KEMI-TORNIO UNIVERSITY OF APPLIED SCIENCES

Testing Mail Server Vulnerabilities and Recommending Control Measures -
A Case of Interglobal Limited

Ademowo, Adewale Adebayo

Bachelor's thesis of the Degree Programme in Business Information Technology

Bachelor of Business Administration

TORNIO 2010

ABSTRACT

Ademowo, Adewale Adebayo 2010. Testing Mail Server Vulnerabilities and Recommending Control Measures – A Case of Interglobal Limited. Bachelor's Thesis. Kemi-Tornio University of Applied Sciences. The Unit of Business and Culture. Pages 60.

The case company in this Thesis is Interglobal Limited located in Nigeria. The aim of this study is to test for mail server vulnerabilities and recommend control measures in dealing with the identified vulnerabilities.

In this thesis, I have x-ray basis of information security; relationships among threat, attacks, and vulnerabilities; threat and security concerns on mail servers and clients; mail server overview and common vulnerability challenges; and vulnerability issues with Interglobal Limited mail servers.

This research has led me to conduct vulnerability scanning of Interglobal Limited mail server through an email client configured on the server. The results of the tests and overview of research objectives have influenced my recommendations on control measures to deal with the found vulnerability and unexpected vulnerabilities in the future.

Communication is one of the key strengths of an organisation. It is imperative for businesses to have email communication for passing across information to the clients and vice versa. The security of mail communication backbone should be of greater importance and concern to individuals and corporate organisations.

Keywords: Information Security, Vulnerability, Mail Server, Mail security, Control Measures, Vulnerability Scanning, Interglobal Limited.

CONTENTS

FIGURES

TABLES

EXPLANATION OF CHARACTERS AND ABBREVATIONS

DLP	Desktop Level Protection
ESMTP	Extended SMTP
EXE	Executable Files
HTA	HTML Application
HTTPS	Hypertext Transfer Protocol Secure
IMAP	Internet Message Access Protocol
IS	Information Security / Information System
ISS	Information System Security
MTA	Mail Transport Agent
IT	Information Technology
JS	JavaScript
OS	Operating System
PIN	Personal Identification Number
POP	Post Office Protocol
POP3	Post Office Protocol version 3
SLP	Server Level Protection
SMTP	Simple Mail Transfer Protocol
SSL	Secure Socket Layer
VBS	VBScript File (Visual Basic Script)
VM	Vulnerability Management
WSUS	Windows Server Update Service

1 INTRODUCTION

In the ever-changing world of global data communications, inexpensive Internet connections, and fast-paced software development, security is becoming more and more of an issue. Security is now a basic requirement because global computing is inherently insecure. As the data goes from point A to point B on the Internet, for example, it may pass through several other points along the way, giving other users the opportunity to intercept, and even alter, your data. Even other users on your system may maliciously transform your data into something you did not intend. Unauthorized access to your system may be obtained by intruders, also known as “crackers”, who then use advanced knowledge to impersonate you, steal information from you, or even deny you access to your own resources (Fenzi & Wreski 1998). These emphases indicate the more reasons why there is need for security in information systems.

1.1 Motivation

The topic of my research work is Testing Mail Server Vulnerabilities and Recommending Control Measures - A Case of Interglobal Limited. The choice of my topic is informed by my thirst for information system (henceforth IS) security, which embodies server security. My research work is based on examining known vulnerability issues with the case company’s mail server and their effects; control measures previously applied to deal with the vulnerabilities and their effects; vulnerability testing, and recommendations on how vulnerability testing can be used to mitigate risks pose by vulnerable server environment in the company.

This work also includes analysis of relationship among three key issues that affect efficiency and reliability of the server and information systems performance and security. The three key issues that affect information system security and pose challenges to information confidentiality, information integrity, and information availability are threat, attack, and vulnerability. Threat and attack are accomplices of vulnerability. Therefore, threat and attack succeed because vulnerable systems exist. To be successful in combating vulnerabilities in any system, these three keys must be studied and understood by a server or network administrator in an organisation. Otherwise, efforts to deal with vulnerable system in the organisation may be fruitless.

My research work will be essential to ensuring information security such as data confidentiality, data integrity, and data availability in respect of mail server environment. Additionally, it will also perform four important functions for an organization. The functions are to protect the organisation's ability to function, enable the safe operation of applications implemented on IT systems, protect the organisation's data, and safeguard the technology assets in use (Whitman & Mattord 2005, 37).

1.2 General Goals

For most businesses today, e-mail is the mission-critical communications tool that allows their people to produce the best results. This greater reliance on e-mail has increased the number of messages sent and received, the variety of work getting done, and even the speed of business itself. Amid this change, employee expectations have also evolved. Today, employees look for rich, efficient access - to e-mail, calendars, attachments, contacts, and more - no matter where they are or what type of device they are using (Microsoft Exchange 2010.)

The most deadly viruses, able to cripple your email system and corporate network in minutes, are being distributed worldwide via email in a matter of hours. Email worms and viruses can reach your system and infect your users through harmful attachments. But that's not all! Some viruses are transmitted through harmless-looking email messages and can run automatically without the need for user intervention (GFI 2010.)

There is need to initiate an efficient and effective way of detecting and controlling vulnerabilities to reduce flaws in a server. This is an in-house approach that is centered on the processes, systems, and strategies required to defend against both internal and external intruders and attackers to the systems. This approach is an indirect means of managing risks due to such flaws. Servers are prone to threats, attacks, and intrusion because there are security holes somewhere in the systems, processes and strategies in place.

The need to ensure secure servers that will enhance business operations, the users' experience, and drastically reduce impacts of attacks and intrusions, is of importance. Therefore, my work will look into the analysis of Interglobal Limited mail server environment which will reflect on type of server available, previous and present challenges on their mail server, and existing security tools employed in dealing with vulnerabilities.

My work will help Interglobal Limited by means of testing and offering recommendations on its mail server vulnerabilities; vulnerability detection and control strategies.

1.3 Research Problems

My research work is Testing Mail Server Vulnerabilities and Recommending Control Measures – A Case of Interglobal Limited. Vulnerability testing is the practice of identifying, detecting, and classifying vulnerabilities in a system (Foreman 2009).

An overview of mail server and its security, analysis of Interglobal Limited server environment, and the main concepts of vulnerability testing and control strategies in Interglobal Limited mail server are treated before focusing on the research questions described below:

(i) What are known vulnerability issues with the company’s mail server and their effects?

This question identifies, itemizes, and reviews known and common vulnerabilities on the company’s mail server. The question looks into the sources of the identified vulnerabilities and also examines impacts of the identified vulnerabilities on the mail server and clients.

(ii) What control measures previously applied to deal with the vulnerabilities and their effects?

This question examines if the company has previously applied any control measures to deal with vulnerabilities in its mail server and what are effects of the control measures. The question also looks at control measures to deal with vulnerability issues in the company’s mail server. It also discusses how security scanning is important and what tools are available to identify, classify, and assess vulnerabilities on mail server environment.

(iii) How can vulnerability testing be used to mitigate risks pose by vulnerable server environment in the company?

The aim of vulnerability test is to detect vulnerabilities and reduce its impacts on information systems to the barest minimum. Therefore, the question explains what vulnerability tests to conduct, analysis of test results, and recommendations on how to take advantage of the results in ensuring the company's data confidentiality, data integrity, and data availability.

1.4 Research Methodology

Research Methodology is a way to systematically solve research problems (Kumar 2008). It is the system of collecting, organising, evaluating, and analysing data for research projects. My research method is a case study. Case study is an in-depth investigation on a specific social unit that gives perfect and well-structured picture of the object (Ryabov 2010). Case study research excels at bringing us to an understanding of a complex issue or object and can extend experience or add strength to what is already known through previous research (Soy 2006).

Since my research work is a case study, I have applied the phases that center on determining the objective of the research, writing a research plan, gathering the data required, organising the received or gathered data, and finally reporting the result (Ryabov 2010).

During data gathering, I have also applied vulnerability testing for vulnerability detection and assessment. This informs the company of the need to perform periodic vulnerability testing of its mail server for possible vulnerabilities and enables the company to be proactive about how to control vulnerabilities in its mail server. In the analysis phase, the data gathered is organized, evaluated, and analysed at this stage. While at the reporting, my research output or result is presented in writing or reported form.

My research work covers the basis of IS security, overview of Interglobal Limited’s mail server environment, vulnerability issues with Interglobal mail server, vulnerability testing, and identified control measures. Analysis of Interglobal mail server environment which reflect on type of server and mail client applicable, previous and present challenges on its mail server, and security tools employed in dealing with vulnerabilities are also considered.

In achieving my aims in this research work, the sources of information for data collection and gathering applied are library; the Internet; an interview with company’s system/server administrator; and vulnerability testing, result of which is valuable in recommending control measures in tandem with previous vulnerabilities experienced at Interglobal Limited.

1.5 Output of the Research

My research work will be based on the following outputs:

- Identifying vulnerabilities in the company’s mail server.
- Finding the effects of vulnerabilities on the company’s mail server.
- Recommending control measures against vulnerabilities in the server.

My research results will be valuable because the output will be useful for Interglobal Limited and provide information on reduction in the time and money spent dealing with vulnerabilities and exploitation of those vulnerabilities. It will serve as valuable reference for professional, guides for novice, and a tool for IS security environment. My research work will be more relevant for individuals or organisations, which do not know or bother about vulnerability, effects of vulnerability, detection of vulnerability, and vulnerability control measures. The research output will help and guide in ensuring secure mail communications.

1.6 Structure of my Thesis

My thesis comprises of seven chapters as briefly described below:

Chapter 1 of my thesis is the introductory chapter and has just been covered above. Chapter 2 of my thesis reflects on the background information of Interglobal Limited, which is my case company. While the chapter 3 reflects on basis of information security, relationships among threat, attacks, and vulnerabilities; threat and security concerns on mail servers and clients. Since the core of my thesis is based on mail server, I have used chapter 4 to discuss mail server overview, Interglobal mail server, mail server and client vulnerabilities, and vulnerability issues as identified by Interglobal Limited. Vulnerability testing, test results and analyses are covered in chapter 5. Chapter 6 explains control measures and recommendations for Interglobal Limited. I have concluded the whole scenario with advice, submissions, and further recommendations in chapter 7.

2 BACKGROUND INFORMATION OF INTERGLOBAL LIMITED

Interglobal Limited is my chosen case company. Interglobal Limited is located in Nigeria and was incorporated in 1992 as a limited liability company that will offer leading-edge information and communication technology products and services. The ethos of INTERGLOBAL is to deliver the optimum service and support which exceeds the expectations of its clients, help its customers enhance productivity, increase business agility, and improve customer loyalty, thereby maximizing its revenue.

Interglobal Limited with 75 staff members has three offices in different states of Nigeria but its head office is located in Abuja Nigeria. The remaining two offices are located in Lagos and Port Harcourt in South-West and South-South regions of Nigeria respectively.

