Global Information Assurance Certification Paper

Table of Contents 1
craig_blaha_gslc.doc 2

Building an Effective Information Assurance Program for a Small Business

By: Craig Blaha

Date Submitted: Thursday, December 16, 2004

Building an Effective Information Assurance Program for a Small Business 1
By: Craig Blaha 1
Date Submitted: Thursday, December 16, 2004 1
Section 1: Executive Summary 3
Section 2: Description of Original Solution 4
Architecture 4
Zone 1 4
Zones 2 and 3 5
Addressing Scheme 5
Authentication, Authorization and Access 5
Auditing, Disaster Recovery and Business Continuity 5
Audiences 6
General Public 6
Customers 6
Suppliers 6
Partners 6
Internal Employees 6
Sales Force 6
Section 3: Points of Agreement 7
Section 4: Points of Disagreement 8
Cost 8
Technical Recommendations 9
Section 5: Improvements 10
Business Overview 10
Assets 10
Scalable Solution 11
Threats 11
Risk 12
Total Cost of Ownership 13
Cost Benefit Analysis 17
Return on Investment 18
Improvements to the Original Proposal 20
Step 1: Defining the Threat 20
Step 2: Creating the Security Policy 21
Step 3: Create the Policy Infrastructure 22
Step 4: Consider Outsourcing 22
Step 5: Technical Improvements 24
Section 6: Conclusion 28
References 29

Section 1: Executive Summary

This paper is a critique of Robert Huber's GCFW practical exam (http://www.giac.org/practical/GCFW/Robert_Huber_GCFW.pdf) submitted on May 15, 2004. The assignment for Mr. Huber was to design the security approach for a fictional fortune cookie company, called GIAC Enterprises. In this paper I summarize Mr. Huber's suggestions, point out the strengths and weaknesses, offer improvements, and define some resources that can be directly translated into an effective presentation for persuading upper management of the need for security.

Moving GIAC Enterprises from a more traditional, single point of sales enterprise to a company whose sales, service, and interaction with suppliers relies primarily on web applications will significantly increase opportunities for growth. Not only will the sales force be able to access the home office remotely, cutting down on order fulfillment time, production costs can also be lowered through automated processes and workflow, and GIAC can reach a broader audience and leverage customer relationship management opportunities that are not currently available.

The benefits of all of these real and potential gains come at a cost; both in dollar costs for infrastructure and personnel, and in increased risk. Anytime mission critical information is exposed to the web, a company opens itself up to a litany of threats. Everything from malicious hackers actively trying to infiltrate the business and steal financial or personal information, to increased possibilities for internal espionage or sabotage, to un-intentional internal threats created through inadvertent data corruption or a user's computer infected with the latest virus.

These threats are varied and continually increasing in both frequency and incidence response cost. The goal of the security plan presented in this proposal is not to mitigate every risk or to ensure that no threat will ever be realized. The goal is to balance mitigation of these risks with the mission, budget and growth opportunities of GIAC enterprises. In order to strike this balance, this proposal has been written with the bedrock principles of security in mind – Data Confidentiality, Integrity and Availability (CIA)[1]. These principles help to identify the assets we are trying to protect, the vulnerabilities in the protection scheme, and the threats posed to those assets both within the company and from the public at large, in order to determine the level of risk.[2]

This proposal takes that risk level and recommends ways to reduce, transfer, or in some cases accept the defined risks.[3] This plan is based on the concept of defense in depth, building mission driven security through components of policy, technology and technical best practices, and user awareness and education. This three pronged approach helps to ensure that GIAC is implementing effective security measures that are cost effective, that facilitate the continued growth of the company, and that are flexible enough to adapt to the continually evolving threats faced by every corporation that does business on the web.

Section 2: Description of Original Solution

Architecture

The network architectural design presented by Robert Huber on May 15, 2004 in his GCFW practical exam (http://www.giac.org/practical/GCFW/Robert_Huber_GCFW.pdf) divides the GIAC enterprise into 3 zones, and access requirements are separated by audience type; general public, sales force and remote workers, customers, partners and suppliers.

Traffic to the different network zones is controlled through a series of security mechanisms layered together to create a “defense in depth” approach to security. This approach appropriately separates the internal network into zones – the demilitarized zone which contains the web, smtp and DNS servers, and the internal network, which contains two VLANs, one for internal employees and one for the server farm. Each zone is surrounded by network based intrusion detection systems. Mr. Huber’s recommendation requires GIAC to centralize on one vendor, CISCO, to limit the range of staff expertise required to maintain these devices.

Access to GIAC internal network resources is controlled first by an internet facing Cisco 1721 border router. This allows GIAC to reject any non-business related traffic at the gate. This border router is followed by a Snort network based intrusion detection system. A Cisco Pix firewall controls traffic at this point, using three ports, one each for the internal network, the DMZ and the internet. Placing the firewall after the border router reduces the load on this device, and enables GIAC to screen the type of traffic traveling from any one network segment to any other. The intrusion detection capabilities of the Cisco Pix firewall are routed to the syslog server, to be combined with the 3 Snort network based IDS’ for traffic analysis.

Zone 1

Zone 1, or the Demilitarized Zone (DMZ), contains the web, DNS and SMTP proxy servers. It is accessible after passing through another network based IDS. All of the servers in the DMZ will be running RedHat Linux on Intel based hardware. These servers will be hardened using the Center for Internet Security Linux Benchmark. Each server will have TCP Wrappers configured, and ssh will be enabled to allow access only to known hosts from the 2 internal VLAN’s. Each server will also have tripwire installed.

The SMTP relay server will bring mail to the exchange server. The DNS server will run Bind, and zone transfers will be limited to suppliers, partners, and the upstream ISP. The web server will be running apache and open ssl, only allowing connections on TCP ports 80 and 443. Connection to the internet will be via sqlnet.

Zones 2 and 3

The internal network is also routed off of the Cisco Pix Firewall. The server farm and internal users are placed behind another IDS followed by a Cisco 3550 router. A Cisco 2950 switch separates the internal users, VLAN 1, from the server farm, VLAN 2. Five servers will be placed in VLAN 2, the exchange server, database server, syslog server, domain controller, backup server and AAA server. All will be hardened, include TCP Wrappers and a banner.

