GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

How to Effectively Secure Your Business

By Albert Yu

SANS Security Essentials GSEC Practical Assignment Version 1.3

1. Abstract

The change of the business needs means the change of the technology requirements. Since the introduction of computer, the way to do business has been dramatically reformed. Once your computer is connected to network, there is a business risk of the critical data being threatened by confidentiality, integrity and availability. This paper will outline the essential approach that helps to determine how to effectively and efficiently secure e-Commerce business, infrastructure, servers, hosts, and applications.

There is no "silver bullet" that one single model will fit for all. The best solution is to understand your business environment on how to make use of your network and computer in doing business. I would discuss the complete cycle of infrastructure security appraisal and protection processes comprised of "risk assessment", "security policy", "hardening infrastructure security architecture" and "incident handling". I strongly believe that every process is linked up with each other and provides a feedback linkage. The success of securing your business is highly dependent on how effectively to execute the following tasks.

2. Risk Assessment

Risk Management, as defined by BS 7799:1999 Part 1, is "assessment of threats to, impacts on and vulnerabilities of information and information processing facilities and the likelihood of their occurrence".

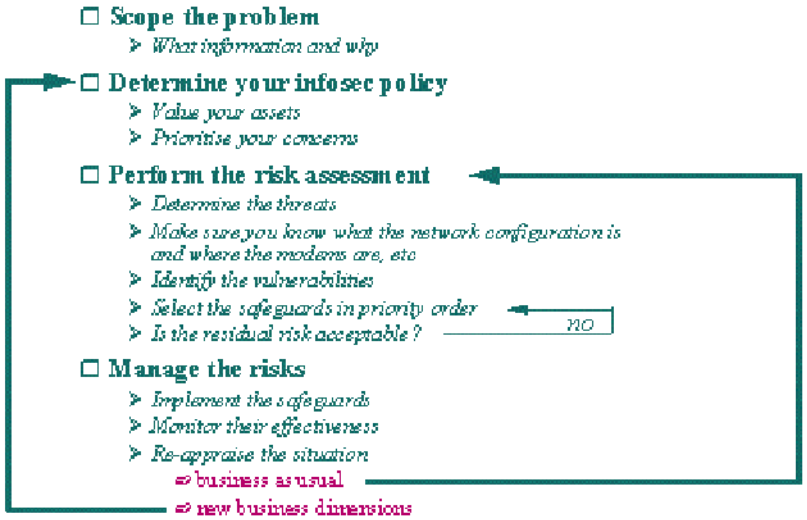

Figure 1. Process model of ISMS (Source: http://www.gammassl.co.uk/topics/IAAC.htm)

In order to understand the threats, we need to know where the vulnerabilities in the

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

infrastructure are. The threats may be from the outsider through the network (i.e.. wireless, leased line, DSL, telephone and so on) or the insider through the local segment. Let's have a look of the threat factors.

Outsider threat factors
- Do you have connections to the "trusted" and "non-trusted" networks?
- Do you provide e-commerce?
- Do you have ~~a~~ remote access to your network?
- Do you have wireless access?

Insider threat factors
- Do you allow users to download software from Internet?
- Do you restrict your users of application access?
- Do you allow users to add their personal software into the desktop?
- Do you disallow any visitors to use your network?

Example: -
If there is wireless access point configured in your network, your staff is capable of accessing the network from anywhere in the large warehouse at 2nd floor.
Determine the threat:
- Attacker may be able to access the network from outside the building or unauthorized areas.

Network configuration protection:
- Is the wireless access point configured with authentication and encryption?
- Testing the access distance to the wireless access point from the authorized area (i.e.. warehouse) and unauthorized area.

Identify the vulnerability
- Assumed the wireless service can also be accessed from the ground floor but is unreachable in the parking area or outside the building.

Select the safeguards:
a) Is the physical security sufficient at the ground floor?
b) Could the wireless access point be relocated to a higher level?
c) Could there be another type of wireless access point supporting shorter distance access?

Manage the risk:
- Upon the acceptable safeguard selected and implemented, it needs to keep monitoring the effectiveness.
- The specific-system security policy needs to be documented and periodically revised with updated safeguard requirement information.
- If no acceptable solution exists, the wireless access may need to be terminated.

3. Security Policy

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The purpose of Information Security Policy is to provide a concise and realistic guidance for the company staff, suppliers and vendors to follow. This is the first line that the companies manage the business risks through the security policies. In general practice, the policies will clearly explain what should or should not be allowed along with the exception procedures upon necessary. The policies may be classified as high-level corporation policy, issue-specific, system-specific and procedural-specific policy. Let's review each of them.