Interglobal Limited has provided a wide range of customers its unique services to enable them address a wide range of systems solutions. Some of these include: Petroleum Technology Development Fund, National Bureau of Statistics – Abuja; Bureau for Public Service Reforms (BPSR) – Abuja; Central Bank of Nigeria – Abuja; Southern Gas Constructors Limited; Hewlett Packard (HP) Nigeria Limited, Lagos; NIGERIAN EXPORT-IMPORT BANK LIMITED (NEXIM), Abuja; United Bank for Africa PLC (UBA), Lagos; Hewlett Packard (HP) Nigeria Limited, Lagos; Bureau of Public Enterprises (BPE), Abuja; Union Bank PLC, Marina, Lagos; Nigeria Export-Import Bank (NEXIM) Ltd, Abuja; Society for Family Health; Intercellular Limited; Nigerian National Petroleum Corporation (NNPC), Abuja; Nigeria – Sao Tome & Principe Joint Development Authority, Abuja; Central Bank of Nigeria – Abuja; United Bank for Africa PLC (UBA), Lagos; Nigeria Communications Commission (NCC), Abuja; Bank of Industry (BOI), Lagos

Organisation Charts of Interglobal Limited

Figure 1 below depicts the organisational chart of Interglobal Limited's management staff and non-management staff.

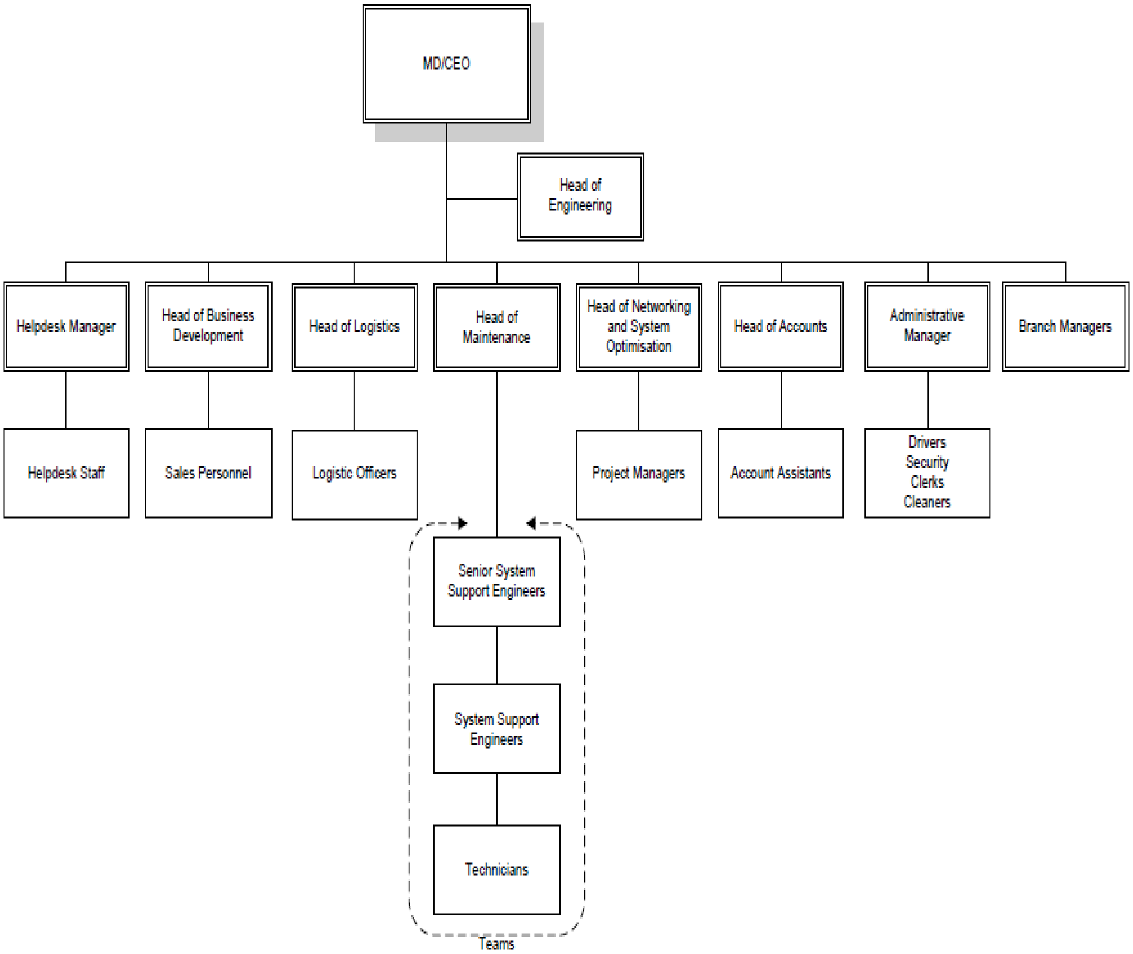


Figure 1: Interglobal Limited - Organisation Charts

Figure 2 below depicts the organisational chart of the proposed Interglobal project chart.

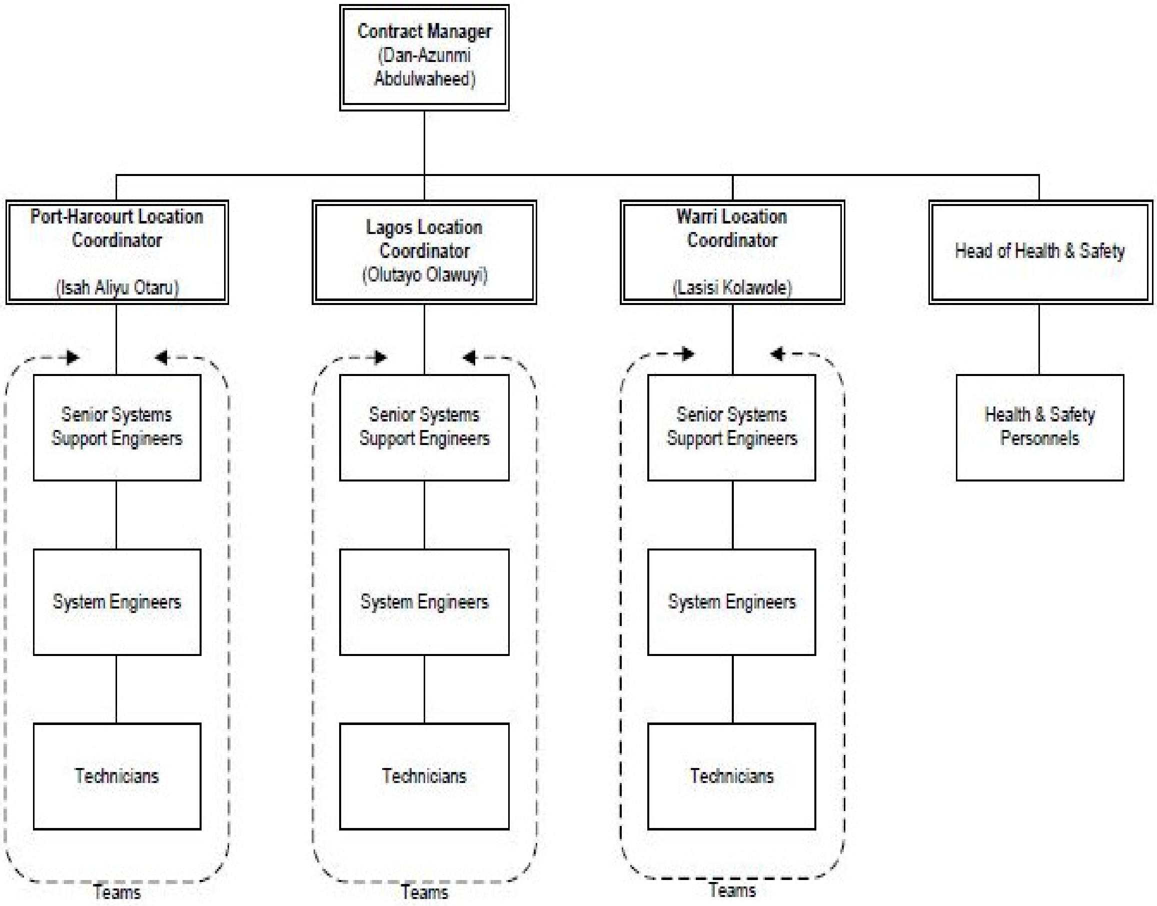


Figure 2: Interglobal Limited - Proposed Project Organisation Charts

3 INFORMATION SECURITY

3.1 Basis of Information Security

The tenets of information security are the goals of ensuring confidentiality, integrity, and availability of information and information system. Confidentiality refers to preventing intentional or unintentional disclosure of communications between a sender and recipient. Integrity ensures the accuracy and consistency of information during all processing stages which are storage, transmission, and deletion. Availability ensures those who are authorized to access resources can do so in a reliable and timely manner (Weaver 2007, 26.) In short, information security is the preservation of confidentiality, integrity, and availability of information.

The tenets of information technology are often represented as a triangle called The CIA Triad, as shown in Figure 3 below (Kinamik 2007, 5.)

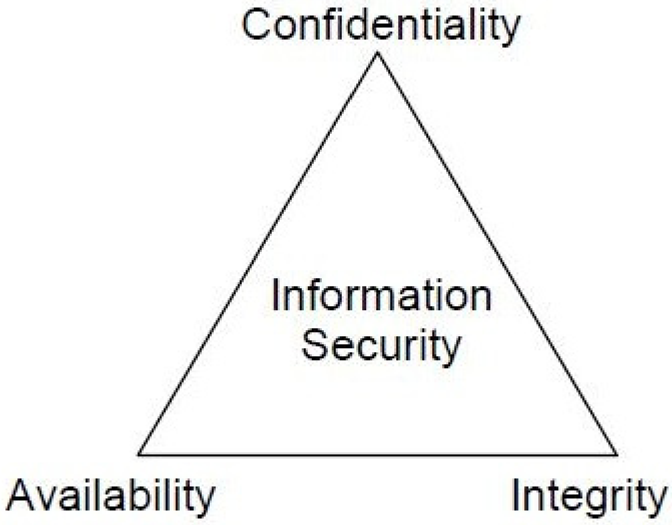


Figure 3: The CIA Triad (Kinamik 2007, 5)

The CIA triad in Figure 3 above is a well known concept in Information Security. The closer one moves towards one apex, the further one is removed from the other two. The idea here is to make the trade off a sensible one, based on the value and sensitivity of the information you are responsible for, and ultimately to end up in the middle of the CIA triad, with the best trade-off of each property for the value of the data you are protecting (Kinamik, 2007, 5.)

The CIA triad is simple but widely-applicable security model that encompasses three key tenets of information security which are confidentiality, integrity, and availability. These three key tenets should be guaranteed in any kind of secure system. The CIA triad is applicable across the whole subject of information security issues and analyses; from access to a user's internet history, user's internet experience to security of encrypted data across the internet. Breaching anyone of these tenets of information security, results in serious consequences for the parties or systems involved (Weaver 2007, 26.)

