# Global Information Assurance Certification Paper

# A Security Manager's Review

*- of an on-line business's security design*

GIAC Security Leadership Certification (GSLC)

Practical Assignment

Version 2.0 (April 19, 2004)

Assignment Option:
Critique a GCFW network security design

Wade Dauphinee
Track 12 / SANSFIRE
Monterey, CA
July 6-10, 2004

Submission date:
13 DEC 2004

# Table of Contents

## Abstract

GIAC Enterprises is an eCommerce business that sells fortune cookie sayings to customers over the Internet. To protect the significant investment made in its on-line web portal, GIACE recently had a network security design prepared for it by a consultant. GIACE management has asked that this design be critiqued to ensure that it meets the requirements and balances the protection costs with the expected return on their investment. The remainder of this document will be spent performing that analysis.

## Executive Summary

The GIACE growth strategy is to harness information technology to streamline its business operations. As a result, a significant investment was made in an Internet facing web portal so that it can conduct efficient business dealings with its customers, suppliers, and partners. These parties must be assured that they will be able to securely, reliably, and efficiently utilize the GIACE web application for it to be successful and provide a return on the investment made.

To ensure that these requirements are met, the proposed network security design was critiqued. That analysis resulted in the following recommended improvements:

1) The current strong password policy should be technically enforced in the web application and operating systems. Since passwords are the primary protection against unauthorized access to GIACENET, this is considered a must-do improvement that is required to protect the integrity of the business. This improvement is estimated to yield a high return on the relatively small investment to be made.

2) Add redundancy to the GIACENET network infrastructure and systems assuming that the projected growth of the company warrants this fairly significant cost of protecting those sales. This is considered a should-do improvement that will help protect GIACE from a significant business interruption.

3) Create a vulnerability scanning program with a focus on the GIACENET portal application. Attackers will constantly be assessing the portal application for weaknesses that become exposed as a result of newly discovered vulnerabilities in the technology or configuration changes. Therefore, it only makes sense that GIACE perform these assessments regularly as well to find and fix vulnerabilities before they can be exploited. This is a should-do improvement that will provide additional protection against a significant business interruption. The returns realized from preventing a system exploit outweigh the investment required for this improvement.

4) Enhance the current threat monitoring capabilities by providing intrusion detection system (IDS) training to the new IDS staff and by implementing the Tripwire® change control software to monitor system changes. The investment required is small in comparison to the benefits that can be realized from the increased visibility and discipline it will bring to network and change activity. This is a should-do improvement that will help minimize system interruption and protect integrity.

5) Refine and test the existing incident escalation procedures and expand them outside of just the IDS staff. This is a should-do improvement that will help reduce business interruptions resulting from security incidents and ensure that the forensic evidence required for system integrity investigations is preserved.

# Technical Solution

The network security architecture proposed for GIAC Enterprises was designed by Bang Shuh Tan in the GIAC Certified Firewall Analyst practical assignment number 496 located at http://www.giac.org/practical/GCFW/Bang_Shuh_Tan_GCFW.pdf. The design is summarized in the categories that follow.

## *Virtual Private Network (VPN)*

The mobile work force and remote administrators connect to the company network through individual VPN connections, which extend from their remote workstation, through the Internet, and terminate on the external firewall. The VPN tunnel encrypts all data that is transmitted to prevent it from being seen by adversaries. VPN connection requests are challenged for credentials. Refer to the later network defenses section for further design details about how VPN users are permitted access.

## *Perimeter Defenses*

The border router and the external firewall form the first line of defense. Ingress and egress access control list filters are applied to the border router's interfaces, and the operating system of the router has advanced filtering capabilities. The border router's network based application recognition (NBAR) feature is utilized to prevent hard to filter peer to peer protocols and applications. The router's configuration is hardened according to best practices. The external firewall provides protection for the DMZ segment and the internal firewall. It also is used to challenge remote VPN connection requests for authentication and authorization. The firewall architecture is explained in more detail in the network defense section that follows.