Addressing Scheme

The addressing scheme is broken down into two sections – internal private and public. The internal private is proposed as following RFC 1918 and setting 10.0, an internal class C. The 2 VLAN's will use separate ranges, with distance between the two ranges to allow for growth. Internal users on VLAN 1 will use 10.1.1.0/24 and VLAN 2 used for the servers will range from 10.129.1.0/24. Port security will require manual addition of new machines. The DMZ uses RFC 1918 192.108.1.0/27 and the public class c address space 2.20.20.0/24 for publicly addressable devices.

Authentication, Authorization and Access

Physical access to the consoles will be controlled. The level and mechanisms of control will need to be clarified as part of a site review. Authentication will be achieved through the AAA server authenticating either to TACACS+ or RADIUS. Authorization will be accomplished through AAA to TACACS. The DMZ uses access control list based on IP address to control access. Two factor authentication will be used for console access, and ssh will be used to access DMZ devices. Timesynch will be achieved through network time protocol server, using timestamps. Passwords will be stored encrypted. Each Snort IDS will have 2 network interfaces – one to monitor the network and one to manage the device using IP connectivity. These devices will not have an IP stack and will monitor the network using passive taps.

Auditing, Disaster Recovery and Business Continuity

Backup tapes stored on site and switched nightly. Monthly vulnerability assessments will be done using NMAP to look for active IP address from an employee's home over a DSL or faster internet connection. Nessus will then be used to scan these active IP addresses for vulnerabilities. The resulting vulnerabilities will be handed over to management in a report. Internal servers and workstations will be assessed in the same manner, but from inside the internal VLAN. An initial assessment of the secure web portal will be performed by an external vendor to ensure adequate protection against SQL injection, cross site scripting and other common attacks, as well as inadequate data integrity checking and verification.

Audiences

General Public

The general public requires view access to the GIAC fortune cookie web site. This access includes information on ordering instructions, description of products and services, contact information, and a link to the secure portal.

Customers

Prospective customers will be able to fill out a form and submit a request to create an account. This request will go through an approval process which requires a GIAC staff member to review the submission and manually create the account. Prospective customers will not have unapproved access to the GIAC secure web portal, and will not be able to submit orders via the web until their account has been created.

Suppliers

Fortune Cookie authors are considered the suppliers in this proposal, and they require access to the secure web portal in order to submit fortune cookie sayings for approval. These submissions will also be approved manually by an internal GIAC staff member, at which time they are moved to a production table in the database. Suppliers will not have direct access to the production database.

Partners

Partners supply translation services as well as printing services. For translation services, approved fortune cookie sayings from the production table will be downloaded to the partner via the secure portal, translated and uploaded back to GIAC via VPN. Printing services will be handled in a similar fashion except that specific orders will drive the print process.

Internal Employees

Some Internal Employees require access to the server farm and the internet in order to conduct their business. There are 15 internal employees running windows 2003 with a required login that includes an acceptable use banner. Internal employees sign an acceptable use policy and undergo security awareness training.

Sales Force

The sales force requires access to the internet, as well as VPN access to internal network resources. They are also running windows 2003 with a required

login that includes an acceptable use banner, and are required to sign an acceptable use policy and undergo security awareness training.

Section 3: Points of Agreement

The basic theories behind this design are sound – creating defense in depth via layering of different technologies, separation of assets using virtual local area networks, and separating high target areas such as the web server using a demilitarized zone. The initial proposal also includes efforts to limit cost using open source where possible and basing infrastructure decisions on widely accepted technologies, such as Cisco hardware. The suggestion of using a VPN is a good idea to get remote workers to access network. I also agree with need for policies such as acceptable use, banners with warnings, change management policy and process, as well as Mr. Huber's suggestion to outsource the initial vulnerability assessment to a third party.

An important suggestion in Mr. Huber's work is to include anti-virus, a firewall and anti-spyware on each host. The suggestion of using the Norton product which combines these tools and updates locally if available or remotely if necessary is an important step in ensuring the other layers of defense in depth are not undermined by weak security from within.

Mr. Huber also discusses the need for security training for all employees on an annual basis. This is an important cornerstone of any good security program, since many of the threats faced in information technology today, such as viruses spread through email attachments, can be averted through user awareness and common sense approaches to security.

Specifically, the following items make sense in the GIAC environment:.[4]

1. Switches
    a. Using Switches instead of hubs increases the complexity of gaining unauthorized access to network traffic, and it allows network administrators to disconnect problem hosts or sections of the network more easily. Some switches also allow system administrators the ability to limit access at the port level as well as restrict options, which helps limit the addition of unauthorized hosts.
2. Firewalls and Network Address Translation
    a. Firewalling Critical Systems
        i. In this proposal, critical systems are placed behind a firewall, with a border router facing the internet. The benefit of this approach versus an internet facing firewall is the number of services allowed through the firewall is limited, reducing the overall management load.

b. Departmental Firewall/NAT

    i. Network address translation is one way to limit an attacker's ability to perform reconnaissance of the network. Since only one IP address is sent out to the internet to represent GIAC enterprises, the services and setup of the internal network is more difficult for an attacker to discern. NAT should be deployed with logging for accountability and troubleshooting purposes.

3. Centralized System Logging

    a. Sending system logs to a central server is one way to limit the possibility that these logs will be modified by an intruder to cover their attack.

4. Virtual Local Area Network (VLAN)

    a. VLAN's are a cost effective way of increasing the layers of defense by separating the internal network into more manageable segments. VLAN's also allow for different access control rule sets, so, for example, the internal users VLAN may allow outbound traffic but denies inbound connection attempts, limiting the paths of attack.

Section 4: Points of Disagreement

I disagree with Mr. Huber's recommendations in one fundamental area – the cost of his proposed solution is not manageable within the scope of the GIAC budget. There are also a few technical points that I disagree with completely which I list in this section. Others are covered in the improvement section since the initial idea is sound, but I recommend a different approach.

Cost

The basic premise is problematic – given limited resources, a small company should consider outsourcing parts of their technical infrastructure such as monitoring and responding to the IDS and web hosting of the basic company web page. Adding a web site and web order capabilities adds 2 staff positions at a minimum, in addition to hardware and software purchases and maintenance. Sharing liability by hiring an outside vendor will greatly benefit the company. A clear example of the justification for outsourcing is the cost of 1 IDS for one year = 4% of total potential annual revenue of GIAC, an unacceptable level given the recommendation to implement 3 separate IDS's as only one part of the total solution.

The proposed solution does scale well, but the up front cost on the lower end of growth is significant and could interfere with sustainable growth.