3.2 Relationship among Threat, Attack, and Vulnerability

The fact that my research work is about mail server vulnerability does not warrant me to limit my scope to vulnerability alone because vulnerable systems exist due to emergence of threats and attacks. Threat, attack, and vulnerability as they affect IS security in a secured environment and their relationship are important concepts to be reckoned with in dealing with information system security and related challenges. Threat, attack, and vulnerability are three key issues that must be clearly understood in order to ensure data confidentiality, data integrity, and data availability; network functionality and integrity; and computer and IT security.

Threat, attack, and vulnerability are three components of risk. Risk is an exposure to loss or possible injury due to unwanted and unwarranted impacts of threats, attacks, and vulnerabilities in information systems (Thywissen 2006, 25). The plans to mitigate these three key components ensure optimum system performance and reduce risks to barest minimum (Business Link 2010).

Threats are activities that represent possible danger to data, loss of privacy, network intrusions, and related consequences. These threats can be unintentional and intentional, targeted or no targeted, and can come from a variety of sources, such as information warfare, criminals, hackers, virus writers, and disgruntled employees and contractors working within an organization (Al-Zubi 2010). More so, last among the sources of threats is a social engineering, which involves using politeness and gullibility to gain access to secure resources through deceit (Weaver 2007, 20).

An attack is an attempt to bypass security controls on a computer. Threats from attacks fall into four categories; namely Denial of Service (DoS) which renders a service inoperative, spoofing which occurs when someone under pretense impersonates an authorized user to steal information, man-in-the-middle which means someone in a network environment pretends as the server and client to capture communications between two computers, and password guessing which involves guessing a username and password in an attempt to gain access to a network or system (Sophos 2006.)

Furthermore, malicious code otherwise known as malware is a software or firmware intentionally placed in a system for an unauthorized purpose. It is also a threat to information security, and it comes in various forms, which among various are virus, worm, and Trojan horse. A virus is a program that replicates but does not propagate itself. A worm is also a program that replicates and at the same time propagates itself, while Trojan horse looks desirable or harmless but actually does damage to data integrity and system functionality. Other types of malware in existence are spyware, adware, wabbits, backdoors, exploits, root kits, key loggers, dialers, and URL injectors (Sophos 2006.)

Vulnerability is a weakness or pothole in a system that could be exploited by threats (MS-ISAC 2010). Vulnerabilities are mainly the intrusion points where information can be accessed without authorization or adequate permission. These could be places in the network infrastructure that can be accessed internally or externally; applications that interoperate with other applications remotely especially on the Internet, such as a Web browser or mail application; and communications protocols that are used for communications across the Internet.

External access points connect any organisation’s systems and network to the Internet or provide access to the organisation’s information from external locations. For instance, if an organisation has a web or mail server accessed from the Internet, it is an external access point. Meanwhile, internal access points provide access to the organisation’s information from internal sources. For instance, a server on the network that does not require a username or password to access information is considered an internal access point.

Other major concerns are the people behind these nefarious activities, who are referred to as hackers. They can exist as hackers or crackers. A hacker may be someone who writes codes to provide a quick solution to a difficult problem, or someone, otherwise known as cracker, who breaks security controls in an information system. Nonetheless, we need to always be aware of them, as they can pose serious security risks to information systems (Weaver, 2007, 17.)

Disgruntled employees who are usually unhappy over perceived injustices meted on them and want to exact revenge by stealing information. Often they give confidential information to new employers. When an employment contract is terminated, security measures should be taken immediately to ensure that the employee can no longer access the company network (Weaver, 2007, 17.)

Sometimes the most serious vulnerabilities facing a company are those internally motivated not externally motivated. For instance, in November 2002, the FBI broke up the largest identity theft ring in U.S. history. A help desk worker at a computer software company allegedly agreed to give passwords and access codes for consumer credit reports to another person, who was able to make unauthorised purchases using the stolen information (Weaver, 2007, 17 – 18.) This further proves that consideration for internal forces is very important in determining the security of information systems.

3.3 Threats and Security Concerns

Threats and security concerns in respect of mail server security are rooted in confidentiality, integrity, and availability. Threats are factors that pose greater challenges to data security. Threat is the practice of misleading and misdirecting a person or an organisation in such a way as to get information or has access to restricted or confidential data in a fraudulent and deceitful way; these can result in incorrect decisions being made and cause failures in hardware devices or networks infrastructure (Department of Commerce 2007).

Threats involving the willful destruction or manipulation of data, information, software or hardware. Potential sources include disgruntled employees or contractors, hackers, maintenance people, activists, customers, suppliers, extortionists, criminals, or terrorists. Deliberate threats can result in consequences including financial loss; loss of public confidence, image, creditability and/or reputation; incorrect or poor decisions being made and/or taking a long time; legal liabilities and breakdown of duty of care; injury or loss of life; inconvenience to the public; breach of service level agreements; breach of statutory or regulatory duty; inability to perform critical or statutory tasks (Department of Commerce 2007.)

Table 1, Table 2, and Table 3 below were adopted from 2007 Government Chief Information Office Guidelines of New South Wales (Australia) Department of Commerce and analyses common threats to security concerns in any organisation; their descriptions and examples of vulnerabilities resulted; and the areas of security concern affected. In the tables “C” stands for Confidentiality, “I” stands for Integrity, and “A” stands for Availability under security concerns.

Table 1 Threat and Security Concerns – I (Department of Commerce 2007)

THREAT	Descriptions and Examples of Vulnerabilities	Security Concern		
		C	I	A
Denial of Service	Disrupts or completely denies service to legitimate users, networks, systems and resources. **Vulnerabilities:** Lack of a firewall. Inadequate network management. Not using the latest version of the operating system can lead to exploitation of the security weakness.			✓
Eavesdropping	Attacker uses software to "listen" to all traffic passing across an internal or external network. **Vulnerabilities:** Unencrypted communications. Lack of physical security over data communications closets or hubs. Use of shared networks that results in traffic being broadcast to any machine on a local segment.	✓		
Fire	**Vulnerabilities:** Lack of physical security. Lack of fire detection devices. Lack of automatic fire suppression system. Availability of flammable materials such as paper or boxes.			✓
Malicious Code	Malicious code refers to viruses, worms, Trojan horses and other undesirable software. **Vulnerabilities:** No anti-virus software. Lack of regular updates of anti-virus software. Inadequate education of staff on software viruses. Uncontrolled downloading and use of software off the Internet. Lack of policy for opening e-mail attachments.	✓	✓	✓
Malicious destruction of data, information or facilities	Anybody with sufficient knowledge and access can render a system unusable if they know what they are doing. **Vulnerabilities:** Lack of physical security. Lack of logical access security (user ID and password) leading to deletion of data. Lack of communication regarding terminated employees leading to terminating employees still having access to systems.		✓	✓

Table 2 Threat and Security Concerns – II (Department of Commerce 2007)

THREAT	Description and Examples of Vulnerabilities	Security Concern		
		C	I	A
Masquerading	A user or computer that has been deceived as to the identity of the person they are communicating with can be induced to disclose sensitive information. **Vulnerabilities:** Lack of identification and authentication mechanisms. Unprotected password tables. Lack of identification of sender and receiver.	✓	✓	
Repudiation	When conducting business over a network or the Internet, both parties must agree that a particular transaction took place. Proper safeguards are needed to ensure integrity and validity of all transactions. **Vulnerabilities:** Lack of proof of sending or receiving a message. Lack of use of digital signatures.			
Sabotage	Insiders have knowledge that provides them with the capability to cause maximum disruption to an agency by sabotaging information systems. **Vulnerabilities:** lack of physical security. Lack of logical access controls. Lack of change management controls. Incorrect access rights.		✓	✓
Social Engineering	It is the practice of misleading and misdirecting a person in such a way as to attain information through social interaction. **Vulnerabilities:** Lack of awareness of the social engineering threat.	✓	✓	✓
Theft and Fraud	Theft can include loss of data, information, equipment or software. Fraud involves stealing by deception. **Vulnerabilities:** Lack of physical security. Lack of application and procedural safeguards leading to fraudulent payments being made. Lack of authentication leading to acceptance of false information and/or provision of information to an unentitled entity	✓	✓	✓

Table 3 Threat and Security Concerns – III (Department of Commerce 2007)

THREAT	Description and Examples of Vulnerabilities	Security Concern		
		C	I	A
Unauthorized Data Access	**Vulnerabilities:** Lack of logical access controls. Inability to authenticate requests for information. Unsecured wireless ports. Inadequate operating policies for handling, processing or storing sensitive information.	✓	✓	
Unauthorized Dial-In Access	**Vulnerabilities:** Unrestricted use of modems to dial into the network. Lack of an inventory of dial-up lines leading to inability to monitor dial up access. Lack of audit logs to detect unauthorized access. Lack of user authentication. Lack of intrusion detection software. Lack of firewall.	✓	✓	
Unauthorized Software Changes	Unauthorized changes to program code can be used to commit fraud, destroy data, or compromise the integrity of a computer system. **Vulnerabilities:** Lack of software configuration management policies and procedures. Lack of configuration management software to enforce configuration management. Inadequate segregation of duties between software developers and operations staff.	✓	✓	✓
Use of Pirated Software	Use of pirated software on a network places the agency in danger of legal action by the software supplier. **Vulnerabilities:** Lack of policy restricting staff to use of licensed software. Inadequate control of software distribution.			✓
Misrouting or re-routing of messages	Accidental misrouting is usually cased by user error. **Vulnerabilities:** Inadequate user training. Sensitive data not encrypted. Lack of proof of receiving a message.	✓	✓	✓
Transmission errors	This may occur due to the failure of any one of the network components that are used for the transmission of data. **Vulnerabilities:** Improper or inappropriate cabling. Inadequate incident handling. Lack of backup facilities or processes. No business continuity plans or procedures.		✓	✓

Threats and security concerns in the Table 1, Table 2, and Table 3 above were adapted from "Government Chief Information Office Guidelines" New South Wales, Australia Department of Commerce. The table is comprehensible enough to clarify what challenges Interglobal limited may be having in respect of its mail server. It is also a useful tool to be applied in other areas of IT/IS security environment in the company when it comes to dealing with vulnerability challenges on mail servers and mail clients.

4 MAIL SERVERS

4.1 General Overview of Mail Server

A server is computer or device on a network that manages network resources. A mail server is a computer that serves as an electronic post office for email. A mail server, also known as a mail transfer agent or MTA, a mail transport agent, a mail router or an Internet mailer. A mail server can be described as a program that stores and forwards Internet mail according to Internet protocols such as IMAP, SMTP, ESMTP or POP (Kayne 2010.)

There exist two main categories of mail server; namely outgoing mail servers and incoming mail servers. Outgoing mail servers are referred to as Simple Mail Transfer Protocol (SMTP) servers while Incoming mail servers come in two main varieties which are Post Office Protocol (POP) or Post Office Protocol version 3 (POP3) and Internet Message Access Protocol (IMAP) servers. Incoming mail servers are best known for storing sent, received messages local hard drives, and storing copies of messages on servers. Common mail server programs are Microsoft Exchange, Macintosh AppleShare IP Mail Server, qmail, Exim, sendmail, and Eudora Internet Mail Server (Singer 2003.)