## *Network Defenses*

The network is divided into five segments. Traffic is restricted between these segments by firewalls. The firewall access control list filters are designed on the principle of least privilege meaning that only the required network communication between systems is permitted. A brief description of each network segment's purpose follows:

- Demilitarized (DMZ)

The DMZ segment contains Internet facing systems that are required for interaction with public entities but need some level of protection.

- Management

  The management segment contains the systems that are used to centrally administer and monitor the infrastructure and systems.

- Restricted

  The restricted segment does not contain systems. It solely provides the link between the external and the internal firewall.

- Secured

  The secured segment contains the business's critical application and database systems.

- Internal

  The internal segment contains employee workstations and shared resources.

There are two firewalls, which provide a two tier defense from the Internet and restrict traffic between the network segments. The external firewall and internal firewall are different makes so that the internal firewall provides a second layer of protection should vulnerabilities be exploited in the technology of the external firewall. The external firewall provides protection for the DMZ segment from Internet connection traffic. It also provides protection for the internal firewall, which is connected to it through the restricted network segment. The internal firewall provides protection for the management, secured, and internal segments. Each firewall operating system and configuration is hardened according to best practices.

VPN connections are challenged for credentials by the external firewall. The external firewall forwards credentials it receives to an authentication, authorization, and accounting (AAA) server, which resides on the management segment. That server then tells the firewall if the credentials pass and, if so, what network resources it can grant the user access to according to what permissions are assigned to those credentials. The AAA server has two permission groups: the remote administrator and the remote user groups. The external firewall has two pools that it assigns network addresses from, one for remote administrator VPN connections and the other for remote user VPN connections. The access control lists differentiate between user and administrator VPN traffic based on these network addresses.

The switch that connects the systems on the DMZ segment has a feature called private VLAN. This feature is configured to protect the external web server, the

SMTP gateway server, and the proxy server. These servers have no requirement to communicate with each other. Therefore, the private VLAN feature of the switch has been utilized to protect each port that these servers are connected to. Since a protected port is not permitted to forward packets to another protected port, if one server is compromised the attacker can not use it to launch an attack against the other two.

The Windows based Active Directory domain controller on the internal segment, is used to authenticate and authorize users and workstations within the GIACE domain.

## *Host Defenses*

The external web server is hardened and installed in a change root (chrooted) environment, which means if an attacker is able to compromise the web server he or she would still have to try to get beyond the root set for the web server in order to reach the operating system files. [1]

Each server and network device's operating system and configuration is hardened according to best practices. Several Microsoft tools were used to automate the hardening of the Windows systems.

The Windows Domain Controller system is also the anti-virus intranet server, meaning that it connects regularly through the proxy server to the vendor's site and downloads the latest anti-virus signature files for internal distribution to the other systems. The Windows based workstations and servers, within the GIACE domain, connect to this server to update their anti-virus software with the latest signature files. The mail server also receives its mail security updates in the same manner.

Patch management of the Windows based workstations in the GIACE domain is architected in the same way as anti-virus. There is a Windows intranet server, on the internal network, that connects to the Windows Update site through the proxy server to download service packs and hot fixes for automatic internal distribution to the workstations. The Windows servers are updated manually so that patch changes are managed in a controlled fashion.

## *Application Defenses*

The external web server in the DMZ controls access to the GIACE web application server, which resides on the secured segment with unique usernames and passwords. Once authenticated, users are authorized to

access functions within the web application based on group membership. A user account is made a member of one of three role based access groups: the customer, supplier, or partner group. The external web server is a reverse proxy for traffic between remote web clients and the web application server. This prevents web clients from having any direct accessibility with the application server.

Only the external web server is trusted to access the application server on the secured segment. The web and application servers authenticate each other using digital certificates to establish the trusted connection.

## *Data Defenses*

In this tiered web application design, only one application level account is permitted to access the database server residing on the secured segment. The application account has only enough access to perform the functions against the database that are required by the application. No user level accounts are used to make connections to the database.

