The council's internetwork (DMZ) infrastructure devices consists of one Cisco 2811 Internet border router, two CheckPoint Firewalls 1 (UTM-1 272) and one Cisco Catalyst 3750G switch. Similarly to Council A, Council B's the IDS feature of the Internet border router was disabled. Both the firewalls have no existing IPS feature; however, the firewalls can be upgraded by a paid add-on IPS feature. Both NAT and PAT are also performed at the firewalls. The switch serves all the internetwork, DMZ and internal network connectivity. See Fig. 3 for more details.

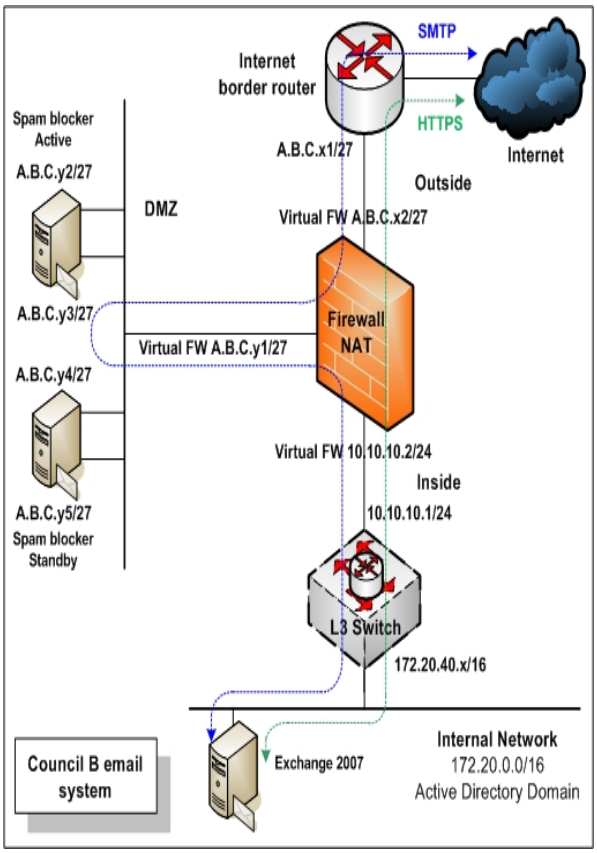

Fig. 3. Council B's current email network diagram.

C. Council C

Council C's email system consists of one MS Exchange 2007 email server and one Internet Security and Acceleration (ISA) 2006 reverse proxy server which are located in the internal network and the DMZ network respectively. Similarly to both Councils A and B, the email application software of Council C's email server is also configured as a simple-architecture. The reverse proxy server is used with the email server for webmail purpose. Both the servers are communicated securely via Transmission Control Protocol (TCP) port 443.

Council C uses an external spam blocker service for scanning unwanted spam email. Incoming cleaned email will pass through Council C's email server whereas outgoing email traffic will forward to the external spam blocker service to inspect and clean any potential spam or virus before forward the cleaned email to the recipients.

There was no Internet border router deployed at internetwork infrastructure of Council C. The infrastructure consisted of two Juniper (SSG-350M) firewalls and one HP (E5412zl) switch. Both the two firewalls act as a main

filtering for all incoming and outgoing network traffics. They also perform NAT and PAT. Both the firewalls are connected and configured as redundancy which one of the firewall operates in active mode and the other operates in a standby mode. In addition, the switch provides connectivity for all the internetwork, the DMZ as well as the internal networks. The switch also acts as an internal central core switch which connects to all the council's access desktop switches. See Fig. 4 for more details.

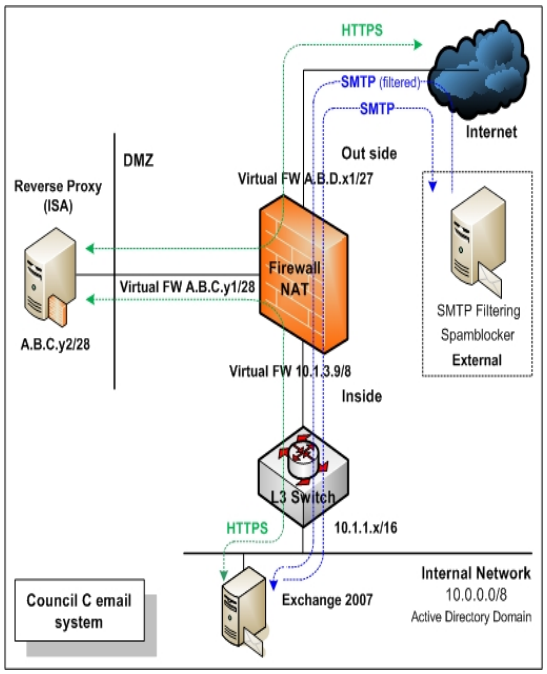

Fig. 4. Council C's current email network diagram.