Mail server does not work alone but operates in tandem with clients which are users' points of operations. Client-end enables users to communicate with server in achieving their data communication or messaging needs. An email client or email program allows a user to send and receive email by communicating with mail servers. There are many types of email clients with differing features, but they all handle email messages and mail servers in the same basic way. Some websites like Google gmail, Yahoo, & MSN also offer public email services, using their own mail servers.

E-Mail process is achieved when a user sends an e-mail message through an email client like Outlook or Eudora; the message is forwarded to a mail server or to a holding area on the same server called a message store to be forwarded later. The mail system uses Simple Mail Transfer Protocol (SMTP) or extended Simple Mail Transfer Protocol (ESMTP) for sending e-mail, and either Post Office Protocol 3 (POP3) or Internet Message Access Protocol

(IMAP) for receiving e-mail. The following figure diagrammatically describes how mail server and mail client are inter-related and operated.

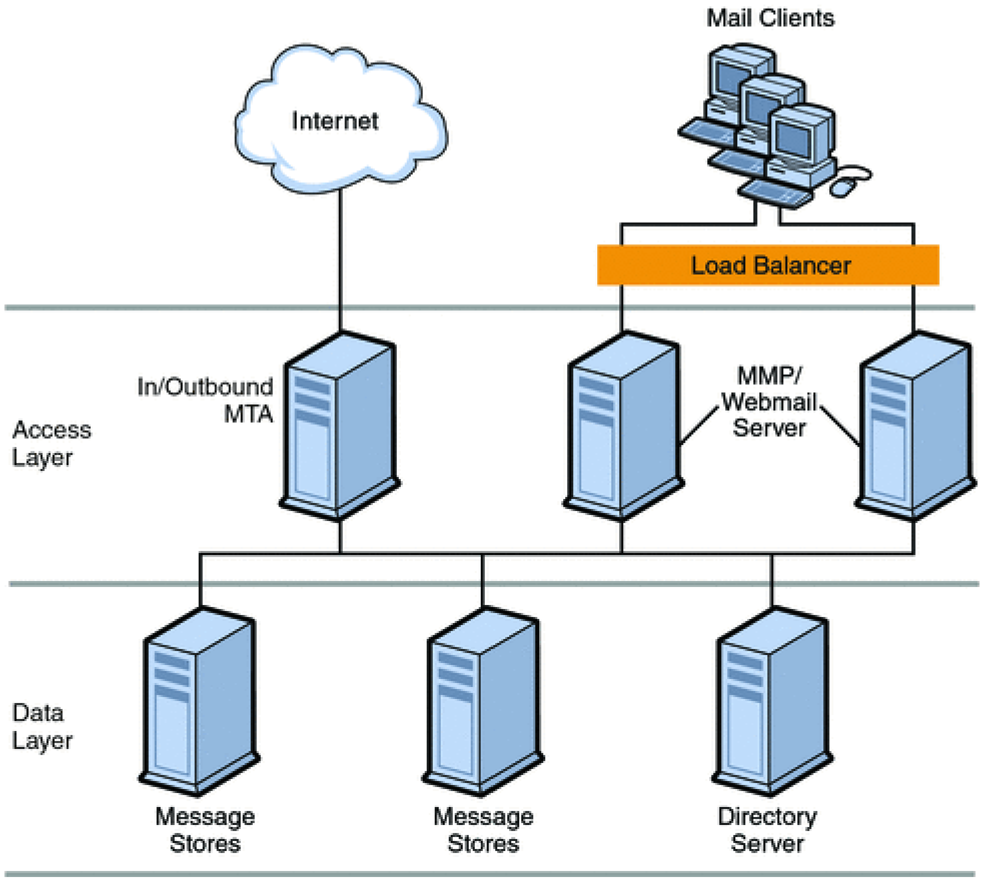


Figure 4: Typical Mail Server Architecture - Mail Server and Mail Client Operational Environment (Shaines & Christineballing, 2010)

The Figure 4 above shows a typical mail server architecture which identifies major components and layers. It also indicates relationship between mail server and mail clients and how they operate together for the purpose of exchanging mail across the network.

The mail server architecture above is a two-tiered architecture which splits the Messaging Server deployment into two layers: an access layer and a data layer. In a simplified two-tiered deployment, you might add an MMP and an MTA to the access layer. The MMP acts as a proxy for POP and IMAP mail readers, and the MTA relays transmitted mail. The data layer holds the Message Store and Directory Server (Shaines & Christineballing, 2010.)

4.2 Overview of Interglobal Limited's Mail Server

The information provided below describes the server technical information of Interglobal Limited. The overview of Interglobal Mail Server lists type of server, server hardware and configurations, server operating systems, mail server architecture, and e-mail client. All these details are required to aid the research work accordingly.

(i). Type of Server: HP ML370 G4
(ii). Interglobal Limited Server Hardware and Configurations: More information about the company server hardware and configurations can be found in Appendix 1.
(iii). Server Operating Systems: Window Server 2008
(iv). Mail Server Architecture: Exchange Server 2007
(v). Email client: Microsoft Office Outlook 2007

4.3 Microsoft Servers Operating Systems

This sub-chapter will look into Windows Server 2008 and Exchange Server 2007; and their few recent vulnerabilities and fixes. This is required because Interglobal Limited uses Microsoft Servers Operating Systems as listed in previous sub-chapter 4.2. My cross examination of Microsoft Servers Operating Systems and Office Outlook related vulnerabilities will provides useful information for my case company and further keep the company aware of what they need to do when they encounter challenges related to the vulnerabilities in their server operating systems and clients.

Windows Server 2008 is an operating system designed to act as an interface between the computer and its user. The Windows Server OS is a platform that you can use to build an infrastructure of connected applications, networks, and Web services. Originally codenamed Windows Server "Longhorn," Windows Server 2008 is built from the same code base as Windows Vista (Kanjilal 2010.)

Microsoft Exchange Server 2007 has been designed specifically to meet the needs of the different groups who have a stake in the messaging system that addresses both enterprise and employee needs while also being cost-effective to deploy and manage (Microsoft Exchange 2010).

Microsoft Servers Operating Systems Related Vulnerabilities and Fixes

1. Microsoft Windows Server Service Vulnerability: This vulnerability has been reported in Microsoft Windows and can be exploited by malicious people to compromise a vulnerable system. The vulnerability is caused due to an error in the Server Service component when processing RPC requests and can be exploited via specially crafted RPC requests. Successful exploitation allows execution of arbitrary code, but requires authenticated access on Windows Vista and Windows Server 2008. According to Microsoft, the vulnerability is currently being actively exploited (F-Secure 2009.) This vulnerability is reported as CVE-2008-4250 in Common Vulnerabilities and Exposures Directory.

Fix: Several patches are available based on the system type. Interglobal system type is x64-based PC. It is recommended that security update for Windows Server 2008 x64 Edition (KB958644) is installed (Microsoft 2008).

2. Vulnerability in Windows Server 2008 Hyper-V and Windows Server 2008 R2 Hyper-V: The vulnerability could allow denial of service if a malformed sequence of machine instructions is run by an authenticated user in one of the guest virtual machines hosted by the Hyper-V server. An attacker must have valid logon credentials and be able to log on locally into a guest virtual machine to exploit this vulnerability. The vulnerability could not be exploited remotely or by anonymous users (Microsoft TechNet 2010.)

Fix: The security updates for this vulnerability downloaded and installed automatically but if automatic update is not enabled on the target computers, then updates need to be checked and installed manually (Microsoft TechNet 2010.)

3. Vulnerabilities in DNS: These are vulnerabilities in the Windows Domain Name System (DNS) that could allow spoofing. These vulnerabilities exist in both the DNS client and DNS server and could allow a remote attacker to redirect network traffic intended for systems on the Internet to the attacker's own systems (Microsoft TechNet 2009[1].)

Fix: The security updates are already available for these vulnerabilities. Microsoft recommends that customers apply the update at the earliest opportunity (Microsoft TechNet 2009[1].)

4. Vulnerabilities in Windows that Could Allow Elevation of Privilege: The vulnerabilities could allow elevation of privilege if an attacker is allowed to log on to the system and then run a specially crafted application. The attacker must be able to run code on the local machine in order to exploit this vulnerability. An attacker who successfully exploited any of these vulnerabilities could take complete control over the affected system (Microsoft TechNet 2009[2].)

Fix: The security updates for this vulnerability downloaded and installed automatically but if automatic update is not enabled on the target computers, then updates need to be checked and installed manually (Microsoft TechNet 2009[2].)

It is recommended to always check on Microsoft Security Bulletin Search page for latest patches and security updates as they are made available by Microsoft TechNet Team in response to fix the discovered vulnerabilities in Microsoft series of products. Interglobal Limited needs to do this because live and breathe of its mail communications are powered by Microsoft products.

In addition, Windows Server Update Service (WSUS) is recommended. WSUS allows quick and reliable deployment of the latest critical updates and security updates for Microsoft Windows 2000 operating systems and later, Office XP and later, Exchange Server 2003, and SQL Server 2000 to Microsoft Windows 2000 and later operating systems (Microsoft 2005.) Table 4 below describes Windows Server update services features at both server-side and client-side (Microsoft 2005).

Table 4 Windows Server Update Services Features (Microsoft 2005)

Server-Side	Client-Side
• Updates for Windows, Office, Exchange Server, and SQL Server, with additional product support over time • Specific updates can be set to download automatically • Automated actions for updates determined by administrator approval • Ability to determine the applicability of updates before installing them • Targeting • Replica synchronization • Reporting • Extensibility	• Powerful and extensible management of the Automatic Updates service • Self-updating for client computers • Automatic detection of applicable updates

4.4 Mail Server and Mail Client Vulnerabilities

This sub-chapter discusses mail server vulnerabilities and mail client vulnerabilities. It is impractical to deal with mail server side alone without considering the mail client side of the scenario when dealing with vulnerabilities. The sub-chapter motivates the need to look into mail client vulnerabilities because most of the attacks are routed through client sides.

Mail server vulnerability is a typical vulnerability that arises when a malicious email is sent to a mail client side of the mail server in question. This vulnerability can cause problems because a virus that can run automatically can be injected through the process. Meanwhile, mail client vulnerability also occurs when malicious email is sent to a mail client. A mail server virus scanner may arrest the virus if it is a known one but if otherwise, the server side may be in danger.

A mail server virus scanner will not be able to detect viruses that are in these vulnerabilities. Therefore, it is very important that mail server AV programs detect these vulnerabilities (Declude 2009.)

Table 5 below lists common vulnerabilities with mail servers and mail clients by explaining them by name, type, and descriptions. These provide general overview of mail server vulnerabilities and mail client vulnerabilities commonly in existence and widely reported by users.