3.1 Corporation Security Policy

This is a high level overall Corporation Security Policy. This policy is mainly to address the organizational policy and the ownership of individual policy. The policy should be easily to reach by each staff such as posting in the corporation web site. The contents of the corporation policy may address to Acceptable Use Policy, Acquisition Assessment Policy, Audit Policy, Information Sensitivity Policy, Risk Assignment Policy and so on. ISO 17779/ BS 7799 Information Security standards are the comprehensive documents and have been acted as the industrial security policy reference. This is a solid foundation to help you developing your company IS policies.

- *Acceptable Use Policy* defines the acceptable use of company assets including computers, servers, network, network access in terms of protecting the corporate resources and proprietary information. In general, this policy applies to everyone as a company employee. For better understanding, I have outlined the template of "*Acceptable Use Policy*" for reference purpose.

Examples:

- ✍ Use of Email - As a corporate policy, all e-mail to clients need to be posted with the standard of proprietary information as a company policy.
- ✍ Use of Internet - No sexy, sanitation, discrimination, offensive, adult web surfing is allowed
- ✍ Anti-Virus Process - All desktop and portable PC needs to be installed with anti-virus software otherwise it is not allowed to connect into the company network through local and remote access.

- *Acquisition Assessment Policy* defines the responsibilities of Information Security Group what are the requirements to assess the acquisition.
- *Audit Policy* defines the standards for conducting the system and networks auditing and risks assessments. This is a critical feedback process to ensure that the securities policies are complied.
- *Information Sensitivity Policy* defines a basic classification of sensitivity information and how to secure the company information in appropriate manner.
- *Risk Assignment Policy* defines standards on when and where the risk assignments need to be performed.

3.2 Issue-specific Policies

It can be further classified into:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Network-specific: -

- ✍ *Router Security Policy* defines the standard routing, accessing and filtering security standards.
- ✍ *Analog/ISDN Line Policy* defines the standard security requirements for using analog/ ISDN lines for communication.
- ✍ *Dial-in Access Policy* must be a crystal standard what and where the dial-in access is allowed and disallowed along with the complete authorization and review procedures.
- ✍ *Internet DMZ Equipment Policy* defines the security standards regarding to the equipment access, protection, physical locations and so on.
- ✍ *Internal and DMZ Lab Security Policy* defines some critical restriction requirements against of the LAB environment. For instance, no production database should be installed in LAB environment. If the LAB environment is connected to outside network, it has to be physical isolated between the LAB and production segment. Otherwise, a security review process needs to be applied before connection.
- ✍ *Extranet Policy* defines the legal usage for linking up the organization network to a 3rd vendors, service providers or client's network under agreed minimum security standards.
- ✍ *Encryption Policy* defines the acceptable encryption algorithms that should be deployed in the organization.

Enterprise Service-specific (Desktop and Server): -

- ✍ *Password Protection Policy* defines standards for password creating techniques, storing and protecting method, and enforcement of scheduled password change.
- ✍ Anti-Virus Policy defines standards where and how to protect the company desktops and servers from the virus affection. Personal PC used for work should be included in the policy clearly.
- ✍ *Database Credentials Coding Policy* defines standards how to store, retrieve and log database usernames and passwords.

Application-specific: -

- ✍ *Application Security Standards* define standards for the minimum application security criteria for the ASP in term of authentication, encryption and coding to ensure the resources and proprietary information secured.

- ✍ *Automatically Forwarded Email Policy* - Documents the requirement that no email will be automatically forwarded to an external destination without prior approval from the appropriate manager or director.

Procedural-specific: -

- ✍ *Third Party Network Connection Agreement* defines standards of the connection usage and requirements that both parties need to agree upon and sign off. The agreement should usually have prepared by legal department.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- *Remote-Access Procedure Policy* defines the remote-access connection security standards from outside networks to ensure the acceptable encryption, personal firewall and anti-virus enforcement applied.
- *Anti-Virus Process* defines the enforcement procedures in order to obtain the latest patches and patch into the network users.

Another Approach
This is an alternative approach for grouping the specific security policies by governing the policies under organizational and functional security. .