Assessment of Security investment:

Overall cost of hardware and software	
Cisco 1721	$1695
Cisco Pix 515e	$5300
Compaq DL 380	$3200
Cisco 2950 Switch	$2500
Cisco 3550 Switch	$2500
TripWIre Software	No purchase cost
Snort 3	No purchase cost
NMap	No purchase cost
Nessus	No purchase cost
External assessment of initial web application security	~$5000
Existing Infrastructure	
Syslog server	No Additional Cost
Database server	No Additional Cost
Backup server	No Additional Cost
Active directory	No Additional Cost
Mail server	No Additional Cost
Overall cost of staff	
Webmaster[5]	$70,000
IS Security Manager[6]	$90,000
Three year Cost of Proposal	$500195
Annual Cost	$166,731.66

The above spreadsheet illustrates the fact that the proposal, not including all of the acquisition costs such as planning and vendor negotiation time, excluding training, implementation and "grave" costs, amounts to approximately 8% of the total *potential* revenue of GIAC. Unless GIAC has stated plans of moving from the fortune cookie industry into the general cookie industry, which would increase the total potential revenue significantly, the 8% or higher annual investment on security is difficult to justify.

Technical Recommendations

There are a number of technical recommendations which can be improved. Over the past year, we have seen monthly reports on the vulnerabilities of Microsoft operating system, Outlook email and Internet Explorer[7]. Any security recommendation should start with eliminating as much of the Microsoft suite as possible. While this may be a difficult move to make politically, a small company stands the best chance of implementing this recommendation, and stands to gain the most by minimizing their exposure to the ongoing cycle of patching, updating and responding to incidents that is common at Microsoft based shops. If the Microsoft operating system and office suite are embedded in the company's culture and workflow, the simple step of changing to Thunderbird and Firefox, Mozilla based email and browser, respectively, severely limits the company's exposure to vulnerabilities.

Any good security program must also start out with a solid security plan, one that is endorsed by upper level management. "The LAN security policy should stress the importance of, and provide support for, LAN management. LAN management should be given the necessary funding, time, and resources. Poor LAN management may result in security lapses. The resulting problems could include security settings becoming too lax, security procedures not being performed correctly or even the necessary security mechanisms not being implemented"[8]

Section 5: Improvements

Business Overview

In order to arrive at specific recommendations for improvement, an overview of GIAC from a business standpoint is necessary. This business overview will discuss the tools necessary to determine whether or not the technical recommendations offered by Robert Huber are fiscally sound and make sense for a small company like GIAC Enterprises.

I will start by describing GIAC, defining the assets that we are trying to protect, the vulnerabilities and threats that are involved and the resulting risk level. At that point I will discuss the concept of total cost of ownership, including cost benefit analysis, return on investment and a method to measure return on security investment.

Assets

Defining assets is an important first step because in order to determine whether a particular solution is appropriate, we need to know the value of what we are trying to protect. Assets include both gross income and the potential income over the next few years that would be threatened if a company's competitors

gained trade secrets or business strategies, or if business partners had their economic data compromised through a breach in the company's system. This type of compromise would not only include the cost to clean up and correct, but the intangible cost of damage to the reputation and the level of trust. For a company that is grossing $50 million per year, the immediate and long term effects of an incident are obviously much higher than if the company is grossing less than $1 million per year.

Assets include not only gross and future revenue, but customer data, fortunes, order information, staff, HR, payroll and business intelligence data (processes, expansion plans, internal memo's and e-mail), and intangible items such as reputation and perception of confidentiality and business security with partners.

After identifying the assets that we are trying to protect, the next step is to determine the value of those assets. Some of the components in that valuation process are[9]:

- The initial and ongoing cost (to an organization) of purchasing, licensing, developing and supporting the information asset.
- The asset's value to the organization's production operations, research and development, and business model viability.
- The asset's value established in the external marketplace and the estimated value of the intellectual property (trade secrets, patents, copyrights and so forth)

Scalable Solution

In order to evaluate whether or not a security design is scalable, the total revenue and growth potential of the company needs to be taken into account. This will allow the security professional to undertake an effective cost benefit analysis for immediate security purchases, as well as make sound recommendations that will allow for realistic future growth.

GIAC Enterprises is a small fortune cookie business with 18 full time employees – 15 administrative and office staff and 3 sales personnel in the field. The example below is taken from an actual fortune cookie company, and illustrates the revenue limits imposed by the size and business model under discussion:

80,000 cookies per day

$.10 / cookie = $8000 per day

x 250 days (5 days/week for 50 weeks)

= $2,000,000/year maximum revenue[10]

The growth potential of the fortune cookie industry is also limited. A search of publicly traded companies does not turn up any fortune cookie companies.[11] It

does point to a number of larger cookie companies that include fortune cookies as a subsidiary, which may be a long term growth direction.

Threats

Threats to any company doing business on the web are numerous and growing[12]. Threats need to be assessed in relation to any individual company situation, but may include external threats such as hackers, viruses, worms, trojans, spy ware, natural disasters, or weather related events.

A threat can be any person, object, or event that, if realized, could potentially cause damage to the LAN. Threats can be malicious, such as the intentional modification of sensitive information, or can be accidental, such as an error in a calculation, or the accidental deletion of a file. Threats can also be acts of nature, i.e. flooding, wind, lightning, etc. The immediate damage caused by a threat is referred to as an impact.[13]

One of the greatest threats to any company comes from company insiders, whether through mal-intent, poor training or human error, insiders can be a liability if they are not addressed. Insider threats include unauthorized access, incorrect access, un-intentional deletion, modification or release of files.

Risk

Risk is defined as "a function of the probability of a given threat agent exercising a particular vulnerability and the resulting impact of that adverse event on the organization"[14]

RISK = THREAT X VULNERABILITY[15]

Vulnerabilities are weaknesses in a LAN that can be exploited by a threat. For example, unauthorized access (the threat) to the LAN could occur by an outsider guessing an obvious password. The vulnerability exploited is the poor password choice made by a user. Reducing or eliminating the vulnerabilities of the LAN can reduce or eliminate the risk of threats to the LAN. For example, a tool that can help users choose robust passwords may reduce the chance that users will utilize poor passwords, and thus reduce the threat of unauthorized LAN access.[16]

The important thing to point out is that in order to have a risk, there must not only be a threat, but an opportunity for that threat to take hold in an environment. This becomes important when considering mitigation strategies such as how soon and how often to patch operating systems, and more importantly, the cost of choosing a particular operating system or software package that may be prone to both vulnerabilities and threats. This idea will eventually be included as a standard component of the total cost of ownership formula, where the cost of the software will include not only the cost to purchase, maintain and support it,

but the cost to patch it and the cost of the risk assumed by that purchase.

