Global Information Assurance Certification Paper

ENTERPRISE SECURITY FRAMEWORK

BY : MOHD RASHID BIN MOHAMAD
VERSION : 1.2F
GIAC USER ID : RASHID001

TABLE OF CONTENTS

Introduction

Distributed systems are becoming in creasingly heterogeneous and the security specifications must take this into account. Therefore, while the emphasis should be on open systems, interoperability with non -conforming systems must also be possible without loss of the functions necessary to preserve the basic security framework and with a minimum of inconvenience for the system administrator or end user.

These services must be provided in a manner, which ensures that the selection of any one facility shall not be to the detriment or exclusion of any of the others.

Background

Information is the most important resource of a modern organization. As such, information must be accurate and reliable at all times. In this age of the Internet, guardians of information finds themselves overwhelmed in the face of unauthorized access as networks are opened when connected to the Internet.

In such cases security services becomes critical to ensure the originality of the information is maintained, and that it shall never be exposed to unauthorized eavesdropping. This is especially so for the enterprise company which are trustees and custodians of e -business information. The need to preserve the integrity, availability and confidentiality of information is a major concern due to sensitivity and value bus iness data. Each organization information base is that critical element which describes items such as operation records, financial aspects, cash -flow information, health care and administrative -base office communications. It is their lifeblood and if conta minated or cut off, it can be critical, perhaps fatal, to their continued viability as a living entity.

This security framework sets the tone by defining security requirements, identifying security mechanism and measures, classifying resources and recommends implementation activities.

The Scope of Enterprise Security Framework

There are there (3) major components in an enterprise communication networks. There are connectivity via ISP (Internet Service Provider), internal Enterprise Company networks, an d Internet Gateway. The ISP networks normally provide the common transport on which users in the enterprise company operates, while all nodes within the VPN (virtual private network) access a gateway for Internet accesses.

Communication Pathway

The security framework outlined in this document will cover the following scope:

- Access of enterprise network by external network
- Access of enterprise nodes by other branches
- Access of the internet by users in internal
- Access by users from internet to the enterprise

Enterprise Security Framework Objectives

A security framework is required by an Enterprise Company to accomplish the objective of creating an effective, consistent, and ongoing information security process throughout the ISP. The framework addresses security needs in terms of integrity, confidentiality and availability of information.

As Enterprise is riding on ISP network; the enterprise alone cannot achieve those objectives. As such on the overall view, the ISP should complement with specific measures to meet the security objectives of integrity, confidentiality and availability of information, on the backbone network (ISP network).

The following are definition of key elements of the enterprise company and the ISP Security objectives as they coexist in the context of enterprise security framework :

Integrity

The Enterprise Company will undertake measures to ensure that no unauthorized transformation of information occurs while the information is under the custody of enterprise LANs.

The ISP will undertake measures to ensure that no unauthorized transformation of information occurs while the information is traversing at ISP network, and when the information is hosted at the ISP.

Confidentiality

The Enterprise Company will deploy controls to ensure that the inf ormation under the custody of enterprise LANs is protected from unauthorized access of compromise.

The ISP will deploy controls to ensure that the information traversing at ISP network, as well as information hosted at the ISP, are protected from unauthorized access or compromised.

Availability/Continuity

The Enterprise Company must establish controls to ensure reliable and available LAN facilities.

An ISP must establish controls to ensure reliable and available WAN (ISP network) facilities to the ente rprise company.

The Enterprise Security Framework

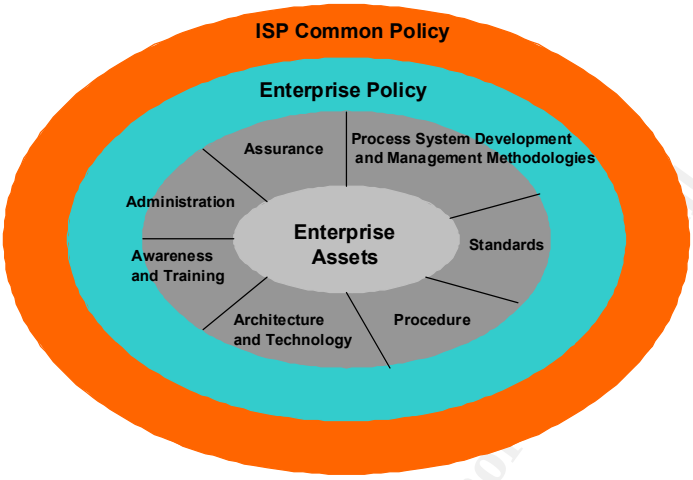
The enterprise security framework identifies the key elements, which collectively contribute to a consistent information security. Each of the key elements requires thorough study for further implemen tation of the associated work elements. This is so that the enterprise objectives of information confidentiality, integrity and availability can be achieved in a totality rather than as an afterthought.