Data Center
- Physical security access
- Server security access
- Backup and Disaster Recovery
- Intrusion protection
- Security audit and review
- Subset of system-specific security policy

Desktop Support
- Authentication
- Encryption
- Internet Access Security
- Firewall
- Anti-Virus protections
- Security audit and review
- Subset of system-specific security policy

Enterprise Service
- Server Security Policy
- Authentication
- Encryption
- E-mail, DNS, DHCP, Browser, Windows Security
- Security audit and review
- Subset of system-specific security policy

Telecom/ Network
- Router Security Policy
- VPN Security Policy
- Wireless Communication Policy
- Firewall/ ACL
- Authentication
- Encryption
- Network Intrusion protection
- Security audit and review
- Subset of system-specific security policy

© SANS Institute 2000 - 2002, Author retains full rights.

4. Hardening Infrastructure Security Architecture

First of all, the infrastructure should be built with the security concept in mind. Referring to Figure 2, it clearly showed the intruder knowledge and attack sophistication is dramatically changing upward. The security policies will provide the baseline guidance. However, the best practice designing and deploying of the infrastructure with the security mindset is an important and critical challenge to mitigate the attacks.

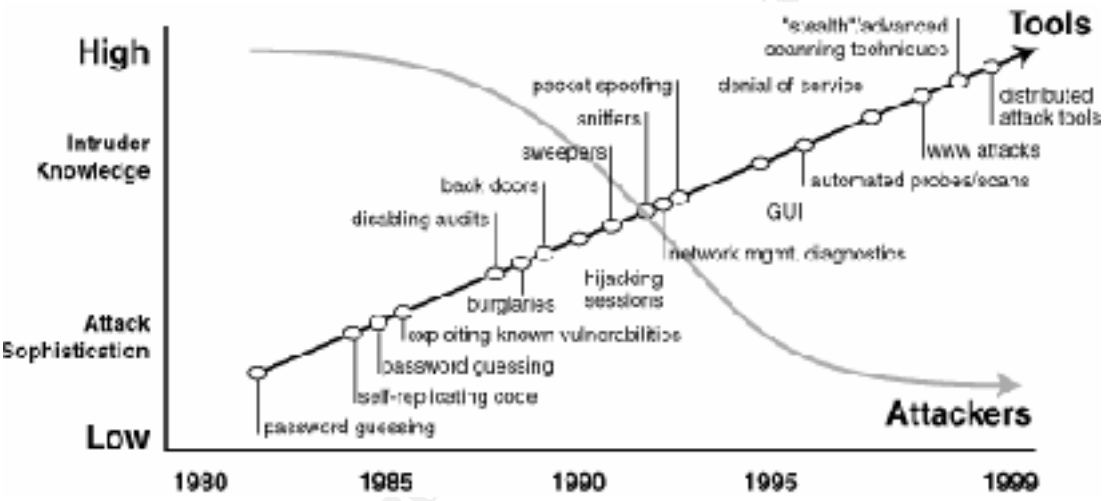

Figure 2. Attack Sophistication vs. Intruder Knowledge (Source: CERT)

In order to harden the infrastructure security architecture, we should list out the most important functions and security issues to be considered along with the infrastructure design.

- Network Security without compromise to performance
- High Availability
- Fully Redundant Solution
- High performance and high throughput
- Scalability and Fault Tolerance
- Stateful Firewall
- To harden the network security affected by Dos, DDos, Resiliency, Privacy, Access, Authorization and Accountability
- Network Management and Security monitoring
- Host and Network Intrusion Detection