With that said, every piece of software or decision includes a certain amount of risk. Therefore, risk management must include technical, physical as well as policy and awareness approaches. Protection approaches include; training and awareness (on hiring, ongoing, upon leaving company), policies – confidentiality, non-compete, non-disclosure, what can and can't be published, working hours, business practices (turn off computer at night etc), remote access minimum standards (firewall, anti-v, anti-spy, patch level), and internal minimum standards and support mechanisms. Account creation and access management, auditing business processes, Sarbanes Oxley, GLB, records retention policy, privacy policy (or lack thereof), alert banner etc.

Total Cost of Ownership

Total cost of ownership is the process of evaluating "the full cost of those potential solutions over their entire lifecycle"[17] The full cost includes direct costs, indirect costs and depreciation, ongoing maintenance costs and grave costs.[18]

Direct

Direct costs include the initial purchase of the hardware and software, as well as vendor maintenance contracts, plus the cost of implementation and staff training. Direct costs also include staff and/or consultant time, the costs of managing the project (which may or may not be included in the implementation costs), and the process of testing and verification after implementation.

Indirect

Indirect costs include upgrades to existing infrastructure, additional space power, cooling and cabling or other requirements for new equipment. Opportunity cost should also be considered - any system requires implementation time and a budget commitment, which locks you into that decision until you have received a reasonable return on your investment.

Depreciation

Depreciation is the calculation of the existing value of the product. The ability to calculate the existing value of any asset makes it possible to perform a number of asset valuation calculations to determine things like replacement rates, return on investment and to perform cost benefit analysis. In general, hardware is depreciated over 5 years and Software over 3 years [19], which means the value of the asset is considered zero at the end of the assets useful life. The value of an asset at any point during the assets life cycle is referred to as depreciable value, and is determined by subtracting the salvage value from the purchase price.

There are many methods employed to determine depreciation. Two common methods are the straight line method and the accelerated depreciation method.

The straight line method essentially assumes the asset will depreciate at a steady rate over the life of the assets useful value. This calculation makes it less complicated to determine an assets value, but due to the refresh rate of technology and the pace of innovation, this method doesn't give an accurate point in time evaluation of value.

The accelerated depreciation method is more accurate at any point over the course of the assets life span. This method uses a calculation to determine an accelerating rate of depreciation over time. Accelerated depreciation more accurately reflects real world scenarios since computers tend to depreciate more rapidly at the beginning of their life cycle.

Determining which formula to use depends on a number of factors. If a wide range of assets are being evaluated, or there is a desire to minimize the complexity of the calculations, the straight line method is a good choice. If the depreciation calculation is being used to determine optimum replacement times, then accelerated depreciation is the method of choice. The final decision should be made in conjunction with the finance department in order to ensure any tax consequences are accounted for.

Straight Line Method

In the straight line method, each year the assets value is reduced by the following equation:

$$\frac{\text{Depreciable Value}}{\text{Assets Useful Life}}$$

Accelerated depreciation

In the accelerated depreciation method, depreciation is equal to the useful life remaining in the asset, divided by the sum of years. This number is then multiplied by depreciable value. The result is the dollar depreciation value for that year, so the last step is to reduce the original depreciable value by this result.

Depreciation = (useful life remaining)/(sum of years)*(depreciable value)
Where Sum of years (5 years of useful life = 5+4+3+2+1 – 15)
Year one Depreciation 5/15 * depreciable value
Year two 4/15 *DV [20]

$$\frac{\text{Useful Life Remaining}}{(\text{Sum of Years}) \times (\text{Depreciable Value})}$$

Depreciation Example: $5300 Cisco Pix515 e.[21]

Assume zero salvage value at the end of its life cycle, and use the IRS baseline[22] of 5 year life for computer hardware.[23]

Using the Linear method of depreciation,

Depreciable value =	$5300
Asset life =	5 years
($5300/5) =	$1060 depreciation each year

Using the Accelerated Depreciation calculation

Depreciable value = $5300 Useful life for first year = 5 *Sum of years = 5+4+3+2+1 = 15*		
End of Year	Formula	$ Value
1	(5)/(15)*(5300) = 1767 5300-1767 =	3533
2	(4)/(10)*(3533) = 1413 3533-1413 =	2120
3	(3)/(6)*(2120) = 1060 2120-1060 =	1060
4	(2)/(3)*1060 = 706 1060-706 =	354
5	1/1*354 =3 54 354-354 =	0

Ongoing Maintenance Costs

In addition to direct, indirect and depreciation costs, any total cost of ownership assessment should include the ongoing maintenance cost of the product. These can include:

- Daily log reviews
- Periodic patching
- Configuration updates and reviews
- Failure monitoring and repair
- Supplies
- Future integration issues
- Scalability
- Will it make other projects more expensive?

Grave costs

"Grave costs" refer to the disposal costs of the asset. In some instances this cost can be considerable, such as disposing of large mainframe systems that are considered hazardous waste. A frequently overlooked cost is ensuring that any equipment or media that is disposed of does not contain any sensitive data. Grave costs can include:

- Hazardous waste disposal
- Removal costs of large equipment
- Securely removing sensitive data

Below is an example of a total cost of ownership evaluation for the implementation of an Intrusion Detection System.

IDS project example – 3 years

Activity	***Estimated Cost***
Acquisition	
20 hours of planning time at $200	$4000 for planning
Acquisition IDS system with hardware and management station	$30k
maintenance at $2000/year	$6000
network tap and hub	$1000
additional power circuit	$1000
total acquisition cost	$42000
Implementation	
using vendor 3 days at $1600/day	$4800
Training	
Primary and secondary engineer – 2 sent to class for $3.5k per class plus travel at $1500	$10,000
Management Costs	
Signature updates, log review, creation and review of weekly reports, quarterly design review. 20 hours/week at $50 hour over 3 years	$150,000
Grave Costs	
Removal, degauss hard drives for disposal, donate functional gear for refurbishment and reuse. 8 hours at $200/hour	$1600
total cost =	**$215,600 over 3 years**

Cost Benefit Analysis

Once the actual cost of an asset has been calculated, there are a few approaches to determining whether that cost is justified. One such method is the cost benefit analysis:

Benefits-cost = net Gain/Loss

As an example, if a company spends $30,000 on the initial purchase + $5,000 /

year on patch management, and that investment helps avoid one instance of welchia that cost $200,000 to clean up, the benefit outweighs the cost substantially. For a cost benefit analysis to make sense, the benefit needs to be measurable, which isn't often the case until after an event has already taken place. This is why a cost benefit analysis is typical a retrospective justification, along the lines of "if we had done X, we would have saved y. So we should do x from now on". To make use of a cost benefit analysis approach, accurate metrics on cleaning up after an incident and things like the cost of system restoration are required.