There are 3 main entities in the Enterprise Security Framework:

1. Enterprise Assets
   This defines all valuable assets belongs to enterprise, is attempting to protect. The non-exhaustive enterprise assets are applications (e.g. E -mail, Financial Management System, MS Scheduler, Enterprise Bulletin, WEB Page, Human Resource System, Helpdesk and other Operations System), documentations and data (hard and softcopy), hardware, people, etc. This list will grow as more enterprise assets are defined.

2. Enterprise Policy (and Procedure)
   Enterprise defines the followin g procedures to prevent and respond to security incidents. It is important that the goal and direction of enterprise be considered. It is also important that the policy conform to existing policies, rules, regulations and laws that enterprise is subject to . It is undoubtedly important to consider security implications in a more global context, i.e. the

policy should address the issues when local security problems developed as a result of a remote site as well as when problems occur on remote systems as a result of a local host or user.



Enterprise Policy addresses the following key elements:

- Standards – are directives and guidelines that assist in the implementation of policies by providing more detail based upon the policy an d policy interpretation. They are used as input to the development of Procedures.

- Procedures – identify the who, how, when, in what order, and with what tools for the actual implementation of the standards.

- Awareness and Training Development – where awareness refers to knowledge of general information protection principles, requirements, and responsibilities; and training refers to the acquisition of skills at a more detailed level and is specific to a particular tool, technology or role.

- Administration – is the organization of the roles and responsibilities necessary to develop, implement, and maintain an effective information protection program within the enterprise.

- Assurance – covers the activities that measure the effectiveness of information protec tion efforts and includes activities to promote and foster an appropriately protected environment. It provides assurance that the system continues to behave as expected.

- Methodologies – System development methodologies facilitate structured approaches to system development, implementation and maintenance. A security methodology ensures that information protection is built into systems from the earliest development stage. It includes disaster recovery and contingency planning.

- Architecture – defines the standards and guidelines of future design and implementation efforts. It allows for many different efforts to result in a coherent and effective overall system. It defines structural guidelines that will continue to be useful over many years. Architecture br ings unity, consistency and simplicity.

3. ISP Policy (and Procedure)

We cannot avoid but to put ISP Policy within the Enterprise Security Framework for the reason of ISP being the medium of Connectivity complementing enterprise LANs, which collectively forms the whole enterprise network. In the same context, the ISP Policy will complement Enterprise Policy in protecting the WAN connectivity of enterprise network.

The framework is developed to protect Enterprise Company, and its assets. There are diffe rences between ISP Policy and Enterprise Policy. ISP Policy applies to all ISP customers subscribing to their services; thus the scope of the policy is to cover the overall view of ISP infrastructure. The Enterprise Policy on the other hand is more specifi c to internal. The uniqueness of Enterprise security requirements must therefore be uniquely addressed in the Enterprise Security Policy.

Network Security Issues and General Guidelines

Network Devices

Networks devices that are NOT carefully deployed will open any organization to a whole lot of risks. Many of the components of a network are designed to allow remote control and access over the network. This can be a point for hacking. To protect against this type of attack, routers and other "intell igent" equipments must have password protection for their system management functions. Placing necessary control measures to the premise where devices are kept must also physically protect all devices.

Inside Points of Attack

Studies have shown 99% of all security breaches involve someone INSIDE the organization, either as a perpetrator or as an accomplice. The security measure against this is to educate all staff and users, and to make it known that security issues are taken seriously.