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

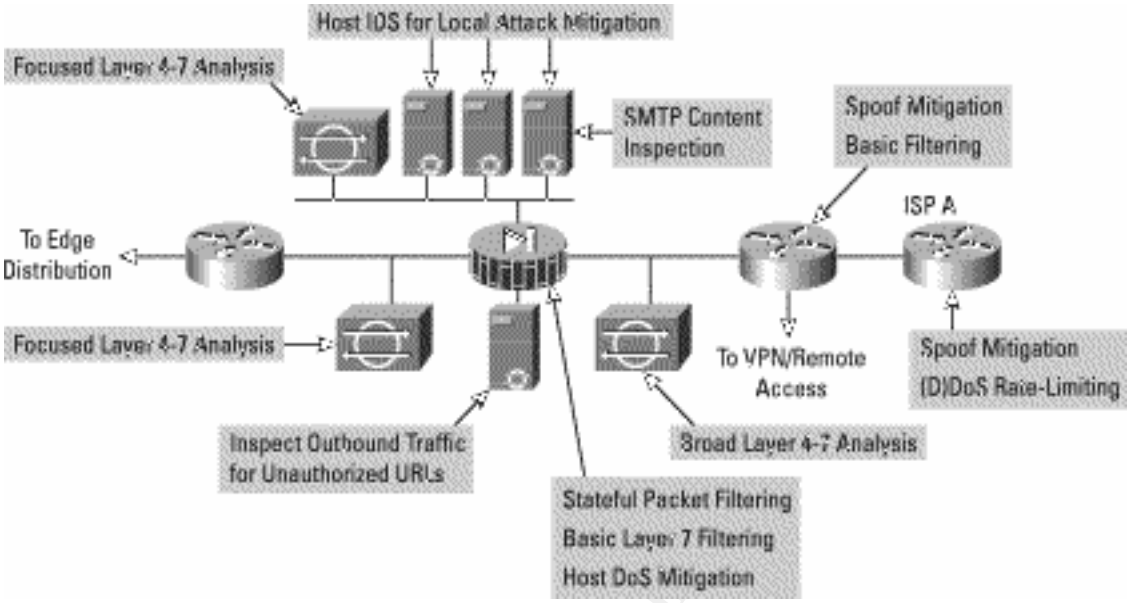

Figure 3. Attack Mitigation Roles for Corporate Internet Module
(Source: http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safe_wp.htm)

The attached infrastructure conceptual design (Fig.3) has been built-in with the security mindset.

- The ISP routers are configured for the anti-spoofing and DDos Rate-limiting
- VPN/ remote access and ISP routers are connected before the **Stateful Firewall** in the external DMZ with the basic filtering and spoofing built-in.
- **Network IDS** is focused on layer 4-7 analysis and spoofing built-in.
- URL filtering for outbound traffic, virus scans, caching are provided through the **Proxy Servers.**
- **Host Intrusion Detection Systems** (HIDS) are implemented into Web servers along with specific SMTP content inspection and anti-virus scanning.
- Intranet users are located in another side of **Edge Distribution.**
- **Server Security, Application/ Database Security and Desktop security** will also be discussed.

Stateful Inspection technology invented by CheckPoint Software Technology and has been widely adopted as the industry standard. "Stateful inspection" means it tracks and controls the flow of communication data passing through the firewall. It controls the decision to accept, reject, authenticate, encrypt, tunnel, NAT and/ or log the communication attempts. Through the internal processes of obtaining, storing, retrieving and manipulating the communication, any improper of access communication state will be rejected and only proper connection state is permitted and processed. By comparing the security protection techniques of "packet filtering", "application gateway" and "stateful inspection", it is no doubt that "stateful inspection" is an advanced powerful technique. Attached is a typical Stateful Firewall Load Balance configuration.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

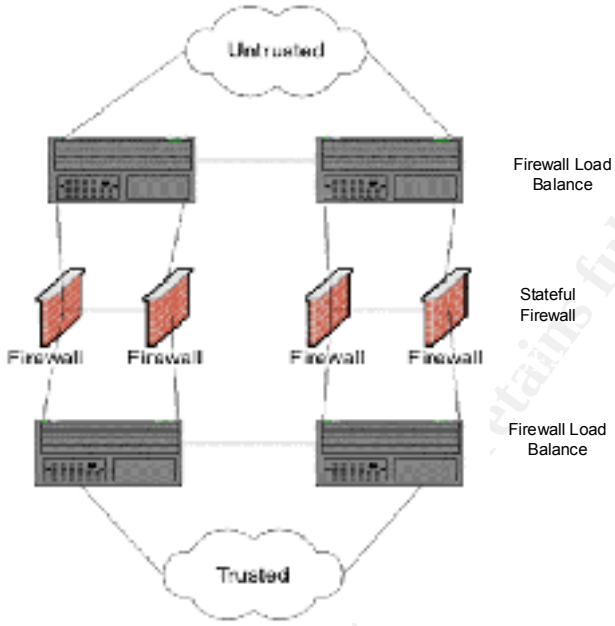

Figure 4. Active-Square™ Firewall Load Balancing
(Source: http://www.foundrynet.com/solutions/appNotes/ironShieldSecurity.html#1)

Network Intrusion Detection System (NIDS) is particular useful in complex network environment such as multi-layer access and control points. The sensors will be placed in different network segments for gathering the traffic status such as "external DMZ segment for monitoring the internet incoming/ outgoing traffic pattern", "internal DMZ segment for monitoring the intranet inbound/ outbound traffic", "web-server segment to monitor any abnormal traffic behavior or attacks." If a packet that is seen by an IDS sensor matches one of its signatures, the alert event will be sent back to the Central Console for severity classification and final analysis to see whether it is a hoax or real attack.