SSL is used to encrypt data in transit over the Internet between the web browser client and the web server. SSL is also used to protect communications between the external web server and the application server on the secured segment.

Secure Shell (SSH) encrypts the data over remote firewall administration connections.

The Terminal Services Remote Desktop Protocol (RDP) is configured to use high encryption to ensure the data over remote management connections is protected from end to end.

The data transmitted by the mobile work force and remote administrators is protected by the encrypted VPN tunnels it is sent through.

## *Resource Defenses*

A Simple Mail Transfer Protocol (SMTP) gateway server that resides in the DMZ is used to relay SMTP mail to the internal mail server. This protects the internal mail server resource from direct exposure to the Internet. The SMTP gateway application is hardened and installed in a chrooted environment.

A Proxy Server that resides in the DMZ is used to forward http and https requests for authenticated users and filter web content.

A split Domain Name System (DNS) architecture is used to protect against a compromise of that service that could lead to a mapping of the internal network. This architecture uses an external, Internet facing, DNS server and an internal DNS server.

A Microsoft Sharepoint portal server is used to grant VPN users access to files and resources in the GIACE domain rather than permitting NetBIOS traffic through the internal firewall. Sharepoint portal security features are utilized to restrict access.

The Simple Network Management Protocol service on the servers and network devices is configured to permit polling connections from the network and systems management server only. The SNMP community strings were also changed from the default.

Windows terminal services, which is used to connect to the management consoles is hardened and only administrators are assigned the user right to logon locally.

There is a 1 minute idle timeout set for SSH firewall connections. Access to all network devices is authenticated centrally by the AAA server.

## *Threat Monitoring*

To provide monitoring and notification of malicious network activity, an intrusion detection sensor is deployed on each of the three network segments that are considered critical to the operation of the business. These are the DMZ, secured and internal network segments. Each of the sensors sends their event logs to both a database for analysis and to a system log server for event notifications. The information in the database can be analyzed through a system running an analysis console. The system log server is running an application that watches the logs and generates notifications. The Linux and Solaris servers are also configured to log their critical events to the centralized system log server. The forward proxy server is running software to track web traffic of users. The anti-virus console is another source of information to monitor for threats such as macro-viruses [2]. The intrusion detection network sensor operating systems are hardened according to best practices.

## Agreement

One way to gauge the effectiveness of a network security design is to determine what other layers of protection it provides in the event that malicious code penetrates the perimeter defenses. The Computer Security Institute and FBI's 2004 Computer Crime and Security Survey reported that the most reported type of attack by respondents was malicious code or virus related attacks. [3] In this design, the other network, host, application, data and resource defense layers offer protection. This is truly a defense in-depth design that gives GIACE the protection it requires to conduct business over the Internet. The following are specific observations to support this opinion. These observations are grouped by prevent, detect or response type controls to demonstrate that all three have been considered.

*Preventative controls:*

- The border router has ingress and egress filters, which will prevent malicious code from initiating any communication or downloads to the Internet.

- Network segmentation and firewalls compartmentalize GIACE's network to contain malicious code in the event one segment were to be penetrated. Access to network resources is based on the principle of least privilege.

- There is an enterprise anti-virus implementation that keeps signatures up to date on systems and protects the mail server by filtering malicious attachments.

- There is an automated solution to keep workstations patched, and servers are kept patched through a managed release process. This eliminates known vulnerabilities that malicious code normally takes advantage of.

- Best practice hardening guides were used to standardize the security configurations of its systems making them less susceptible to penetration by malicious code.

- A forward proxy server is used to enforce acceptable use of Internet resources through web traffic filtering. This, again, helps contain malicious code from being able to reach inappropriate or known malicious web sites.

*Detection controls:*

- An IDS system and staff have been implemented to ensure signs of intrusion or anomalies that would indicate malicious code are quickly

detected and responded to.

- The forward proxy server also monitors web traffic, which helps in the detection of malicious code.