Return on Investment

Another method of justifying a purchase is the return on investment calculation. As with cost benefit analysis, this calculation depends heavily on established metrics to make a case. When discussing return on investment in relation to a security investment, it is important to discuss intangible benefits. By definition these are difficult to quantify, so they tend to be left out of the return on investment calculation. Intangible benefits of improved security can include protecting the reputation of the company from negative press, maintaining customer confidence, and the competitive advantage of maintaining the integrity of business secrets.

The ROI calculation is:

%ROI = (benefits – costs)/costsx100[24]

Payback period = monthly costs/monthly benefits

The payback period is the time it takes the system to pay for itself.

An example of a return on investment calculation:

If it cost us $5000 /month to clean up viruses, and the license was $30k, payback period is 6 months.

An alternative way to calculate return on investment in a security environment is the return on security investment model proposed by Taz Daughtrey and Becky Neary from James Madison University. This method the idea of risk exposure, or the probability that an incident will occur multiplied by the consequence of that occurrence. This calculation gives us the ability to compare not only risk, but the cost or severity if that risk is realized. Based on this comparison, we can strive to avoid the risk by reducing the probability, or mitigate the risk by reducing the consequence, or both.

To calculate the return on this type of investment, we measure the costs of achieving security against the costs of not achieving it. This is accomplished by dividing the level of reduction in risk exposure by the cost of the countermeasures.

Risk Exposure = **Probability** of occurrence **X Consequence** of occurrence

Risk Avoidance ➔ reducing **probability** of occurrence

Risk Mitigation ➔ reducing **consequence** of occurrence

$$ROSI = \frac{\textbf{R}\text{eduction in }\textbf{R}\text{isk }\textbf{E}\text{xposure}}{\textbf{I}\text{nvestment in }\textbf{C}\text{ountermeasures}}$$

Measure costs of achieving security

- **Prevention**
- **Appraisal**

Against costs of not achieving

- **Detection**
- **Containment**
- **Recovery**
- **Remediation**

The bagel virus or variant of it is a good starting point for an ROSI calculation. The probability of another bagel variant being released is relatively high – we'll estimate it at 80%. The consequence of this particular virus is user downtime and the cost to remediate. If we estimate each of those at 2 hours – 1 hour of down time and 1 hour of staff time to remediate per virus instance – times $30/hour, we have a cost of $60 per virus instance. Multiply this by a .8 probability of occurrence, and we have a factor of $4.8 per user.

If our proposed countermeasure is to invest $5 per month in anti-virus protection, 4.8/5 gives us an ROSI of .96. We can see just by comparing the $4.80 per user to the $5 that the return is worthwhile, using this calculation we can demonstrate that the cost of achieving security in relation to this virus alone nearly justifies the cost of the anti-virus license.

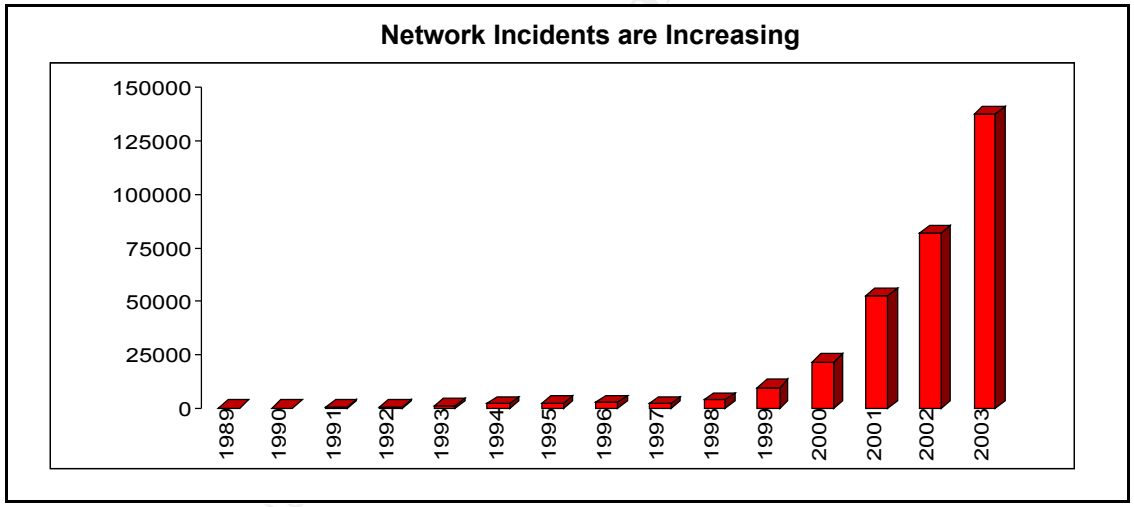
Improvements to the Original Proposal

In order to improve on the original proposal, the technical mitigation strategies need to be scaled back and the policy and procedural steps need to be fortified. A small company with a tight budget and limited growth potential needs to focus on quick wins and a sustainable security infrastructure, one built on policy and end user awareness, backed by strong technical resources.