Table 5 Mail Server and Client Vulnerabilities (Declude 2009)

Name	**Type**	**Descriptions**
CLSID Vulnerability	Client	This vulnerability occurs when an E-mail uses a 'CLSID' as an extension.
Conflicting Encoding Vulnerability	Server	This vulnerability occurs when the headers of an E-mail claim that two or more different encoding types are used.
Outlook 'Blank Folding' Vulnerability	Server	This vulnerability occurs when there is a line in the headers with just a single space or a single tab character.
Outlook 'Boundary Space Gap' Vulnerability	Server	This vulnerability occurs when there is a space or tab in the MIME boundary.
Outlook 'CR' Vulnerability	Server	This vulnerability occurs when an E-mail contains a single 'CR' character within the E-mail headers (as opposed to a 'CR' followed by an 'LF', which is used to end a line in SMTP).
Outlook 'Long Boundary' Vulnerability	Server	This vulnerability occurs when an E-mail has a MIME boundary that is longer than allowed by the RFCs.
Outlook 'Long Filename' Vulnerability	Client	This vulnerability occurs when an E-mail has an attachment with a name longer than 256 characters long.

Outlook 'MIME header' Vulnerability	Client	This vulnerability occurs when certain safe MIME types are used, but a potentially dangerous file type is attached.
Outlook 'MIME segment in MIME post amble' Vulnerability	Server	This vulnerability occurs when it appears as though a MIME segment is occurring after the end of the MIME body.
Outlook 'MIME segment in MIME preamble' Vulnerability	Server	This vulnerability occurs when it appears as though a MIME segment is occurring before it should.
Outlook 'Space Gap' Vulnerability	Server	This vulnerability occurs when there is a space in one of the MIME headers where there is not normally a space.
Partial (Fragmented) Vulnerability	Server	This vulnerability occurs when one E-mail is split into separate parts, each in a separate E-mail.

With the table above, more insights are provided into common vulnerabilities with mail servers and mail clients. The table explains the vulnerabilities to make them more comprehensible in order to apply them in treating the results of the vulnerabilities. It is such a simple table that Interglobal Limited can easily understand more about mail server and mail client vulnerabilities and their descriptions.

The first step of combating mail server and mail client vulnerabilities is to know the vulnerabilities and what actually cause the vulnerabilities. At least, the company will be able to fight its known enemy. Table 4 will be a viable tool for Interglobal Limited and whoever makes reference to this research work.

4.5 Vulnerability Issues with Interglobal’ Mail Server

From the interview conducted with the representative of Interglobal Limited, the identified vulnerability issues are spam attacks while there have been challenges on POP download of mails from another webmail server and mailbox problems.

Irrespective of the location, whether at work or at home, spam is annoying, time consuming, dangerous, and cause you headaches because it forces you to waste time on determining which mail is legitimate and which is spam.

A typical Spammer sends a flood of traffic that overwhelms and overloads a mail server. The consequences are as listed below:

- It delays email delivery.
- It delays legitimate and genuine messages from reaching their intended recipients on the target network.
- It fills the target Inbox with number of ridiculous emails.
- It degrades the Internet speed which also affects server loading.
- It allows unauthorised access to confidential data such as target user’s details on his/her contact list.
- It changes target user’s search results on any search engine.
- It causes the depletion of system resources which may in extreme case, crash the mail server.

5 VULNERABILITY TESTING AND RESULTS

5.1 Vulnerability Testing

Vulnerability Testing is a very important process to adopt in any organization in order to improve and enhance system efficiency, data confidentiality, data integrity, and data reliability.

A vulnerability tester or scanner is a software tool used to scan systems for weaknesses. It performs function of vulnerability analysis and assessment, which defines, identifies, and classifies the security holes in a computer server, network, or other communication device. Vulnerability scanners may exist as desktop applications such as the case of Nikto, Whisker/libwhisker, Wikto, Acunetix WVS, and N-Stealth; and also exist as online applications as the case of GFI e-Mail System Testing Zone and HackerTarget. There are several vulnerability scanners but few are recommended. Hence, before forging ahead with the testing proper, the features of the few identified vulnerability scanners will be explained in the next paragraphs.

Desktop Vulnerability Scanner

The following lists briefly describe few selected desktop vulnerability scanners that can be used for future server scanning by Interglobal. The selections are made from the list of top 10 web vulnerability scanners at SecTools.org (Nmap/SecTools 2010).

1. Nikto: This is a free web server scanner and it is used to conduct comprehensive tests against web servers for multiple items, including over 3200 potentially dangerous files/CGIs, versions on over 625 servers, and version specific problems on over 230 servers.
2. Whisker/libwhisker: Libwhisker is a Perl module which can be used for HTTP related vulnerability testing. It can be applied for testing HTTP servers for many known security holes, particularly the presence of dangerous CGIs while Whisker is a scanner that used libwhisker.

3. Wikto: Wikto is an open source MS Windows adapted version of Nikto that checks for flaws in web servers. It adds various interesting pieces of functionality, such as a Back-End miner unlike Nikto.
4. Acunetix WVS: This is a commercially available web vulnerability scanner that automatically checks web applications for vulnerabilities such as SQL Injections, cross site scripting, arbitrary file creation/deletion, and weak password strength on authentication pages.
5. N-Stealth: This is a commercially available web server security scanner that has updated database than free web scanners such as Whisker/libwhisker and Nikto. N-Stealth is Windows only and no source code is provided.

Online Vulnerability Scanners

The following lists briefly describe few selected online vulnerability scanners that can be used for future server scanning by Interglobal:

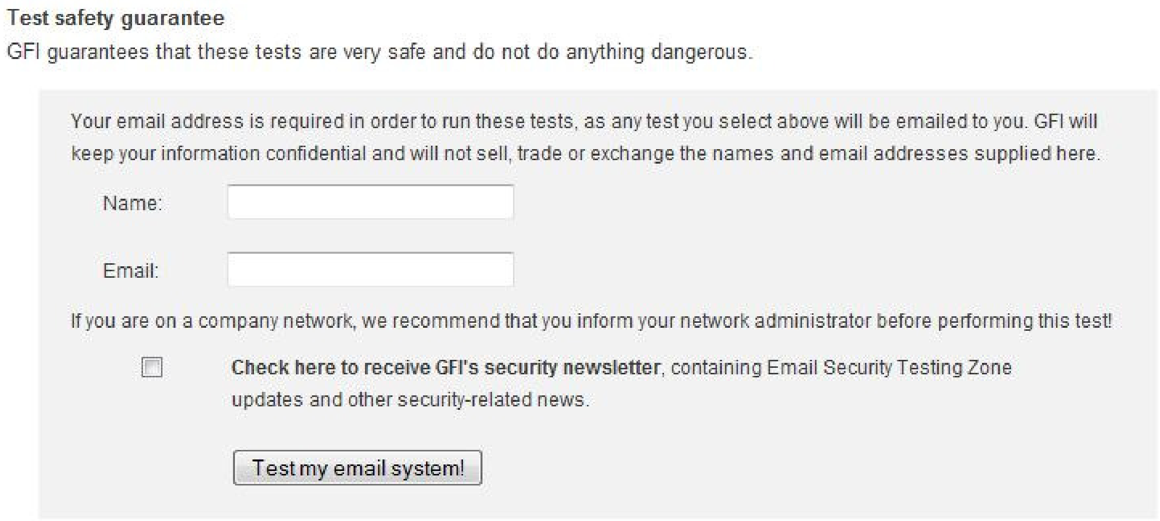
1. GFI e-Mail System Testing Zone: This is an online vulnerability scanner and assessment platform that is designed to detect whether an email system is safeguarded against a number of email-borne threats (GFI 2010).
2. HackerTarget: This is a provider of open source security scans with easy tools to use and it is convenient. This scanner requires no installation but only use target and email address. HackerTarget incorporate different online vulnerability scanners in a platform. Among various integrated scanners are Nmap Port Scan, OpenVas Vulnerability Scan, SQL Injection Scan using SQLiX and sqlmap, Nikto Web Server Scan, Joomla Security Scan, Sub Domain Scanner, BlindElephant Website Fingerprint, and WhatWeb Web Site Scan (HackerTarget 2010).

Testing for vulnerabilities using automated tools is an efficient way to determine existing holes and system patch level. Although many automated scanners are currently on the market and in the underground, it is important for the tester to identify and incorporate the current underground scripts/exploits into this testing. However, manual verification is necessary for eliminating false positives, expanding the hacking scope, and discovering the data flow in and out of the network (ISECOM 2006.)

5.2 Vulnerability Testing Zone

An online vulnerability scanner is used to carry out vulnerability testing on Interglobal Limited mail server. The choice of selection of the scanner in use was determined by the company in compliance with their internal policy. I have chosen GFI email system testing zone for the purpose of my research work in determining if any vulnerability exists on Interglobal mail server or clients.

An email is set-up on Interglobal domain for the purpose of the tests. All tests are carried out on the Interglobal mail server through the created email, thesis@integlobalimited.com. GFI email system testing zone, an online vulnerability testing platform was used to test the security of email system setup on the company's mail server. In addition to the utilization of GFI email system testing zone, manual verifications were also conducted for some of the vulnerability tests where applicable. Figure 5 below shows the screenshot of GFI e-mail system testing zone for online mail server vulnerability testing through the email set-up on the target server.



Test safety guarantee

GFI guarantees that these tests are very safe and do not do anything dangerous.

Your email address is required in order to run these tests, as any test you select above will be emailed to you. GFI will keep your information confidential and will not sell, trade or exchange the names and email addresses supplied here.

Name:

Email:

If you are on a company network, we recommend that you inform your network administrator before performing this test!

☐ **Check here to receive GFI's security newsletter**, containing Email Security Testing Zone updates and other security-related news.

Figure 5: GFI e-Mail System Testing Zone

The following vulnerability tests were conducted through the GFI e-Mail System Testing Zone:

i. Attachment with no filename vulnerability test: This test was carried out to examine whether Interglobal mail server accepts an attachment with no filename containing executable code that can bypass content checking security solutions.

ii. Long filename vulnerability test: This test was carried out to indicate whether Interglobal mail server blocks emails with attachments having long filenames, which can be used to trick a user into double-clicking the attachment, which can execute the malicious code it contains on the system.

iii. Popup Object Exploit vulnerability test: This test was carried out to determine if Interglobal mail server is vulnerable to the Popup Object Exploit which can automatically launch files on a vulnerable system.

iv. Double file extension vulnerability test: This test was carried out to show whether Interglobal mail server accepts emails which contain attachments with double file extensions.

v. ActiveX vulnerability test: This test was carried out to find out if Interglobal mail server is vulnerable to the ActiveX exploit.

vi. CLSID extension vulnerability test: This test was carried out to reveal whether Interglobal mail server detects and blocks files with Class ID (CLSID) extensions.

vii. Fragmented message vulnerability test (for Outlook Express): This test was carried out to check whether Interglobal mail server-level anti-virus/content checking system detects and blocks emails using the fragmented message exploit.

viii. MIME header vulnerability test called Nimda & Klez testing: This test was carried out to examine whether Interglobal mail server is protected against emails using the MIME exploit.

ix. Object Codebase vulnerability test: This test was carried out to examine whether Interglobal mail server detects and blocks emails using the Object Codebase exploit.

x. VBS attachment vulnerability test: This test was carried out to check whether Interglobal mail server blocks VBS attachments.