D. Email protocols

Currently SMTP and Hypertext Transfer Protocol Secure (HTTPS) are used for standard email and webmail respectively at all three selected councils. However, other related email protocols such as Post Office Protocol (POP3) and Internet Message Access Protocol (IMAP) were not used at any of the three selected councils.

The email systems of both Councils A and B are allowed webmail (HTTPS) traffic get through their email infrastructures directly without any inspection to their email servers which are located in their internal networks. Differently, the email system of Council C uses its firewalls to inspect the webmail traffic before forward to its reverse proxy server and the email server respectively.

IV. Data Analysis and Results Finding

Data was collected, analyzed and tested using the five stages of the implementation framework as described in Section 2. The results and findings of all the five stages on each the email systems are displayed in a table format for each stage for simplicity.

Stage 1: Network surveying – The email related technical network documentation was gathered for each of the selected councils. They were found to be only partly updated. The MS Exchange 2007 email server was deployed as part of a single server architecture which was not according to the best practice recommendations for larger organizations [9], [10] at all three selected councils.

Stage 2: Internetwork infrastructure reviews

TABLE II: Internet Border Router Review

Email system infrastructure review: Internet border router			
Descriptions	***CoA***	***CoB***	***CoC***
Internet border router deployed	Yes	Yes	No
Internet border router redundancy/alternative internet link deployed	No	No	No
The router configured against IP spoofing attacks	No	No	NA
Access Control List (ACL) rule to allow ONLY permitted related email protocols for in/out	No	No	NA
Best practice user name and/or password and strong password encryption Message-Digest Algorithm 5 (MD5) used	Yes	No	NA
Allow administration of the router via unsecured communications (HTTP and Telnet)	Yes	Yes	NA

TABLE III: IDS/IPS Review

Email system infrastructure review: IDS/IPS			
Descriptions	***CoA***	***CoB***	***CoC***
IDS feature/device in existence	Yes, on the internet border router	Yes, on the internet border router	No
IDS enabled	No	No	NA
IPS feature/device in existence	Yes, on the firewall	No, but can be added on to the firewall	Yes, on the firewall
IPS enabled	No	NA	Yes
IPS depth inspection on SMTP and HTTPS enabled	NA	NA	Yes

TABLE IV: Firewall Review

Email system infrastructure review: Firewall			
Descriptions	***CoA***	***CoB***	***CoC***
Firewall deployed	Yes	Yes	Yes
Firewall redundancy deployed	Yes	Yes	Yes
Stateful firewall	Yes	Yes	Yes
Firewall configuration rule to allow ONLY permitted related email protocols for in/out	No	No	No
Best practice user name and/or password and strong password encryption (MD5) used	Yes	No	No
Allow administration of the firewall via unsecured communications (HTTP and Telnet)	Yes	Yes	Yes

TABLE V: SWITCHES REVIEW

Email system infrastructure review: Switches			
Descriptions	***CoA***	***CoB***	***CoC***
Standalone external gateway switch deployed	Yes	No	No
Standalone DMZ switch deployed	Yes	No	No
Appropriate Virtual Local Area Network (VLAN) used	Yes	Yes	Partly
ACL applied to block unwanted devices	Yes	No	No
Anti Address Resolution Protocol (ARP) spoofing and poison attacks enabled	No	No	No
Port broadcast-storm control enabled	No	No	No
Port security limits MAC address to a port enabled	No	No	No
Best practice user name and/or password and strong password encryption (MD5) used	Yes	No	No
Allow administration of the firewall via unsecured communications (HTTP and Telnet)	Yes, HTTP only	Yes	Yes

Stage 3:Auditing review of the email servers of the three selected councils (services and system identification, port scanning and vulnerability detection).