- The anti-virus console and system log server also serve as intrusion detection sources.

*Response controls:*

- GIACE has incident escalation procedures established in the event a security incident is detected, such as a malicious code outbreak.

In addition to the above controls, GIACE has the following encryption and password controls to help protect the confidentiality of its fortune sayings and the integrity of its systems:

- SSL encryption is used to protect the GIACENET portal application data in transit.

- A strong password policy was adopted for the external portal application to prevent unauthorized access.

## Disagreement

It is clear that availability is GIACE's most important security requirement as seen by the 7X24 requirement for their GIACENET web portal. Any system down time will directly translate to lost revenues. However, the current non-redundant network architecture is not designed to meet that availability requirement. The GIACE network is connected to only one Internet Service Provider (ISP). A failure of that ISP connection would mean the business's on-line presence would become unavailable to its customers, partners, and suppliers, which would directly affect their bottom line. Additionally, each system and network device that is a component of the GIACENET and GIACEINT portal solution is a single point of failure. Mr. Tan provides a recommendation to enhance the existing design with a redundant and high availability design on page 112 of his practical assignment.

The internal private IP addressing scheme uses obvious private address networks like 192.168.1.0. This could result in conflicts with the remote networks of employees connecting via VPN. This may also prove to be especially problematic if GIACE continues to grow and decides to interconnect other offices.

Although GIACE seems to have some level of change management in place, as evidenced by how they handle implementation of server patches, they do not have a change control system to monitor for unauthorized changes. Good operational security practices suggest that you should be aware of all changes to your critical infrastructure and systems, treating any unauthorized change as a security incident. [4] Change control cannot be on the honor system at GIACE if it is to meet its 7X24 availability requirement for the web application.

Overall though, I thought Mr. Tan's design was very well done and I have no other disagreements with it.

## Improvements

The following is a listing of the potential improvements to the GIACE security design that were considered before any in-depth analysis and prioritization.

- Use networks at the upper end of the reserved IP address space blocks for private networks rather than the obvious network ranges it is using now. [5]

- GIACE should consider a second Internet connection from a different ISP. This will mitigate the risk of their web portal application becoming unavailable in the event their current provider experiences network problems and is unable to provide connectivity.

- Redundancy should be added for the critical network devices and servers that are currently single points of failure in the GIACENET system.

- Since GIACE depends highly on its Internet presence, they should look at taking all the precautions necessary to protect its Internet domain name. One such precaution is checking the whois domain name database to ensure that their name is not due to expire soon and that all the contact information is accurate.

- Although GIACE has incident escalation procedures established, it was indicated that they need to be refined by the IDS staff. This response plan should be further developed and tested by having a facilitator present the team with potential incident scenarios.

- Implement Tripwire® change control software on the critical network devices and external web portal systems to detect unauthorized changes. Have a separate group or change manager monitor for unauthorized changes. Make detection of an unauthorized change a security incident.

- Implement a vulnerability scanning program. Microsoft Baseline Security Analyzer (MBSA) was used at implementation to scan the Windows based servers. Likewise, the network mapper (nmap) tool was used to test the firewall rules. However, this type of vulnerability scanning activity must be a regularly scheduled activity and incorporate the other critical components of the system. A web application scanner should especially be investigated to test the GIACE web portal application for vulnerabilities that could be exploited by an attacker.

- GIACE's anti-virus software should be investigated to ensure that it includes a malware scanner, activity monitoring, and file and resource integrity checking since malware accounts for more compromises than hackers.

- The current IDS staff is new to intrusion analysis. These staff members should be provided with intrusion detection training like that provided in the SANS Institute's intrusion detection in-depth track.

- GIACE management is aware of the dangers associated with e-commerce and has supported the measures taken to improve their security posture. However, this support should be documented in a GIACE security program policy that can be communicated in order to set the tone for the entire organization that security controls are an important part of GIACE's strategy to meet its business goals. This will provide direction for compliance with the technical security policies, requirements and standards established for GIACE by Mr. Tan.