Step 1: Defining the Threat

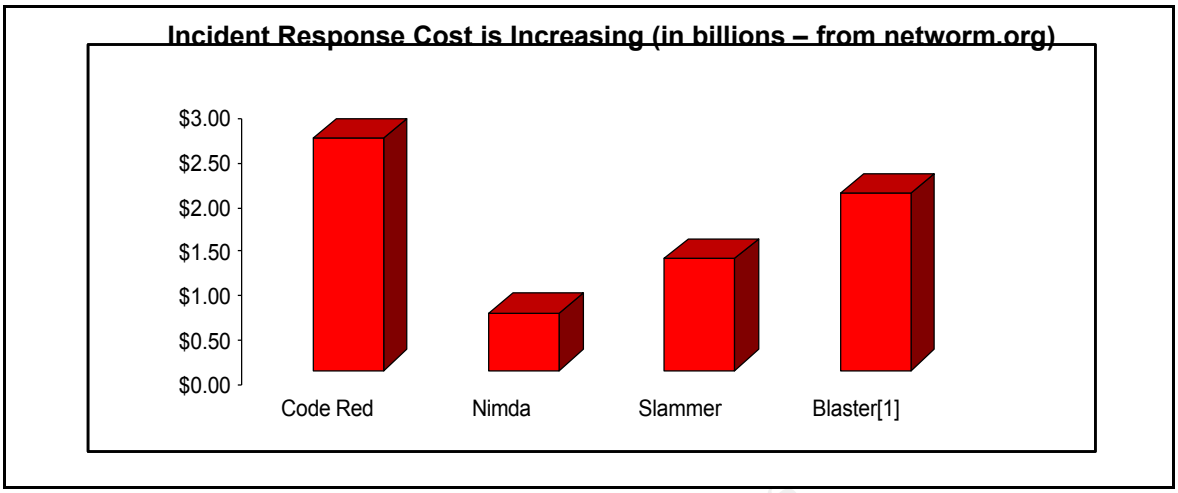
The first step in outlining a well rounded, effective, flexible and scalable layered approach to security is to clearly understand the threats to the company. Network incidents and the cost of these incidents are increasing. A presentation to upper management that details this increase and gives examples of the cost, commitment and necessary aspects of a layered approach to security is essential. This presentation would rely on the facts, figures and graphs included below.

Rate of Incidents



Source: CMU Computer Emergency Response Team
Last updated January 22, 2004

Cost



- As much as 60% of corporate data resides unprotected on PC desktops and laptops. [25]
- "The most common effect of a virus infection, reported by 70 percent of respondents, was rendering a PC unavailable to the user, the study found. Sixty-nine percent of respondents said that viruses had cost productivity, while 37 percent reported loss of data due to viruses." [26]

Awareness

- "83 percent of the survey group said they use an antivirus application, only 73 percent update their definition files regularly."[27]

Financial Commitment

- "Financial services companies are spending approximately 6% of their IT budgets on information security."[28]
- "47% hired extra security staff compared with 2001."[29]
- "Only 19% of respondents said they had reduced the number of IT security staff, despite the slowdown in the economy." [30]

Step 2: Creating the Security Policy

The next step is to work with senior management to develop an information security policy that will outline the importance of information security and set the vision for the future of information security at the company. This policy should begin with a mission statement to guide the actions of security professionals as they make decisions, as well as addressing the following goals[31]:

1. Maintain the confidentiality of data as it is stored, processed or transmitted on a LAN;

2. Maintain the integrity of data as it is stored, processed or transmitted on a LAN;

3. Maintain the availability of data stored on a LAN, as well as the ability to process and transmit the data in a timely fashion;

4. Ensure the identity of the sender and receiver of a message;

The security policy should also take into account the scope of information security, what assets are being protected and the limits the security team should observe. Issues of assessing the security policy and posture of the company, and establishing a governance structure should be addressed.

Step 3: Create the Policy Infrastructure

Once the security policy is in place, the policy infrastructure should be established to ensure that the particular technical steps that are taken to protect the network support the security mission. The specific policies that should be established are[32]:

1. **Identification and authentication** - is the security service that helps ensure that the LAN is accessed by only authorized individuals.

2. **Access control** - is the security service that helps ensure that LAN resources are being utilized in an authorized manner.

3. **Data and message confidentiality** - is the security service that helps ensure that LAN data, software and messages are not disclosed to unauthorized parties.

4. **Data and message integrity** - is the security service that helps ensure that LAN data, software and messages are not modified by unauthorized parties.

5. **Non-repudiation** - is the security service by which the entities involved in a communication cannot deny having participated. Specifically the sending entity cannot deny having sent a message (non-repudiation with proof of origin) and the receiving entity cannot deny having received a message (non-repudiation with proof of delivery).

6. **Logging and Monitoring** - is the security service by which uses of LAN resources can be traced throughout the LAN.

7. **Incident Response Procedures** – Define the various types of anticipated incidents and outline the expected response procedures according to internal guidelines and legal requirements.
8. **Auditing and Vulnerability assessment** – establish the role of the auditor, the limits of the audit and the procedures to be followed.

Step 4: Consider Outsourcing

Organizations are turning to outsourcing as a way to transfer a degree of risk to an outside service provider. Gartner reports that by 2005, 60 percent of enterprises will outsource the monitoring of at least one network boundary security technology[33].This approach has many benefits for a smaller firm like GIAC, including the ability to leverage a highly trained professional staff, with 24 hour availability and existing infrastructure and reporting mechanisms. Services that are being outsourced include[34]

- Network boundary protection, including managed services for firewalls, intrusion detection systems (IDSs), and virtual private networks (VPNs)
- Security monitoring (may be included in network boundary protection)
- Incident management, including emergency response and forensic analysis. (This service may be in addition to security monitoring.)
- Vulnerability assessment and penetration testing
- Anti-virus and content filtering services
- Information security risk assessments
- Data archiving and restoration
- On-site consulting

The META Group, a research and IT consulting company, expects to see maturity in these services in the following order[35]:

1. Managed VPN and firewall
2. Vulnerability scanning
3. Intrusion detection
4. Security monitoring and response
5. Authentication and administration

As one example, an MSSP claims it can set up and monitor security on a 250-user network on a single T1 (1.5 Mbps) Internet gateway for about $75,000 a year, excluding hardware.[36] These services would require 2 -3 full time staff, at a minimum of $70,000[37] if hired in house. In addition, a client organization can convert variable costs (when done in-house) to fixed costs (services), realize a tax advantage by deducting the managed security service provider (MSSP) fee expenses from current year earnings versus depreciating internal assets, and experience cash flow improvements resulting from the transfer of software licenses (and possibly personnel) to the MSSP.[38]

According to a recent survey[39] of 24 corporations that have outsourced key portions of their security infrastructure, these are some things to consider:

1. Integrate information security and privacy into vendor selection process.
2. Appoint a high-level officer to assume responsibility for evaluating vendors for adequacy to meet corporate policy and legal requirements.
3. Evaluate historical experience and reputation of the vendor. One way is to look at complaints and trace patterns back to a given activity or campaign under the control of the outsourced vendor.
4. Consider the vendor's location, critical infrastructure and national backbone issues.
5. Consider cultural and ethical dimensions that may impact due care in the maintenance and protection of customer or employee information.
6. Perform site evaluations and, when appropriate, consider independent audit.
7. Provide good faith disclosure to customers about outsourcing risks (including fair redress process to report problems directly to the company).
8. Ensure the vendor performs background checks, and provides good supervision to its employees.
9. Ensure the vendor has an upstream communication mechanism for security and privacy breaches immediately after they occur.
10. Balance sound information security and privacy risk management against economic (cost minimization) objectives.