Confidentiality of Passwords

Explanation to all users on the purpose of passwords is critical in any security implementation. End Users should be educated against sharing of passwords, or to put the passwords where anyone can see them. In order to ensure that password s really perform authentication,

- passwords should be considered strictly personal - just like keys (which is what they are)
- passwords should be memorized, not written down; it is easier for someone snooping around to look at the paper than to read your mi nd
- should not be trivial to guess (so avoid common words, or people's names)

Effective deployment of Authentication

- one common database can be used for all or most authentication functions
- users can select their own passwords
- passwords that fail the tri viality checks are disallowed by the password - change command
- passwords must be new (i.e. any word that has been used as a password before is disallowed)

Ethernet Packet Snooping

The basic local area technologies (Ethernet, token ring) all involve attaching a number of individual workstations to the same "wires". While this makes it inexpensive to build high -performance networks, it also means that anyone with the right tools can look at those wires and see what everyone else is doing. This is great for t roubleshooting, but bad for privacy. In the case of Ethernet, the tools are readily available: Any PC with a network interface card can be used for eavesdropping with a small program which most programmers could write in a day given the right documentation. Such programs - intended as troubleshooting tools - are readily available from electronic bulletin boards and other public sources. The good news is that they only work on the local "wires": In the worst case, within your building. With a little more car e and a little more money spent on equipment (filtering bridges or switching hubs), only within the department or workgroup.

Outside Attacks

Wiretaps

When network traffic leaves the building, it generally goes either on a microwave radio link, satellite link, by leased lines or by a dial -up modem link. While most people worry the most about the dial -up links, they are ironically the most secured of these connections. The modern high -speed

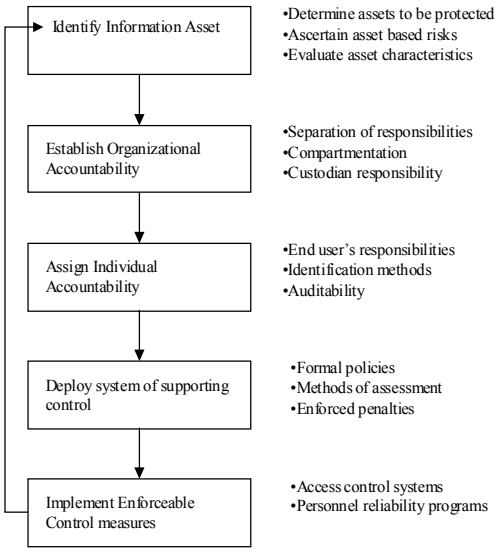
modem connection is almost completely immune to wiretapping: Both ends are transmitting at full speed, and each of them can recover the incoming data stream only because they know their own signal and can subtract it in real-time. A third party eavesdropping will have no way of separating the two simultaneous data stream s. With leased lines, you have to trust the Telephone Company to protect you from wiretapping. If you trust them to protect your voice telephone lines, you are already relying on such trust.

Dial-In Ports

Dial-In ports are usually a major point of unauth orized access. It is proposed that dial-in ports be NOT allowed for direct access into the Enterprise Network Infrastructure.

General Guidelines

The following flowchart is used in modeling this security framework for Enterprise Company :



Security Implementation

Implementing security in totality within the Enterprise is in another words, implementing standards, procedures, awareness and training development, administration, assurance, methodologies and architecture. Each has been described within the Security Framework section.

The following section discusses the architectural implementation of security within the Enterprise Company as a recommendation.

Network Security Implementation

Physical Layer attributes Network

Network Recovery Center
Network Recovery Center provide network resiliency in terms of hot backup for lines, load balancing and rerouting if Network Control Center fails. This will ensure service continuity and availability of network to the enterprise.

Fiber Optical Physical Netwo rk Backbone
Network backbone is mainly on optical fiber, which are very difficult to tap into information traversing the backbone. It is so difficult that a hacker would have to invest excessive and substantial resources and high expertise, before he can s uccessfully hacked in. This is due to the high -tech design of the fiber optic technology and the highspeed level information is travelling.

Physical Security
All network devices are located in a secured computer room where access is restricted to only a f ew dedicated personnel.

Network technology and its supporting system, NMS

Network Topology
The network topology is should be used as hierarchical partial -meshed topology, which means at least two trunk lines are connecting to one network node. This wil l allow network resiliency and load balancing.

Jumbled up, Packetised and Proprietary data
The information from Enterprise Company as they traverse the network cloud is proprietary and packetised. This would mean that even if information were tapped into, it would be very difficult to translate the information into meaningful text.