- Security awareness training should be provided to the GIACE staff to protect against accidental disclosure or interruption of services due to non-compliance with established security policy and standards.

- GIACE's business is highly dependant of the availability of its technology. As a result, it should establish a team to lead the business continuity process planning lifecycle.

- It is not clear if GIACE is able to structurally enforce its strong password policy. If it does not, I would recommend that it make that modification to its portal application as well as enforce it through Windows and Linux password policies. I also recommend that they obtain a password auditing tool to regularly check and enforce compliance to the policy. I recommend that GIACE consider adding a two factor authentication solution, such as RSA's SecurID, to its radius authentication for VPN connections.

- GIACE should configure the content monitoring system, on its forward proxy server, and the network based IDS sensors to inspect traffic for confidential information leaving its network. GIACE's confidential information includes its fortune cookie sayings as well as its list of customers, suppliers and partners.

- GIAC has a mobile sales force, teleworkers and remote administrators. I recommend that these staff use some form of encryption software, such as Pretty Good Privacy (PGP), to encrypt the sensitive files stored on their laptops, which are accessed infrequently. This will ensure that GIACE's confidential information is not disclosed in the event these remote machines get stolen or compromised. PGP software should also be used by employees to protect sensitive email transmissions.

Each potential improvement was then analyzed against the assumed feasibility, organizational constraints, and the level of risk posed to the organization's

critical assets. The critical assets were considered to be GIACE's most important assets that would cause the company large adverse impact if something happened to them. [6] The critical assets were determined to be:

- The fortune cookie sayings because it is the product that generates their revenues.
- GIACE's customer, supplier and partner information since this would be valuable information to a competitor.
- The Internet connection since it provides the only way for this eCommerce business to sell its products to customers and interface with its partners and suppliers.
- The GIACENET external web portal system because it serves as the company's storefront to its customers, partners and suppliers.
- Its Internet Domain name because that's how its presence is found on the Internet.

The top five improvements that directly contribute to the protection of the above critical assets were then selected to have a total cost of ownership (TCO) and return on investment (ROI) analysis performed on them. These five areas for improvement are:

1) Add redundancy and high-availability to the network infrastructure and systems.
2) Create a vulnerability scanning program with a focus on the external web portal application.
3) Technically enforce the GIACE strong password policy in the web application and operating systems.
4) Enhance the threat monitoring capabilities by:
   a) Implementing the Tripwire® change control software to monitor changes to the critical systems and network devices
   b) Providing IDS training to the new IDS staff.
5) Refine and test the existing incident escalation procedures and expand them outside of just the IDS staff.

Each improvement's TCO and ROI calculation that follows demonstrates why it should or should not be considered for implementation at this time.

## *Add redundancy and high-availability*

### TCO Calculation

Direct Costs

- Hardware costs of:
  - A second border router
  - A secondary PIX firewall
  - A secondary Checkpoint firewall server
  - A secondary Cisco catalyst switch for the DMZ
  - 6 additional Cisco catalyst switches for the high availability design
  - A load balancer device bundle to front end the external web portal application servers
  - The redundant servers for the external web, database and application servers

- Software costs of:
  - The Checkpoint software for the secondary firewall
  - The Operating System and application software required for the redundant GIACENET servers.

- Maintenance costs for:
  - The redundant network equipment.

- Other costs such as:
  - The cost of a second Internet connection
  - The cost of transferable public TCP/IP address space

Indirect Costs:

- The rack space and power required for the additional equipment.

Depreciation Costs:

- The depreciation costs of the hardware and software purchases with the hardware costs being the most significant.

Implementation Costs:

- The project planning cost. A project manager will most likely be required to plan and schedule this implementation.

- The resource and professional service costs required to install and configure the redundant network devices and servers. I would estimate this cost to be quite significant considering the expertise required.
- The cost of testing the infrastructure and application post implementation.

Training Costs:

- The cost of training the administration staff to support the technologies and configuration required for high availability mode.