Step 5: Technical Improvements

Following are the technical improvements necessary to improve the security posture of GIAC:

1. Flexible IP Address Assignment
    a. Using DHCP or BootP, network and resource access can be traced back to an individual machine's MAC address, increasing non-repudiation.
2. Scanning and DMZ to allow network access
    a. Scanning hosts connected to the network for vulnerabilities using tools such as NetReg helps to decrease the risk that a compromised, legitimate host behind your firewall becomes a threat to critical assets. By scanning on an ongoing basis and sending vulnerable systems to a Demilitarized zone or separate VLAN with no access to internal resources, the spread of threats such as virus outbreaks can be slowed and their impact lessened.
3. Firewalls and Network Address Translation
    a. Firewalling Critical Systems
        i. In addition to other security measures, critical systems should be placed behind a firewall. The benefit of this

approach versus a internet facing firewall is the number of services allowed through the firewall are far fewer, making the device much more manageable.

b. Departmental Firewall/NAT

i. Network address translation is a valuable practice, since it is one way to limit an attacker's ability to perform reconnaissance of the network. Since only one IP address is sent out to the internet to represent GIAC enterprises, the services and set up of our internal network is more difficult to discern. This option should be employed with adequate logging to ensure that individual host activity is traceable for accountability and troubleshooting purposes.

4. Virtual Private Network (VPN)

a. Two of the primary uses for VPN's are to protect data in transit via encryption and to authenticate users.

b. Notably, VPN's can introduce insecurities in a network because they can turn a remote user's system into a dual-homed host, creating an avenue of attack from the Internet. For instance, if an individual connects from home via a broadband Internet connection with a VPN that client does not include a software firewall, an intruder could break into the user's home machine from the Internet and then connect to the institution's network via the user's VPN connection. This security weakness can be mitigated by requiring remote users to install software firewalls. Home users can also be encouraged to create layers of security by setting security standards for their home computers and by using inexpensive Small Office Home Office (SOHO) devices that have some firewall/NAT functionality.

5. Virtual Local Area Network (VLAN)

a. VLAN's are a cost effective way of increasing the layers of defense by separating the internal network into more manageable segments. They also allow for different access control rule sets, so that the internal users VLAN may allow outbound traffic but denies inbound connection attempts.

b. VLAN's using same address space

i. Along the same lines, one addressing scheme proposed by Stephen Northcutt in the Security Leadership Essentials for Managers course is to assign one IP range for all of your internal VLAN's. This approach helps to limit the effectiveness of external reconnaissance since it is difficult to differentiate your critical resources from your DMZ, for

example.

6. Remote Access Security

    a. Particular attention should be paid to remote access users. Either by enforcing the “gold standard” desktop configuration by scanning the users system prior to granting access, or by fire walling off their access to limit the damage remote users can do. Since our remote users will primarily be sales people and will need access to our critical systems, some scanning and DMZ process needs to be put in place.

7. Wireless Local Area Network (WLAN) Security

    a. Wireless Access Points should not be allowed. A wireless access policy with severe penalties should be put in place.

8. Directory Services

    a. LDAP should be used, if possible, as the directory service. Since it is open source and in wide use, LDAP will address the dual issues of cost and scalability that have been mentioned throughout this proposal.

    b. A password management policy that enforces strong password creation (8 characters or more, special characters, no words, can’t reuse passwords and passwords expire in 30 days), application timeouts of 30 minutes, 2 factor authentication, and password auditing need to be put in place.

9. Web Server Security

    a. Important Web servers such as the institutions main server and other publicly accessible Web servers are major targets of attack from the Internet. Additional measures to protect these systems against malicious or accidental harm include making all updates on a staging server, running Common Gateway Interface (CGI) on a separate server, and having a hot backup server. Using a staging server that is separate from the main server enables you to restrict direct access to the main server and make updates to the main server in a more controlled fashion. Placing CGI on a separate server prevents intruders from gaining access to the main server via insecure programs. A backup server that is regularly synchronized with the main server enables you to recover from an incident quickly by replacing the primary server with the backup. Additional recommendations for securing public Web servers are available from CERT (http://www.cert.org/security-improvement/modules/m11.html).

10. Central patching system –

a. Using SUS or a vendor supplied product, such as PatchLink, all servers and hosts should be maintain a current patch level as measured by the Center for Internet Security Benchmarks. Departments and individuals should be rewarded for maintaining these standards, and a penalty should be included if an area falls behind.

11. Systems Vulnerability information

a. Companies such as LUHRQ provide a service that allows a company to submit information about the equipment they are running and have alerts issued to the network administrators as vulnerabilities or security issues are released by the vendor or recognized by the community. This can be a valuable time saving service to consider as GIAC continues to grow.

12. Metrics

a. In order to determine the effectiveness of the security solution, certain aspects of network and business performance should be tracked. The % uptime of the network and related systems is a valuable starting point. There are many reasons a system may go down, so tracking the reasons behind the outage will be important in creating a clear picture. Other statistics such as # and type of viruses caught by the network anti-virus software, # and type of viruses caught by the host software, # and type of viruses that needed to be manually removed, # of incidents reported by the IDS vs. # of legitimate instances of compromise, staff time spent maintaining systems and layers of defense, and the staff time spent responding to incidents and patching systems. The specific metrics for each company should be determined by the following categories[40]:

i. Performance Goal
State the desired results of implementing one or several system security control objectives/techniques that are measured by the metric.

ii. Performance Objectives
State the actions that are required to accomplish the performance goal.

iii. Metric
Define the metric by describing the quantitative measurement(s) provided by the metric. Use a numeric statement that begins with the words “percentage,” “number,” “frequency,” “average,” or other similar terms.

iv. Purpose

Describe the overall functionality obtained by collecting the metric. Include whether a metric will be used for internal performance measurement or external reporting, what insights are hoped to be gained from the metric, regulatory or legal reasons for collecting a specific metric if such exist, or other similar items.

v. Implementation Evidence
List proof of the security controls' existence that validates implementation

vi. Frequency
Propose time periods for collection of data that is used for measuring changes over time.

vii. Formula
Describe the calculation to be performed that results in a numeric expression of a metric.

viii. Data Source
List the location of the data to be used in calculating the metric

ix. Indicators
Provide information about the meaning of the metric and its performance trend. Propose possible causes of trends identified through measurement and point at possible solutions to correct the observed shortcomings. State the performance target if it has been set for the metric and indicate what trends would be considered positive in relation to the performance target.