Centralized NMS
Centralized NMS provide security management as follows:

- User authentication using UNIX id/password validation
- User authentication for securing access to objects and manipulation of objects
- Use of community strings to validate SNMP service primitives

- FTP security with the use of encrypted id/password

TCP/IP

Network Address Translation (NAT)

NAT is implemented to hide internal addressing information to the Internet, and this should be implemented at the Enterprise gateway to Internet. This concept of public and private address is a form of protection to a network that requires anonymity.

Firewall

The main function of a firewall is to centralize access control. A firewall serves as the gatekeeper between the untrusted Internet and the more trusted internal networks. If outsiders or remote users can access the internal networks without going through the firewall, its effectiveness is diluted. For example, if a trav eling manager has a modem connected to his office PC that he or she can dial into while traveling, and that PC is also on the protected internal network, an attacker who can dial into that PC has circumvented the firewall.

Similarly, if a user has a dial-up Internet account with a commercial ISP, and sometimes connects to the Internet from their office PC via modem, he or she is opening an unsecured connection to the Internet that circumvents the firewall.

Firewalls provide several types of protection:

- They can block unwanted traffic.
- They can direct incoming traffic to more trustworthy internal systems.
- They hide vulnerable systems, which can't easily be secured from the Internet.
- They can log traffic to and from the private network.
- They can hide information like system names, network topology, network device types, and internal user ID's from the Internet.
- They can provide more robust authentication than standard applications might be able to do.

Software Application Security Implementation

Applications implemented in the Enterprise are mainly having a minimal of userid and password as its access control implementation.

Recommendations:

a. Userid and password is the weakest form of authentication, as this is normally implemented in a text fo rmat and if tapped into, can be

easily exposed to unauthorized users. The enterprise should exercise the Confidentiality of Password as described in the previous section.

b. The Enterprise should address the following issues which normally arise:
   - Who is authorized to grant access those application and approve usage
   - Who may have system administrator privileges
   - What are the user's rights and responsibilities
   - What are the rights and responsibilities of the system administrator vs. those of the user
   - What do you do with sensitive information

Applications can implement the following security measures:
- Authentication – a guarantee that a message really has come from the person who claims to have sent it.
- Non-repudiation – the certainty of knowing that the sende r of the message cannot later deny having sent it
- Confidentiality – evidence that the contents of the message have not been disclosed to third parties.

To implement the above security measures, applications can make use of the Public Key Infrastructure (P KI) technology. With PKI, enterprise officers will make use of public and private keys, as well as digital certificates to allow authentication and digital signature (non - repudiation).

Security Software Implementation

There will be three (3) points a t which automated security clearance has to be obtained.

I. Entry into Enterprise Virtual Private Network
II. Entry into Enterprise local network
III. Entry into Enterprise Applications

Each of the above points should implement one or a combination of th e following security procedures:

i. Traffic Inspection
ii. Client and User Authentication
iii. Encryption

Apart from the above, other mechanism to ensure data integrity and access controls should also be implemented:
- Network Address Translation

- Policy Routing
- Content

Security Level

Three security levels are proposed: (Refer to access Matrix for details on Implementation)

Level I:
This security level is the most stringent and is applied to resources that are most sensitive and valuable and are accessibl e by only a selected group of users. The enforcement of Security procedures will be at all three (3) Entry Points.

Level II:
This security level will be implemented for resources that are sensitive and valuable and can be accessed by registered users of t he Enterprise. Enforcement will be at Point I and Point III.

Level III:
This security level is liberal and will be applied on public accessible information and applied at Point I and Point II.

Security Procedure

Five security procedures are proposed:

I. Traffic Inspection

It is a security mechanism that intercepts and inspects all inbound and outbound packets of a network. Though the architecture of traffic inspection is dependent on the selected control system, this mechanism provides for efficient in spection method from its ability to extract information such as application and ports from TCP/IP packets.

Two types of Inspection is available:

- Applications/Services Request Check
  Each access to Enterprise Servers can be tracked to ensure only approved applications on specific ports are allowed (Web - HTTP, Mail applications – SMTP, FTP, etc).
- TCP/IP port Access Check
  Each access to servers on ports other than for allowable services should be rejected.