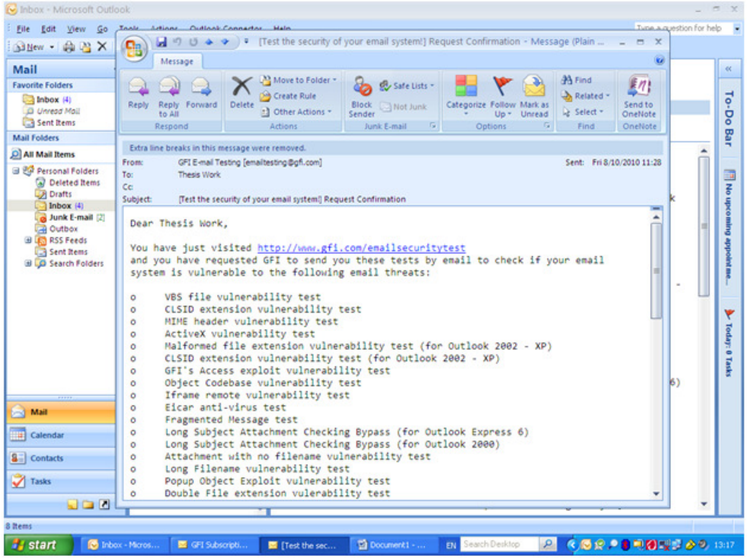
xi. Access exploit vulnerability test: This test was carried out if Interglobal mail server is vulnerable to the Access exploit vulnerability.

xii. Long subject attachment checking bypass test: This test was carried out to check if Interglobal mail server accepts email with long subjects. Long subjects can be used to bypass attachment checking.

As it has been recommended that manual verification may also be useful in conducting vulnerability tests where applicable; the vulnerability tests for Attachment with no filename, Long filename, and Double file extension were manually conducted in tandem with GFI platform to further confirm the existence or non-existence of such vulnerabilities in Interglobal mail server.

5.3 Vulnerability Test Results

These tests conducted on Interglobal mail server through the GFI email testing zone are to detect whether Interglobal mail server and client are safeguarded against a number of email-borne threats. Some of the tests execute automatically, demonstrating vulnerabilities within Outlook and email clients which run the files automatically upon receiving or viewing the email. Others require the end user to run the attachment. Figure 6 below shows the screenshot of the email set-up on Interglobal Mail server for GFI e-Mail System Testing and lists the vulnerability tests under process.



[Test the security of your email system!] Request Confirmation - Message (Plain ...

Extra line breaks in this message were removed.

From: GFI E-mail Testing [emailtesting@gfi.com]
Sent: Fri 8/10/2010 11:28
To: Thesis Work
Cc:
Subject: [Test the security of your email system!] Request Confirmation

```
Dear Thesis Work,

You have just visited http://www.gfi.com/emailsecuritytest
and you have requested GFI to send you these tests by email to check if your email
system is vulnerable to the following email threats:

o     VBS file vulnerability test
o     CLSID extension vulnerability test
o     MIME header vulnerability test
o     ActiveX vulnerability test
o     Malformed file extension vulnerability test (for Outlook 2002 - XP)
o     CLSID extension vulnerability test (for Outlook 2002 - XP)
o     GFI's Access exploit vulnerability test
o     Object Codebase vulnerability test
o     Iframe remote vulnerability test
o     Eicar anti-virus test
o     Fragmented Message test
o     Long Subject Attachment Checking Bypass (for Outlook Express 6)
o     Long Subject Attachment Checking Bypass (for Outlook 2000)
o     Attachment with no filename vulnerability test
o     Long Filename vulnerability test
o     Popup Object Exploit vulnerability test
o     Double File extension vulerability test
```

Figure 6: Dedicated set-up email for GFI e-Mail System Testing on Interglobal Mail server

For tests involving an email attachment, such as the VBS and the CLSID extension, if the attached file in the test email can be run, then the mail server is vulnerable: The test creates a file on the desktop called gfi-test.txt, which contains vital system information. If the attached file in the test email cannot be run, this is an indication that the server is not vulnerable to VBS attachment and CLSID extension vulnerabilities. For the MIME header and ActiveX vulnerability tests, text file gfi-test.txt appears on the desktop to indicate that the mail server is vulnerable to the exploit being tested for. In this case, gfi-test.txt is created automatically and contains vital system information (GFI 2010.)

Test Results Extracts

Tables 6, Table 7, and Table 8 below are test result extracts as they appear in the email set-up as responses for the test. The responses indicate the level of vulnerabilities in the areas as test results imply. Reply is only received when the testing entity or parameter signifies that vulnerability exists:

Table 6 VBS attachment vulnerability Test

Test Replies for VBS attachment vulnerability Test
VBS attachment vulnerability test has just been performed on your computer. Opening this mail automatically activates the test. _* If you can see gfi-test.txt_ _If the text file gfi-test.txt appears on your desktop, then you are vulnerable to this exploit._ _The text file demonstrates this: It has read vital information about your system, showing you that, in fact, it could have done anything it wanted on your system had it contained harmful code. (Note that the file in this test does not do anything malicious; it is just an example of a file which should be blocked at server level.)_ _* If you cannot see gfi-test.txt_ _If you cannot see the file, this means you have effective client-based email security. Note that, for your network to be secure, every machine on your network must have such client-based protection installed, including your servers. Server level security is recommended as additional protection._

Table 7 Access Exploit Vulnerability Test

Test Replies for Access Exploit Vulnerability Test
Access exploit vulnerability test has just been performed on your computer. Opening this mail automatically activates the test. ** If you can see gfi-test.txt* *If the text file gfi-test.txt appears on your desktop, then you are vulnerable to this exploit.* *Embedded VBA code within an Access database file (.mdb) that in turn lies within an Outlook Express email file can circumvent security measures in certain circumstances. Vulnerabilities within Internet Explorer and Outlook allow such content to be executed automatically.* *The text file demonstrates this: It has read vital information about your system, showing you that, in fact, it could have done anything it wanted on your system had it contained harmful code. (Note that the file in this test does not do anything malicious; it is just an example of a file which should be blocked at server level.)* ** If you cannot see gfi-test.txt* *If you are cannot see the file, this means you have effective client-based email security. Note that, for your network to be secure, every machine on your network must have such client-based protection installed, including your servers. Server level security is recommended as additional protection.*

Table 8 Long Subject Attachment Checking Bypass Test

Test Replies for Long Subject Attachment Checking Bypass Test
The Long Subject Attachment Checking Bypass test email (for Outlook Express& Outlook) was mailed to you separately. If this email includes an attachment with a long subject line, then your mail server has just accepted and sent you a potentially dangerous email - because in Outlook Express, long subjects can be used to bypass attachment checking. This means your server is relying on desktop level security to protect you. You may be prompted to run or save this attachment as soon as you preview or open this email. Please select the option to run it. ** If you can run this file* *If you can run this file, then you are vulnerable to this type of attack. The attachment with its long subject contains executable code that has circumvented the security settings of your network.* *As you can see, the enclosed attachment has read vital information about your system, showing you that, in fact, it could have done anything it wanted on your system had it contained harmful code. (Note that the file in this test does not do anything malicious; it is just an example of a file which should be blocked at server level.)* ** If you cannot run this file or if you do not receive the file at all* *If you do not receive the file or if you are unable to run the file, this means you have effective client-based email security. Note that, for your network to be secure, every machine on your network must have such client-based protection installed, including your servers. Server level security is recommended as additional protection.*

5.4 Analyses of Test Results

Table 9 below briefly describes the output of the tests conducted on GFI email system testing zone using the email set-up. The table has been structured to indicate the type of vulnerability test conducted, response or reply as received in the email which indicate the level of vulnerability on the mail server when the email is configured, and comments on the responses. In the response row, positive indicates presence and confirmation of vulnerability existence in the mail server under test while negative response confirms that the mail server under test is secure against the corresponding vulnerability.

Table 9 Analyses of Test Results

Type of Tests Conducted	**Responses**	**Comments**
Attachment with no filename vulnerability	Negative	Interglobal mail server is secure against this type of exploit.
Long filename vulnerability	Negative	Interglobal mail server is secure against this type of exploit.
Popup Object Exploit vulnerability	Negative	Interglobal mail server is secure against this type of exploit.
Double file extension vulnerability	Negative	Interglobal mail server is secure against this type of exploit.
ActiveX vulnerability	Negative	Interglobal mail server is secure against this type of exploit.
CLSID extension vulnerability	Negative	Interglobal mail server is secure against this type of exploit.
Fragmented message vulnerability	Negative	Interglobal mail server is secure against this type of exploit.
MIME header vulnerability	Negative	Interglobal mail server is secure against this type of exploit.
Object Codebase vulnerability	Negative	Interglobal mail server is secure against this type of exploit.
VBS attachment vulnerability	Positive	Interglobal mail server is vulnerable to this type of exploit.

Access exploit vulnerability	Positive	Interglobal mail server is vulnerable to this type of exploit.
Long subject attachment checking bypass	Positive	Interglobal mail server is vulnerable to this type of exploit.

From the tests conducted, it has been found that Interglobal mail server is secured against most parameters for vulnerability testing, as only three proved to be positive while nine proved to be negative in responses. Positive responses indicated that the mail server is vulnerable to the exploits which are VBS attachment vulnerability, Access exploit vulnerability, and long subject attachment checking bypass. These three confirmed exploits are perpetrated through the use of HTA, VBS, JS, and EXE files. Therefore, spammers use these loopholes as advantages to perpetrate their nefarious acts by spamming or sending spam messages to the email address resident on their target domains or server.

HTA, VBS, JS, and EXE files through which VBS attachment vulnerability, Access exploit vulnerability, and Long subject attachment checking bypass are exploited also serve as abode for worms and viruses to spread on the target victim’s computers and networks.

6 CONTROL MEASURES AND RECOMMENDATIONS

6.1 Control Measures Overview

Control measures are basically standard, guidelines, rules, and strategies required to minimize risks posed by threats and vulnerable systems. Control measures also initiate improvement of IS security. It is essential to secure network infrastructure by minimizing the number of access points to it, and put a firewall in place in case Internet access is required. On the web server, it is advisable to use Hypertext Transfer Protocol Secure (HTTPS) protocol, which uses Secure Socket Layer (SSL) protocol for secure communications. Application and file security measures are achieved by ensuring that the latest security patches are well installed, user-level security is enforced and local-level file security is enabled.

Staff enlightenment and education in the areas of data and system security are the most important aspects of managing risks on IT/IS security environment. These can be in form of preventive, enforcement and incentive measures.

6.2 Vulnerability Analysis

Vulnerable system is the genesis of risk in an information system. Risk management is the practice of identifying, classifying, re-mediating, and mitigating risks. Risk management can also be defined as the process of assessing risks and taking steps to avoid, or transfer, or mitigate, or accept them by introducing control strategies (VA Office of Research & Development 2007.)