Proxy Servers provide a logical single access point between Intranet users and Internet services. Intranet users need to connect to Internet web service via the proxy server for port translation and access filtering. The advantages are to filter out any disallowed URL access, proxying the Internet and Intranet services, caching and the first point of anti-virus scanning. The mentioned capabilities can be add-on or built-in a single device. More functions are turned on; it implies more CPU processes required. At the time of product selection, the functionalities and performance are very important elements to be considered.

Host Intrusion Detection System (HIDS) is capable of real-time monitor traffic

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

analysis. Should there be any attack signatures detected, the system (HIDS) will send the alert messages to the central IDS console and other configured media such as paging, email, central NMS and so on. In this case, the HIDS is specially implemented to monitor the DMZ web server status. The firewall and packet filtering functions are managed by other components. Some off-shelf products are already combined the capabilities of packet filtering firewall, application firewall, and proxy service and intrusion detection together. These products are the excellent tools for protecting the user stations.

Edge Distribution provides the traffic aggregation from the various elements at the edge. Traffic can be filtered and routed from the edge modules into the core. For the network connections from the trusted network, the unnecessary firewall can be eliminated. For the network connections to the non-trusted network (VPN/ remote access), an additional separate firewall is sufficient because the traffic will be routed and governed by the web server firewall upon the 3-tier firewall employed.

Server Security - In network security protection, the enterprise web servers and core services (DNS, proxy, ftp and mail server) can fully be protected by two layers (3-tiers) Firewall protection. The typical Internet Firewall is one layer (2-tiers) for isolating the Internet and Intranet. The web servers and core services are normally installed within the internal DMZ and supported by packet filtering. By employing 3-tiers stateful firewall approach, the web servers are located between two sets of firewall. The Internet traffic needs to pass through the top firewall facing to Internet and the Intranet traffic has to route through the bottom firewall facing to private network. This solution will provide a solid inbound and outbound network security.

Application/ Database Security - the network security is hardened but we should not overlook the application and database security. The essential security protection such as anti-virus software, authentication, encryption, access control, and account administration should have been posted in the security policy and should be implemented & audited periodically.

Desktop Security - The general practice is any critical data should not be stored into the desktop station. No games should be loaded into the working PC. Unauthorized Internet download must be prohibited. These policies should be documented as a standard of security policy in each company. However, it doesn't eliminate the issue of virus and worms spread. Therefore the best effort is to build a solid foundation on your desktop station.

Anti-virus software is almost a must to be installed and needs to be updated periodically to ensure the update virus patches being installed. The anti-virus software will protect the client and server, disk media, files, and email-attachment to scan and eliminate any known virus.

Personal firewall installation is very arguable. If the company network is considered fully protected, should we need to spend the money for installing the personal firewall

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

in each desktop? Do the users know how to manage the firewall? I'd suggest being decided after the risk analysis. However, the portable and desktop stations will be connected to Internet through non-trusted network (i.e. DSL, cable modem or dial-up) that should install with the personal firewall. Some personal firewall products already provided the capabilities of packet-filtering, application-level IDS, stateful inspection and monitoring of signature attack.

Network & System Audit
Please be aware of the feedback loop, network and system audit is a critical process to ensure the proper security protection done and to find out any security holes left. It is the only way to keep enforcing the security strength by continuous improvement. Through the internal audit resource or employing the 3rd party is your choice.

5. Incident Handing

Incident Handling is a precautious preparation on how to deal with security impact to the company such as fire, flood, earthquake, malicious codes, virus and hoax information, cyber-theft, worm spread and so on. The following procedures will lead you through the complete security incident response. I posted the latest SNMP vulnerable as an example in the incident handling response.

1) *An emergency response team community should be pre-selected with their responsibility defined*.
   The contact list should include the primary and backup person's office, home, mobile and pager numbers. Their responsibilities in term of "network", "client/server", "firewall", "mail-group" and so on. The management contact list should include the relationship managers, individual business line CIO and ISS management committee.