Ongoing Management Costs:

- The cost to manage and monitor the additional infrastructure and servers to be added.

Decommissioning Costs:

- The cost to remove the equipment and wipe the disks and configurations.

### ROI Calculation

The ROI is the estimated cost savings of the sales that would be lost due to a network outage less the costs described above in the TCO calculation then divided by those costs and multiplied by 100.

### Recommendation

The final recommendation is to implement the redundancy and high availability improvement assuming that the projected growth of the company warrants this cost of protecting those sales. This is considered a should-do improvement that will help protect GIACE from a significant business interruption.

## *Create a vulnerability scanning program for the web application*

### TCO Calculation

Direct Costs:

- The hardware costs of a machine that meets the minimum system requirements of the scanning software applications.

- The software costs of a web application scanner and a vulnerability scanner that is able to scan both Windows and Linux systems.

- The maintenance costs of the vulnerability scanner applications.

Indirect Costs:

- The cost of additional space and power for the management console machine.

Depreciation Costs:

- The depreciation costs of the scanner hardware and software.

Implementation Costs:

- The initial implementation and configuration costs of the vulnerability scanning software tools.
- The cost of developing the vulnerability scanning process and documentation.

Training Costs:

- The cost to train resources how to use the vulnerability scanning software to properly analyze and detect the application and systems weaknesses that could be exploited by an attacker.

Ongoing Management Costs:

- The costs of the ongoing manual review of the vulnerability scan reports.
- The cost of regularly updating the vulnerability scanning software.
- The cost associated with the ongoing tuning of the vulnerability scan policies.
- The ongoing review and maintenance of the vulnerability scanning process documentation.

Future Integration Costs:

- The cost of the additional vulnerability scan software licenses required to scan new systems or web applications that are added over time.

Decommissioning Costs:

- The cost to dispose of the vulnerability scanner hardware and degauss the hard drive.

## ROI Calculation

The ROI is the estimated cost savings from preventing system downtime and integrity loss as a result of an attacker exploiting a weakness in the web application, less the costs described above in the TCO calculation then divided by those costs and multiplied by 100. There may also be a return in the form of higher sales if customer confidence in the web application increases as a result of this mitigation activity.

### Recommendation

The final recommendation is to implement this improvement. This is a should-do improvement that will provide additional protection against a significant business interruption. The returns realized from preventing a system exploit outweigh the investment to be made.

## *Technically enforce the GIACE strong password policy*

### TCO Calculation

Implementation Costs:

- To design, develop, configure, and test the necessary code changes within the web portal application as well as the policy enforcement within the operating systems.

Training Costs:

- To train the help desk staff to support the calls that will result from users being forced to enter a strong password.
- To conduct awareness seminars and communiqués about the reasoning behind and importance of selecting a strong password.

### ROI Calculation

The ROI is the estimated cost savings from preventing the theft and integrity damage that an unauthorized party could cause by logging in with compromised credentials, less the costs described above in the TCO calculation then divided by those costs and multiplied by 100.

### Recommendation

The final recommendation is to implement the strong password enforcement improvement. This is a must-do improvement that GIACE requires to protect its integrity. The improvement is estimated to yield a high return on the relatively small investment to be made.

## *Enhance the existing threat monitoring capabilities*

### TCO Calculation

Direct Costs:

- The hardware costs of implementing a dedicated machine for a Tripwire® management console.
- The cost of the Tripwire® software to be installed on the critical servers and network devices.
- The maintenance costs of the Tripwire® software.

Indirect Costs:

- The cost of additional space and power for the management console machine.

Depreciation Costs:

- The depreciation cost of the Tripwire® software and the management console hardware.

Implementation Costs:

- The initial implementation and configuration costs.
- The cost of developing the change control process and documentation.

Training Costs:

- The cost of training for the IDS staff since they are new to intrusion detection.
- The cost of Tripwire® training.

Ongoing Management Costs:

- The cost to the ongoing manual review of Tripwire® reports and events.
- The cost of regularly updating the IDS and Tripwire® software.