TABLE VI: AUDIT REVIEW ON THE COUNCIL'S EMAIL SERVERS

Auditing review on the councils' email servers			
Descriptions	***CoA***	***CoB***	***CoC***
Best practice user name and/or password used on the Operating System (OS)	No	No	No
Best practice used on OS password policy	No	No	No
Unnecessary TCP and User Datagram Protocol (UDP) services ports opened	Yes	Yes	Yes
Missing patches	Yes	Yes	Yes
Missing service packs	Yes	No	Yes

TABLE VII: AUDIT REVIEW ON THE COUNCIL'S SPAM BLOCKER

Auditing review on the councils' spam blockers			
Descriptions	***CoA***	***CoB***	***CoC***
Best practice user name and/or password used	Yes	Yes	NA
Allow administration of the spam blocker via unsecured communications (HTTP and Telnet)	No	No	NA
Unnecessary TCP and UDP services ports opened	No	No	NA

Stage 4: Spoofing testing and vendor security benchmarking.

TABLE VIII: SPOOFING REVIEW

Spoofing review on the councils' email servers			
Descriptions	***CoA***	***CoB***	***CoC***
Using the email server, sending an email from one internal address to another internal address	Yes	Yes	Yes
Using the email server, sending an email from one external address to another external address	No	No	No
Using the email server, sending an email from one internal address to an external address	No	No	No
Using the email server, sending an email from one external address to an internal address	Yes	Yes	Yes

TABLE IX: VENDOR SECURITY BENCHMARKING REVIEW

MS Exchange 2007 benchmark review on the councils' email servers			
Descriptions	***CoA***	***CoB***	***CoC***
Configuration of the council's Mailbox server role as per recommended best practice	Partly	Partly	Partly
Configuration of the council's Hub Transport server role as per recommended best practice	Partly	Partly	Partly
Configuration of the council's Client Access server role as per recommended best practice	Partly	Partly	Partly

Stage 5: Email system security policy review

TABLE X: EMAIL SYSTEMS SECURITY POLICY REVIEW

Email systems security policy review on the selected councils			
Descriptions	***CoA***	***CoB***	***CoC***
General email usages policy in use	Yes	Yes	Yes
General email related (Internet) usages policy in use	Yes	Yes	Yes
Information security policy (email related) to the councils' staff in use	No	No	No
Information security policy – technical to the councils' IT staff in use	No	No	No
Regular update or review the email related policy	No	No	No
Advise general email usages including security awareness to new starter	Yes	Yes	Yes
Frequently advise their staff for IT security information including email related	No	No	No

V. DISCUSSION

As per recommendations to best practice, there were inadequate settings, configurations and implementations of the related email system devices in all five testing stages based on the results presented earlier. These shortcomings are a possible cause of concern for potential risks in the three selected WA council's email systems.

With respect to these inadequacies in the operation of the

related email system devices, there were six main factors uncovered in this study. They include (1) the lack of IT security standards awareness of industrial best practices by staff, (2) inadequate specific knowledge, (3) inefficient communication between the staff, (4) limited IT training for staff as a result of limited budget, (5) staff not having enough time for task completion and (6) reliance on external consultants for specific IT projects.

1) The lack of IT security standards awareness of industrial best practices by staff: There were two audits conducted which included several discussions and meetings for each of the selected councils. For example, there was no standalone DMZ switch deployed at both Councils B and C. In addition, the following lists summarizes the overall common findings which related to the first factor from the three selected councils:
   - There was no Internet border router redundancy/alternative Internet link deployed at all selected councils; and
   - The architectural design of the email servers was not in line with the MS Exchange 2007 recommendations of best practices [9], [10] at all selected councils.

   The can be considered of lacks of knowledge and should be resolved by providing further training to their IT operation staff.
2) Inadequate domain or service specific knowledge: There was evidence of missed and inadequate configuration of the Internet border router's ACL, the DMZ switch's codes, the firewall rules, the unnecessary ports and the services installed on the email servers at all three selected councils. This was due to the fact that the staff were not well versed in these technical areas for the correct implementation. See Tables 1 to 5 for more details.
3) Inefficient communication between the IT staff: It was evident that the firewalls for the email servers were inadequately configured. For example, wrong port numbers were assigned as a result of oral miscommunication between the IT staff at all three selected councils. In addition, the lack of a change management process at all three selected councils also contributed to the potential for inefficient communication between the IT staff.
4) Limited IT training for staff as a result of a limited training budget: There were limited IT training budgets allocated at all three selected councils. Typically, the IT administrator was able to attend only one or less related IT training course per year. This occurred at all three selected councils over the past five years. This training policy may be directly attributed to insufficient knowledge for managing the email system. In addition, all the IT administrators at all selected councils have never attended specific industry or equivalent training in both firewall and MS Exchange 2007 related courses.
5) Insufficient time for task completion by the IT staff: At all three selected councils, the IT staff had several duties and diverse tasks which sometimes resulted in some of the tasks being continuously left incomplete or unattended. Additionally, there was also no time left for proper documentation at all three councils as presented in Stage 1.
6) Reliance on external consultants for specific IT projects: The three selected councils reliance on outsourcing to solve the expertise problem may be a possible disadvantage in terms of a lack of knowledge transfer for the IT staff. This is evidenced by the fact that the firewall systems at all three selected councils were implemented by external consultants. In addition, the email servers (MS Exchange 2007) at all three selected councils were also deployed by external consultants. Consequently, historical records of implementation and maintenance were deficient and not readily available. This point out that there was poor contract management by all the three selected councils.