2) *Verify the incident to determine a virus or hoax*
   Verification process is a very important part to ensure the right resources will be allocated. The source of information needs to be traced. In this case, it's acknowledged by several of major vendors of the impact to their products. The Information Security Officer forwarded an alert message to the Emergency Response committee members and invited a conference with a brief description of the SNMP vulnerabilities.

3) *Identify the real impact*
   Upon the incident confirmed that it is not hoax information. We need to understand the possible impact to networks, servers, applications or particular services. In the conference, the information security officer has clearly explained the impact. Whatever devices are managed by SNMP protocol will be impacted.

4) *Assign resource to deal with the technical focus*

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Enterprise service is assigned to determine the devices that are being managed by SNMP. The same effort is assigned to Network support. Besides, the external vendors' assistance was asked to give proper assistance when necessary. Upon the tasks assigned, a daily meeting was scheduled to ensure the proper follow-up and the progress of resolution.

5) *Define the resolution and prioritize the fix and resources*
The server end would need a patch to be installed and some vendors might not have the fix in next few days. It's the same as network equipment, particular OS upgrade was recommended but it would take time to complete. The top priority was assigned to ensure the perimeter routers being protected by access-list control. The rest of resolution issues will be taken action ASAP.

6) *Prevent the re-infection procedures*
Upon the OS upgrade and server patch implemented, there was a review how to avoid the re-infection. One of the tasks was to ensure no default SNMP community left in any network or server component. This will reduce the risk of attacks for any related SNMP issue.

7) *Establish the communication channels*
In order to avoid any uncertainty, the ISS incident in-charge should only inform the emergency response committee at the beginning of the incident handling. Upon the issue and resolution surfaced, at this time we need to keep user and management informed of the progress.

8) *Review the case and document any incident response issue.*
This is always a good practice to avoid the same mistake reoccurred. ISS should document the entire events, resolution methods, difficulties and follow-up items if any. The finalized document would be distributed within the committee members to ensure an agreed official case.

9) *Dry run*
If your company does not have any experience of incident handling. It would suggest managing a dry run to ensure the proper procedures and information in place. It certainly helps in case of any real situation occurs.

10) *Defense in depth security training and management support is also essential to the success of the incident handling.*

** Refer the cyber-attack to your local FBI office http://www.fbi.gov/contact/fo/fo.htm

6. Conclusion

No matter whether the business has driven the new technology or the breakthrough

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

technology has created the business, the chain-effect will allow a gap for the threat and vulnerability. To ensure a company to survive in the cyber-attack age, hardening the infrastructure is certainly one of the critical missions. Besides, we cannot overlook some key processes, such as risk assessment, security policy, system & network security audit and incident handling to enforce the complete and successful security protection. This is a cycle-effect that needs to be kept under continuous reviewing, updating and improving.

The more effective the cycle-effect be operated, the more efficient your infrastructure will be protected from the security threat and vulnerability.

References: -

1. Dr. Brewer, David "Risk Assessment Models and Evolving Approaches"
http://www.gammassl.co.uk/topics/IAAC.htm

2. eWeek "Best practice"
http://www.eweek.com/article/0,3658,a=20280,00.asp

3. SANS "Introduction to the SANS Security Policy"
http://www.sans.org/newlook/resources/policies/policies.htm

4. Cisco "SAFE Blueprint"
http://www.cisco.com/warp/public/779/largeent/issues/security/safe.html

5. Convery, Sean and Trudel, Bernie "A *Security* Blueprint for *Enterprise* Networks"
http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safe_wp.htm

6. Network Security: An Executive Overview
http://www.cisco.com/warp/public/cc/so/neso/sqso/netsp_pl.htm

7. Foundry "IronShield™ Security"
http://www.foundrynet.com/solutions/appNotes/ironShieldSecurity.html

8. Checkpoint "Stateful Inspection™ Firewall Technology"
http://www.sofaware.com/html/tech_stateful.shtm

9. Network Appliance "Case Study - Fast and Secure Web Access"
http://www.netapp.com/case_studies/hypovereins.html

10. Symantec Corporate Solution "Lower IT Costs through Better Ant-virus Management"
http://securityresponse.symantec.com/avcenter/reference/nvxwp2b.pdf

11. CERT Coordination Center "Incident and Vulnerability Trends"
http://www.cert.org/present/cert-overview-trends/cert-history-trends-2000-08-17.pdf

© SANS Institute 2000 - 2002 Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Last Updated: May 23rd, 2017

Upcoming Training

Click Here to {Get CERTIFIED!}

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
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
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 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	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	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