- The cost associated with the ongoing tuning of the IDS and Tripwire® policies.
- The ongoing review and maintenance of the system and process documentation.

Future Integration Costs:

- The cost of the Tripwire® agents required for any additional critical servers and network devices that are added over time.

Decommissioning Costs:

- The cost to dispose of the management console hardware and degauss its hard drive.

### ROI Calculation

The ROI is the estimated cost savings from preventing system downtime and integrity loss as a result of an undetected change or intrusion, less the costs described above in the TCO calculation then divided by those costs and multiplied by 100.

### Recommendation

The final recommendation is to implement this improvement to GIACE's existing threat monitoring capabilities. This is a should-do improvement that will provide additional protection against a significant business interruption. The investment required is small in comparison to the benefits that can be realized from the increased visibility and discipline it will bring to network and change activity.

## *Refine and test the existing incident escalation procedures*

### TCO Calculation

Direct Costs:

- The hardware required for any incident response forensic equipment such as a laptop and external hard drive for drive copying and evidence collection.

- The software required for the response kit such as an operating system license for the laptop or commercial forensics software.

- The maintenance costs for any commercial software tools purchased for the response kit.

Depreciation Costs:

- Of the hardware and software purchased for the response kit.

Implementation Costs:

- The time required to further define and document the incident escalation processes, checklists and templates.
- The cost to test the defined incident escalation processes and tools.

Training Costs:

- The cost of training the required response resources on the incident escalation process.
- The cost of specialized training for the staff in incident response and forensic readiness.
- The cost of awareness training for staff and external parties to inform them about how to properly report a security incident.

Ongoing Management Costs:

- The cost associated with the time required for ongoing response team meetings and preparation activities.

## ROI Calculation

The benefit of this improvement are the estimated cost savings from reduced downtime in the event of a security incident, as well as, the savings from preventing a loss of integrity by having the ability to quickly determine and respond to the root cause of a security incident.

The ROI is the above benefit less the costs described in the TCO calculation then divided by those costs and multiplied by 100.

## Recommendation

The final recommendation is to implement this improvement to GIACE's existing incident escalation procedures. This is a should-do improvement that will help reduce business interruptions resulting from security incidents and ensure that the forensic evidence required for system integrity investigations is preserved.

## Conclusion

I believe that the network security architecture proposed by Mr. Tan meets the security requirements of GIAC Enterprises. It is a well thought out technical design that layers security to protect the company's substantial investment made in the GIACENET web portal. The five improvements recommended in this proposal will build on that secure design to give GIACE management assurance that its critical assets are protected. I believe that the design represents a strategic investment in security by providing the right amount of protection to those assets that are critical while not overprotecting those which are not.

# References


1) Zdziarski, Jonathan A. “Chrooting Daemons and System Processes HOW-TO” 19 Oct 2002. URL: http://www.securiteam.com/securityreviews/6K00F2K5PA.html (20 Nov. 2004)

2) Cowan, Crispin. “Avoiding Macro Viruses” URL: http://www.sans.org/resources/macro.htm (05 Dec. 2004)

3) Robert Richardson, Lawrence A. Gordon, Martin P. Loeb, and William Lucyshyn. “2004 CSI/FBI Computer Crime and Security Survey” 10 Jun 2004. URL: www.gocsi.com (11 Dec 2004)

4) Kevin Behr and George Spafford. The Visible Ops Handbook: starting ITIL in 4 practical steps Eugene: ITPI, June 2004

5) Rekhter, Y. “RFC 1918 – Address Allocation for Private Internets” Feb 1996. URL: http://www.faqs.org/rfcs/rfc1918.html (04 Dec.2004)

6) Christopher Alberts and Audrey Dorofee. Managing Information Security Risks: The OCTAVE Approach Boston: Addison-Wesley, June 2002

7) Northcutt, Stephen. SANS Security Leadership Essentials for Managers Bethesda: The SANS™ Institute, July 2004