VI. Conclusions

The results from the testing and analysis of these three selected councils have shown that the implementation framework can be used for auditing as well as testing email infrastructure security particularly in the similar structure, architecture or environment. As previously outlined there were many common points of vulnerability or security issues uncovered as a result of the research. Many of the issues uncovered were not just purely technological in focus. In fact, many of the serious issues revolved around poor process and human factor issues that contributed to a poor security position for example the lack of resources for training and education. This was a major issue and one that all councils can readily address and get a better standard of service with minimal financial outlay.

There were also significant issues with the technical security and as you would expect many of these were easy to fix and gave the councils a stronger security posture with minimal cost. The framework also uncovered some unforeseen issues with configuration and security of the systems tested. As a result of this study, the implementation framework, presented here can be used to audit an email system, particularly in Windows server environment and one deploying MS Exchange 2007.

It is also possible for this framework to be adopted by any councils or organizations with similar architectures and get

discernible outcomes. The adoption of the framework may be used as a guideline in auditing or testing the security of their email system provided that it is in compliance with their existing ICT policies. Furthermore, the framework may also be used as a basis for documentation of their email system.

REFERENCES

[1] A. Fadia, The unofficial guide to ethical hacking, 2nd ed. USA: Thomson Course Technology, 2006.

[2] A. Basta and W. Halton, Computer security and penetration testing 1st ed. Boston: Thompson, 2008.

[3] J. Stewart, "Third-party mail relay (open relay) and Microsoft Exchange Server," vol. 2008: SANS Institute 2003.

[4] P.Herzog, "OSSTMM 2.2 Open-Source Security Testing Methodology Manual," 2006, http://isecom.securenetltd.com/osstmm.en.2.2.pdf.

[5] CIS, "Center for Internet Security Benchmark for Exchange 2007 for Windows Server 2003 Version 1.0," 2007, http://www.cisecurity.org/tools2/exchange/CIS_Benchmark_Exchange2007_1.0.pdf.

[6] B. Rathore, O. Herrera, S. Raman, M. Brunner, P. Brunati, U. Chavan, M. Dilaj, and R. Subramaniam, "Information Systems Security Assessment Framework (ISSAF) draft 0.2.1 Information System Security Groups,"2006. http://www.oissg.org/downloads/issaf-0.2/index.php.

[7] G.Lyon,"Nmap Security Scanner," 2008, http://nmap.org/download.html.

[8] GFI, "Network vulnerability scanner, security scanner and port scanner," 2009, http://www.gfi.com/lannetscan/.

[9] Microsoft Exchange Documentation Team, "Exchange Server 2007 Planning," 2007, http://www.microsoft.com/downloads/details.aspx?FamilyID=1A6EFDD6-D80E-489D-9A1D-8F3E01BAA3C5&displaylang =en&displaylang=en.

[10] Microsoft TechNet, "Exchange Server 2007 Design and Architecture at Microsoft," 2007, http://www.microsoft.com/downloads/details.aspx?FamilyID=98C522BC-814A-421A-99C0-D964ED119C0D&displaylang=en&displaylang=en.

Professor Craig Valli Craig is currently the Head of School and a Professor (Digital Forensics) within the School of Computer and Security Science at Edith Cowan University (ECU). He is also the Director of the secau - Security Research Centre within ECU.

He has over 20 years experience in the IT Industry and consults to industry and government on network security and digital forensics issues. Craig main research and consultancy focus is on securing networks and critical infrastructures, detection of network borne threats and forensic analysis of cyber security incidents.

Sunsern Limwiriyakul has been working in the IT industry for several years in the areas of information technology and communication network. He is currently undertaking his doctorate research at Edith Cowan University, Perth, Western Australia in the field of network security. His research interests are in Internet and network security.