The function to calculate risk can be defined as follow:

Risk (asset) = (T * V) / C

Where T is the threat, V the vulnerability, and C the control or safeguard measures employed to protect the assets. The asset need not be a single system, but can be a collection of systems grouped by function such as the human Resources systems or e-Mail servers, by physical or logical location such as New Jersey or systems in the corporate demilitarized zone or even by system administrators or group or users (Tipton & Krause 2008, 5.)

Once the assets and the threats to them have been identified, the system administrator can now determine what kind of security measures to endorse. Decision on appropriate risk management strategy should be on top list, then follow by the examination of the four general categories of risk management in order to determine which to implement from the list below:

- Avoidance: This involves use of safeguard to prevent risks occurrence.
- Transference: This involves transfer of risks to less-significant information assets.
- Mitigation: This involves process of reducing the impacts of risks.
- Acceptance: This involves acceptance of risks without control or mitigation (Smith & Komar 2003, 6.)

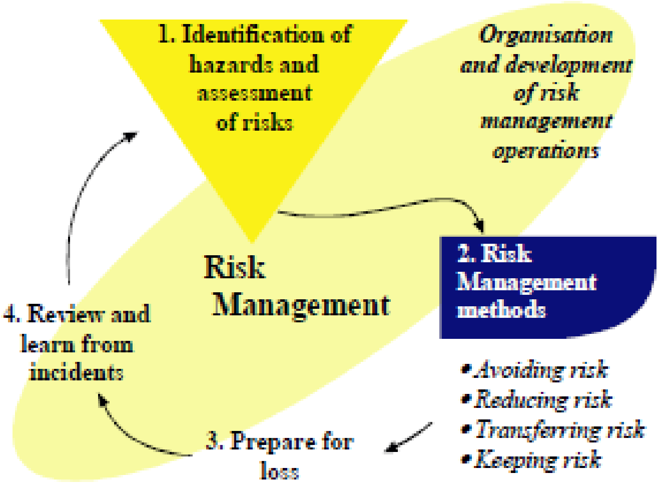

1. Identification of hazards and assessment of risks
Organisation and development of risk management operations
Risk Management
2. Risk Management methods
• Avoiding risk
• Reducing risk
• Transferring risk
• Keeping risk
3. Prepare for loss
4. Review and learn from incidents

Figure 7: Vulnerability Analysis Diagram (IOSH 2002, 5)

Figure 7 above shows the vulnerability analysis diagram which explains briefly vulnerability analysis as a rough risk management tool that comprises identification of hazards, assessment and prioritisation of risks, and management of risks. Management of risk involves planning, implementation and the review of control measures.

6.3 “Know Yourself and Know Your Enemy”

“If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle”

– The Art of War, Sun Tzu

The Art of War is a classic military-strategy text written more than 2000 years before computers were invented and many of the statements therein are still relevant to computer security nowadays. Table 8 below describes the principle of battle in a binary decision table, which is a vital tool in determining defense and control measure in an information security environment.

Table 10: Decision table of knowing your enemy and yourself (Smith & Komar 2003, 15)

	Know your enemy	**Do not know your enemy**
You know yourself	**You will generally succeed**	**You will succeed sometimes**
Do not know yourself	**You will succeed sometimes**	**You will never succeed**

According to the decision table of knowing your enemy and yourself, an administrator will generally succeed in managing security risks if he/she knows him/herself and the enemy. An administrator will sometimes succeed if he/she knows either him/herself or his/her enemy and he/she knows neither his/her enemy nor him/herself respectively. When dealing with information security, knowing yourself and yourself is not easy job to do but with the decision table above, the task may be lessen and make it easier to tackle issues and challenges affecting information security (Smith & Komar 2003.)

“Know Yourself”

It is imperative to know yourself at first in tackling information security issues. The following must be achieved in knowing yourself:

- Accurately assess your own skills
- Process detailed documentation of your network or system
- Understand the level of organizational support you receive (Smith & Komar 2003, 15.)

“Know Your Enemy”

Knowing yourself is not enough to combat any attack to your systems. Knowing your enemy is as complicated as knowing yourself – may be even more so (Smith & Komar 2003, 17). It is important for an administrator to know his/her enemies by indentifying attackers on the organisation’s information system. Administrators are able to know their enemies by virtue of previous attacks on their system or experience from others. By preparing to know your enemies, you are bound to achieve the following:

- Understanding external attackers
- Understanding internal attackers
- Knowing what motivates attackers (Smith & Komar 2003.)

6.4 Recommendation for Interglobal Limited

VBS attachment vulnerability, Access exploit vulnerability, and Long subject attachment checking bypass are the three confirmed vulnerabilities on the Interglobal mail server as indicated by the positive responses. These vulnerabilities are perpetrated through the use of HTA, VBS, JS, and EXE files. These files are factors that encourage more of spam messages going through the company mail server. Spammers usually use the loopholes as advantage to perpetrate their nefarious acts by spamming or sending spam messages to the email address resident on the target domains or server. If the target mail server has no content filtering solution, the spam messages are successfully routed to clients. Spam messages have been confirmed as challenges on the Interglobal mail server because they usually receive them in their emails.

In handling and preventing these exploits; HTA, VBS, JS, and EXE file types that execute codes; must be treated as dangerous files as they act as points of exploits by attackers and hackers. Server and client level securities are very essentials in dealing with confirmed and anticipated vulnerabilities. These will prevent the malicious attachment with executable files from reaching the users' desktop environment and company's network.

To be on a save side, it is recommended that Interglobal blocks file types that often carry viruses and those with more than one file-type extension. File types that often carry viruses are EXE, COM, PIF, SCR, VBS, SHS, CHM, JS, HTA, and BAT file types. It is unlikely that Interglobal will ever need to receive files of these types from the outside world. Some viruses disguise the fact that they are programs by using a double extension, such as .TXT.VBS, after their filename. At first glance a file likes LOVE-LETTER-FORYOU. TXT.VBS or ANNAKOURNIKOVA.JPG.VBS looks like a harmless text file or a graphic. Block any file with double extensions at the email gateway (Sophos 2006.)

In most cases, attachments do not execute automatically but many users under deceit of social engineering and other methods are easily led into running dangerous files (GFI 2010). The simple solution to this problem is to be aware and be cautious. Staff enlightenment may be very helpful. Application of reliable email content filtering solutions both at server and client level; and installation of latest software patches and security updates are advisable.

In addition, ensuring adequate data security and promptly attending to major security concerns such as confidentiality, integrity, and availability; and ensuring that the server is secure against many types of vulnerabilities; it is imperative that some or all of the following are implemented on the Interglobal information system at the Desktop Level Protection (DLP) and Server Level Protection (DLP) where necessary.

- Content filtering solutions
- Malware and Antivirus protection

- Authentication and password security
- Operating system and mail client security
- Packet filtering
- Firewalls
- Intrusion detection system
- Auditing and log files
- Physical security
- Routers and access control (Smith & Komar 2003.)

Spam Attacks Control Measures

Since spam attacks have been identified as a concern to the security of Interglobal mail server, it is important to explain some methods required in combating spam or reduce the impact to the barest minimum. The following methods as ways of advice tends to be helpful in handling spam related cases on email clients and consequently on mail server (Net-Security 2010).

1. It is important that Interglobal staff beware of social networking spam which is very common nowadays. The emergence and popularity of social media has aroused the chance for spammers to do nefarious acts on their target. Unsolicited e-mails or inboxes are sent out to several email addresses with malicious links which have possibilities of infecting the company's computers, networks, and mail server.

2. Ignore or delete spam related messages and know how to respond properly to them. Usually unfamiliar e-mail messages should be handled with caution, most especially when they come with suspicious links. In opening suspicious link it is advisable to use some browsers with built-in plugs-in for spam security that detect and alert spam related links. Such feature is available on Google Chrome and Latest Mozilla Firefox Browsers.

3. Do not click on links from emails you can not trust or suspicious to be spam. If you are not so sure of the link origin, do not attempt to click it, as this may lead to unauthorised data disclosure, system crash, and server failure.

4. Ensure that your computer operating system and security software are up to date. The information gathered from the representative of Interglobal Limited indicates that the server operating systems, server architecture, and mail client are up-to-date. This has been a factor that reflected on the vulnerability testing results, as the server is not vulnerable to most of the vulnerability parameters tested.

5. Install a dedicated anti-spam application both at server and desktop level. It is not enough to rely only on the in-built security features of the server operation systems and email client, but to added security tools to combat the known and unknown enemies. More reasons to install a third-party software to further secure the mail server, mail clients, networks, and users' desktop environments.

There is need to assemble a group of methods that work in a coordinated fashion to provide protection against a variety of threats because no single security component or method by itself can be expected to ensure complete protection for a network or system – or even an individual host computer. (Weaver, 2007, 27)

Mail server vulnerability is an aspect of information security and managing information security is somehow difficult. In order to manage IS adequately and appropriately, combination of technical, business, and people skills are required. Knowing how to handle vulnerabilities and vulnerable system is a catalyst to managing IS risk effectively. Indentifying vulnerabilities in systems tend to relieve security personnel on managing risk in an organisation. Without a good understanding of vulnerabilities and related issues, it may be impossible to secure information system effectively and efficiently.

The most fundamental skills in securing mail server, a typical information system, are the understanding the underlay and big picture of security. By understanding the underlay and big picture of security on how to secure information system as well as the limitations of security, you can avoid spending more time, more money, and more energy attempting impossible, try and error methods, or impractical security measures (Smith & Komar 2003, 8.)

Administrator and IS security officer should always bear it in mind that information security is all about risk management in its entirety and that there is no ideal situation in any system, which implies that no system is completely secure. Every system no matter how is vulnerable but the level and gravity of vulnerabilities differ. The level of risk is determined by the level of importance of the assets that are meant to be secured and the control system available. This equally determines the level of security threats those assets are exposed to. Administrators and IS security officers must understand how to evaluate his/her organisation's assets value, the threats to such assets, and the necessary control measures to drastically deals with the threats and perceived risks.

In order to ensure optimum information security, there is a need to identify possible threats, attacks, and vulnerabilities; and their corresponding risks, then follow the appropriate control strategies and measures to avert the ample effects that may arise from their emergence.

Vulnerability Scanning in the Future

Considering the limitations encountered on the choice of vulnerability scanning tools to be adopted based on Interglobal Limited internal policy that restricted me to conduct only surface scanning, I would recommend to the company to utilize any of the vulnerability scanners discussed in Chapter 5. The vulnerability scanners have the capabilities of deep scanning of server vulnerabilities and support advanced analyses of the results. The vulnerabilities scanners are Nikto, Whisker/libwhisker, Wikto, Acunetix WVS, N-Stealth and HackerTarget. Nikto, Whisker/libwhisker, and Wikto are open source vulnerability scanners and therefore are free to be used while Accunetix WVS and N-Stealth are commercial web vulnerability scanners. However, trial versions of those commercial scanners can be downloaded and used but with limitations on results.