II. Authentication

- Client
  Client authentication allows for a user to be validated prior to access. Authentication is done based on the client workstation with a known IP address obtained from the authentication process. Transparent authentication will be the desired method. Once authenticated, the client from the workstation can access any applications allowed by the security system.

- User
  User authentication allows a known user to be validated independent of workstation IP address. Only limited applications support this form of authentication. HTTP (web) supports this authentication method.

- Applications Level Authentication
  This authentication regime is implemented by the applications server and provides authentication for users specific to the applications and datasets associated with the application.

III. Encryption

Encryption is one of the most secure methods of providing security over public networks such as Internet. Encryption can be implemented as an option.

IV. Network Address Translation

All Enterprise Servers will NOT be explicitly identified to the Internet. The IP addresses of all Enterprise Servers that are advertised to the Internet are different from the one set on the Servers. Network Address Translation is performed at network gateways that will point to the correct servers. This concept of public and private address is a form of protection to a network that requires anonymity.

V. Policy Routing

This is a technique that will ensure all inbound traffic are routed (redirect) to a specific internal gateway. By doing this, security measures implemented at the gateway cannot be bypassed. While this technique is recommended, its full deployment will be carefully done, as there could be performance issues that need to be addressed.

VI. Content Security

Content filtering is the process of examining incoming or outgoing data for a variety of problems and attributes. Action can then be taken based upon the type of problem or attribute encountered. A key feature of content filtering is the ability to customize the list of problems and attributes and what actions should be taken on them.

This customization normally can be modeled after elements contained within the enterprise security policy.

The actions involved in content security such as :

a. E-mail scanning and monitoring
Checks all e-mail inbound ant out bound for confidential data, excessive file size and proprietary material. Messages are scanned using keywords and phrase. Email attachments infected by a virus or Trojan might be cleansed or quarantined.

b. Web content
Checks all web activity by identifying and managing web content containing racist or hate material, banned files, pornography, profanity and potentially lost or corrupted material.

c. Downloadable applications execution
Checks all content for viruses, Java sc ripts, ActiveX and .exe. These can be attached to e-mails or hidden behind downloadable material from Web. If the data contains malicious Active -X or Java code, the content security server can be configured to remove the offending code, or block the page e ntirely.

d. Quarantine and block sensitive data
Any data infected with a virus or Trojan, content management server can be configured to delete the file, quarantine the file, or clean the file. If the file contains inappropriate content, the content se curity server can be configured to block the offending material.

Access Matrix
Enterprise will need to define all resources and users, as well as classification of users. It is proposed that the following matrix be used:

No. Resources	User Class	Security Procedure	Enforcement Point
01.			
02.			
03.			
04.			
05.			

Using the above Access Matrix diagram, each user is assigned not only an ID on the system, but also a role to play. Each object is then given a list of what users roles are allowed to access that object. If the user is on the list, they are allowed. If the user is not on the list, their access is denied.

Conclusion

Implementation of a comprehensive security framework will help ensure a secure e-business in an "always on global eco nomy. By taking the three e's – establish, educate and enforce approach to the whole security framework, enterprise businesses gain a high degree of confidence, while fostering a harmonious and trusting work environment.

References

1. Information Securi ty KickStart Highlights – The SANS Institute 2001
2. Security Manual – An Introduction To Security *http://www.securityfocus.com/data/library/index.html#_Toc444596077*
3. TrueSecure Corporation - Hurwitz Report : A Practical Approach to a Comprehensive Security P rogram *http://www.trusecure.com/html/tspub/whitepapers/trusecure_methodology.pdf*
4. Executive Insights on Content Security : Proactively Addressing Potential Liabilities in the New Economy *http://www.contenttechnologies.com/products/collateral/pdfs/content_se curity.pdf*
5. Bradley Cohen : Introduction to Enterprise Content Filtering *http://www.sans.org/infosecFAQ/email/content_filter.htm*
6. Compaq Compurter Corp : Compac Enterprise Security Fr amework *http://www.compaq.com/support/techpubs/whitepapers/ecg248a0897.html*
7. Open ROUTE Network, Inc : Internet Security Primer *http://www.techguide.com/html/intsec.pdf*

Last Updated: May 23rd, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event