7 CONCLUSIONS

The main objective of this research work which is center on identifying vulnerability challenges on Interglobal mail server and possible control measures was achieved. The research work has sensitised Interglobal Limited about giving attention to vulnerabilities in its mail server and other aspect of its IS. This research work is valuable because the output will be useful for Interglobal Limited and provide information on reduction in the time and money spent dealing with vulnerabilities and exploitation of those vulnerabilities. It has given the company opportunities to discover the challenges on its mail server without much cost implication. It helps the company to know more about vulnerabilities, effects of vulnerability, detection of vulnerability, and vulnerability control measures. The research output will help and guide in ensuring secure mail communications.

This research work has really widened my knowledge of vulnerability challenges on information systems and how to tackle them before they affect the information systems. It has put me in better position compare to when I started writing my thesis; to recommend and share ideas about vulnerability management. This research work is a starting point for my exploit of the IS vulnerability concerns; and has open my mind and arouse my interest to forged ahead in the future.

To young researchers who might want to explore this area of study, vulnerability management as a concept is more of newly sectionalized topic in the information security world. More often, vulnerabilities have not been treated as an entity but alongside other security concerns such as threats and attacks. I perceived more opportunities in the future in this area of study as companies will see need to engage vulnerability managers. Vulnerability management is just a saying that “Prevention is better than cure” which ensures that information system is less vulnerable. I intend to pursue my future research work on vulnerability management as being inspired by this research work.

REFERENCES

Printed

Al-Zubi, Ahmad Ali 2010. Threats Sources Identification. Canadian Journal on Network and Information Security Vol. 1, No. 1, April 2010. <http://ampublisher.com/April%202010/NIS-1004-015.pdf>

Foreman, Park 2009. Vulnerability Management. Auerbach Publications, New York. <http://www.infosectoday.com/Articles/Intro_Vulnerability_Management.htm>

Kumar, Rajendar 2008. Research Methodology. S.B. Nangia, New Delhi.

Smith, Ben & Komar, Brian 2003. Microsoft Windows Security Resource Kit. Microsoft Press. Redmond, Washington.

Thywissen, Katharina 2006. Components of Risk - A Comparative Glossary. United Nations University - Institute of Environment and Human security. Bonn. <http://www.unisdr.org/eng/library/Literature/9985.pdf>

Tipton, Harold F., & Krausse, Micki 2008. Information Security Management Handbook. Sixth Edition Volume 2. Auerbach Publications, Florida.

Weaver, Randy 2007. Guide to Network Defense and Countermeasures. Second Edition. Course Technology Centage Learning, Boston.

Whitman, Micheal E. & Mattord, Herbert J. 2005. Principles of Information Security. Second Edition. Thomson Learning Inc., Massachusetts.

Whitman, Micheal E. & Mattord, Herbert J. 2008. Management of Information Security. Second Edition. Thomson Learning Inc., Massachusetts.

Not Printed

Business Link 2010. Information Security Best Practice. Downloaded 18th September, 2010. <http://www.businesslink.gov.uk/bdotg/action/layer?topicId=1075406921>

Declude 2009. Mail Server Vulnerability and Mail Client Vulnerability. Downloaded 29th October, 2010 <http://www.declude.com/Articles.asp?ID=107>

Department of Commerce 2007. Threats and Security Concerns. (Adopted from

Government Chief Information Office Guidelines of New South Wales, Australia). Downloaded 6th November, 2010. <http://oregon.gov/DAS/EISPD/ESO/IACCoP/ThreatsConcerns.doc>

F-Secure 2009. Microsoft Windows Server Service Vulnerability. F-secure Corporation. Downloaded 25th November, 2010. <http://www.f-secure.com/vulnerabilities/SA32326>

Fenzi, Kevin & Wreski, Dave 2004. Linux Security HOWTO v2.3. Downloaded 2nd October, 2010. < ftp://sunsite.unc.edu/pub/Linux/docs/HOWTO/Security-HOWTO>

FileInfo 2010. Common File Types. Download 10th November, 2010. <http://www.fileinfo.com/common.php>

GFI 2009. Protecting your network against Email threats. Downloaded 26th October, 2010. <http://www.gfi.com/whitepapers/network-protection-against-email-threats.pdf>

GFI 2010. General: Frequently Asked Questions. Downloaded 25th June, 2010 <http://www.gfi.com/emailsecuritytest/faq.htm>

GFI 2010. GFI Email Security Testing Zone. Assessed 26th October, 2010 <http://www.gfi.com/emailsecuritytest/>

HackerTarget 2010: Security Vulnerability Scanning. Download 21st November, 2010 <http://hackertarget.com/security-vulnerability-scanning/>

Interglobal Limited 2008. About Us. Downloaded 18th October, 2010 <http://interglobaltd.com/>

Kanjilal, Joydip 2010. Addressing Security Vulnerabilities in Windows Server 2008 RC2. MC Press Online. Last Updated 21st March, 2010. Downloaded 25th November, 2010. <http://www.mcpressonline.com/security/microsoft/addressing-security-vulnerabilities-in-windows-server-2008-rc2.html>

Kayne, R. What is a Mail Server? Downloaded 20th May, 2010 <*http://www.wisegeek.com/what-is-a-mail-server.htm*>

Kinamik Data Integrity 2007. The CIA triad: Have you thought about Integrity? A Whitepaper by Kinamik. Downloaded 10th October, 2010. <http://www.kinamik.com/download/Kinamik-Whitepaper_CIA.pdf>

Mail Server - Glossary of terms related to LDAP. Downloaded 20th May, 2010 <http://www.gracion.com/server/guide/docs/Glossary.html>

Microsoft 2005. Windows Server Update Services Product Overview.

Downloaded 25th November, 2010.
<http://technet.microsoft.com/en-us/windowsserver/bb466208.aspx>

Microsoft 2008. Security Update for Windows Server 2008 x64 Edition (KB958644). Downloaded 25th November, 2010.
<http://www.microsoft.com/downloads/en/details.aspx?familyid=7B12018E-0CC1-4136-A68C-BE4E1633C8DF&displaylang=en

Microsoft Exchange 2010. Exchange Server 2007 Product Overview. Downloaded 17th October, 2010.
<http://www.microsoft.com/exchange/2010/en/us/exchange-2007-overview.aspx>

Microsoft TechNet 2009[1]. Microsoft Security Bulletin MS08-037 – Important. Downloaded 25th November, 2010.
<http://www.microsoft.com/technet/security/bulletin/MS08-037.mspx>

Microsoft TechNet 2009[2]. Microsoft Security Bulletin MS09-012 - Important. Downloaded 25th November, 2010.
<http://www.microsoft.com/technet/security/bulletin/MS09-012.mspx>

Microsoft TechNet 2010[1]. Microsoft Security Bulletin MS10-010 - Important. Downloaded 25th November, 2010.
<http://www.microsoft.com/technet/security/Bulletin/MS10-010.mspx>

Microsoft TechNet 2010[2]. Microsoft Security Bulletin Search. Downloaded 26th November, 2010.
<http://www.microsoft.com/technet/security/current.aspx>

MS-ISAC 2010. Local Government Cyber Security. Multi-State Information Sharing and Analysis Center. Downloaded 12th November, 2010.
<http://www.msisac.org/localgov/documents/Cyber-Security-Risk-Management-for-Local-Governments.pdf>

Net-Security 2010. 5 tips for protecting against spam attacks. Last updated 15th October, 2010.
<http://www.net-security.org/secworld.php?id=9996>

Nmap/SecTools 2010. Top 10 Web Vulnerability Scanners. Download 21st November, 2010.
<http://sectools.org/web-scanners.html>

ISECOM 2010. OSSTMM 2.1 Internet Technology Security Testing. Downloaded 18th October, 2010

<http://www.isecom.org/projects/osstmm.2.1.c.shtml>

PCMag 2010. Definition of: MIME exploits. Downloaded 30th October, 2010 <http://www.pcmag.com/encyclopedia_term/0,2542,t=MIME+exploit&i=47048,00.asp>

Ryabov, Vladimir 2010. Lecture Material on Scientific Writing and Research Work. Downloaded 16th June, 2010.

SAINT Corporation 2010. Vulnerability Scanning with SAINT. Downloaded 15th May, 2010 <http://www.saintcorporation.com/solutions/vulnerabilityScan.html>

SANS Institute 2001. System Administrator - Security Best Practices. Downloaded 10th June, 2010. <http://www.sans.org/reading_room/whitepapers/bestprac/system_administrator_security_best_practices_657>

Shaines & Christineballing 2010. Two-tiered Messaging Server Architecture: Planning an Oracle Communications Messaging Exchange Server Sizing Strategy. Oracle' Wikis Home. Last updated: 13th August, 2010. Downloaded 6th November, 2010. <http://wikis.sun.com/display/CommSuite/Planning+a+Messaging+Server+Sizing+Strategy>

Singer, Daniel E., 2003. SOA Definitions - Mail server. Last Updated 22nd January, 2003. Downloaded 7th November, 2010. <http://searchsoa.techtarget.com/sDefinition/0,,sid26_gci876011,00.html>

SME Vulnerability Analysis: SME Risk Management Toolkit by Institution of Occupational Safety and Health (IOSH) – April 2002. Downloaded 30th October, 2010. <http://www.pk-rh.fi/pdf/en/vulnerability-analysis-booklet>

Sophos 2006. A to Z of Computer Security Threats. Downloaded 18th September, 2010. <http://www.sophos.com/sophos/docs/eng/sophos-a-to-z.pdf>

Soy, Susan K. The Case Study as a Research Method. The University of Texas at Austin. Last Updated 12th February, 2006. Downloaded 20th May, 2010 <http://www.ischool.utexas.edu/~ssoy/usesusers/l391d1b.htm>

VA Office of Research & Development 2007. Key Points Related to Privacy & IT Security. Downloaded 18th September, 2010.

<http://www.research.va.gov/resources/data-security/docs/Key_Points.pdf>

What is a Mail Server? Downloaded 22nd November, 2010.
<http://whatismyipaddress.com/mail-server>

Appendix 1

Interglobal Limited Server Hardware and Configurations

- OS Name: Microsoft® Windows Server® 2008 Enterprise
- Version: 6.0.6001 Service Pack 1 Build 6001
- Other OS Description: Not Available
- OS Manufacturer: Microsoft Corporation
- System Name: GLOBE1
- System Manufacturer: HP
- System Model: ProLiant ML370 G4
- System Type: x64-based PC
- Processor: Intel(R) Xeon(TM) CPU 3.20GHz, 3200 MHz, 1 Core(s), 2 Logical Processor(s)
- BIOS Version/Date: HP P50, 7/19/2007
- SMBIOS Version: 2.3
- Windows Directory: C:\Windows
- System Directory: C:\Windows\system32
- Boot Device: \Device\HarddiskVolume1
- Locale: United States
- Hardware Abstraction Layer: Version = "6.0.6001.18000"
- User Name: INTERGBL\Administrator
- Time Zone: W. Central Africa Standard Time
- Installed Physical Memory (RAM): 5.00 GB
- Total Physical Memory: 959 MB
- Available Physical Memory: 2.54 GB
- Total Virtual Memory: 19.4 GB
- Available Virtual Memory: 15.9 GB
- Page File Space: 14.6 GB
- Page File: C:\pagefile.sys