13. Monitoring

a. Network logs should be maintained for 30 days, unless otherwise requested for criminal or troubleshooting issues.

b. Intrusion Detection is a good first step in monitoring the network and increasing our ability to quickly locate problems or attacks. Intrusion prevention systems are fast becoming a popular replacement to IDS. The setup overhead is the same – network administrators need to establish a baseline of normal activity on the network, set a series of definitions that define the type of anomaly the IDS should send up an alert about. After doing the work required to set up this level of baseline, there is a strong argument for automatically shutting down traffic that does not fit your normal patterns, while alerting your security staff of the issue. This thinking reflects the change from allow/deny thinking to the more restrictive, and secure, deny/allow approach.

Section 6: Conclusion

I agree with the solution put forth by Mr. Huber. The basic methodology of defense in depth is sound, the technical considerations were well thought out. There is room for improvement, especially in the area of making the business case that supports the technical approach. Given the type of company used in this exercise, it is clear that potential revenue was limited, which would compel the company to accept more risk than Mr. Huber's plan allowed for.

My suggestions and discussion of the original plan focused on the hard choice between accepting a risk and investing in proper mitigation, since there are very few companies with unlimited security resources. The most difficult decision a security professional is faced with is where to stop working to improve security and accept the risk. The process outlined in this paper should not only help with that decision, but arm the security manager with some facts and resources to make a strong case to upper management as to how and why these decisions are being made.

This approach introduces upper management to the break down of technical solutions into categories:

- Must do's
- Should do's
- Nice to haves

And the idea that the cost of security increases exponentially as the level of security goes up. This forces upper management to focus on 90% solutions which offer the highest security at lowest cost. Using this information and the resources found in the SANS security leadership course, the security professional can successfully translate technical security language into technical business language. This translation allows for more thorough understanding of the threats and costs involved in the security decisions at hand, which creates the foundation for sound business decisions regarding security.

References

[1] SANS Institute Track 12 Defense-In-Depth. Volume 12.2. SANS Press, 2004. page 7-6.
[2] Government Micro Resources, Inc. (GMRI) "Risk Mitigation Strategy" (20 August, 2004).http://www.gmri.com/dev2go.web?anchor=xyz2corp .
[3] Krutz, Ronald L., Vines, Dean Russell. The CISM Prep Guide. Wiley Publishing, Inc. Indianapolis, Indiana. 1993. p. 85-86.
[4] Educause security resources and effective practices "Security Architecture Design" (22 August, 2004) http://www.educause.edu/SecurityArchitectureDesign/1261.
[5] Salary.com "Salary Wizard Basic Report" (10 September, 2004) .http://swz.salary.com/salarywizard/layoutscripts/swzl_compresult.asp?zipcode=08618&metrocode=184&statecode=NJ&state=New+Jersey&metro=Trenton&city=Ewing&geo=Ewing%2C+NJ+08618&jobtitle=Webmaster&search=&narrowdesc=IT+--+All&narrowcode=IT03&r=salswz_swzttsbtn_psr&p=&s=salary&geocode=&jobcode=IT10000153.
[6] Salary.com "Salary Wizard Basic Report" (10 September, 2004) http://swz.salary.com/salarywizard/layoutscripts/swzl_compresult.asp?zipcode=08618&metrocode=184&statecode=NJ&state=New+Jersey&metro=Trenton&city=Ewing&geo=Ewing%2C+NJ+08618&jobtitle=IS+Security+Manager&search=&narrowdesc=IT+--+Manager&narrowcode=IT07&r=salswz_swzttsbtn_psr&p=&s=salary&geocode=&jobcode=IT10000234.
[7] US-CERT "Vulnerability Note VU#713878" (10 September, 2004) http://www.kb.cert.org/vuls/id/713878.
[8] Federal Information Processing Standards Publication 191 Specifications for Guideline for The Analysis Local Area Network Security. November 9, 1994, Page 9.
[9] Krutz, Vines. p.93
[10] Fortune Cookie Supply .Com (10 September, 2004) http://www.fortunecookiesupply.com/ .
[11] EDGAR Database US securities and exchange commission (10 September, 2004) http://www.sec.gov/edgar/searchedgar/webusers.htm .
[12] CERT Coordination Center "Removing Roadblocks to Cyber Defense" (10 September, 2004) http://www.cert.org/congressional_testimony/Pethia_testimony_Mar28-2000.html.
[13] Federal Information Processing Standards Publication 191 Specifications for Guideline for The Analysis Local Area Network Security. November 9, 1994, page 8.
[14] Krutz, Vines. p.85.
[15] SANS Institute Track 12 Defense-In-Depth. Volume 12.2. SANS Press, 2004 page 7-16.
[16] FIPS PUBS 191 p.8.
[17] SANS Institute Track 12 Security Leadership Essentials for Managers Management Practicum. Volume 12.5. SANS Press, 2004 page 37.
[18] SANS Institute Track 12 Security Leadership Essentials for Managers Management Practicum. Volume 12.5. SANS Press, 2004 pages 36 – 37.
[19] IRS Depreciation, Depletion, and Amortization (10 September, 2004) http://www.irs.gov/publications/p225/ch07.html .
[20] SANS Institute Track 12 Security Leadership Essentials for Managers Management Practicum. Volume 12.5. SANS Press, 2004 page 45.
[21] zdnet.com (10 September, 2004) .http://google1-zdnet.com.com/PIX_515E_DC_Chassis_Unrestricted_SW_2_FE_Ports_VAC/4505-3245_16-9690366.html
[22]IRS Depreciation, Depletion, and Amortization (10 September, 2004) http://www.irs.gov/publications/p225/ch07.html .
[23] IRS Depreciation, Depletion, and Amortization (10 September, 2004) http://www.irs.gov/publications/p225/ch07.html .
[24] SANS Institute Track 12 Security Leadership Essentials for Managers Management Practicum. Volume 12.5. SANS Press, 2004 page 78.
[25] IDC analyst Cynthia Doyle, Business Continuity in 2002: It's Not Business as Usual, April 2002.
[26] Connected Corporation (14 September, 2004) http://www.de.connected.com/downloads/Items%20for%20Downloads/Facts%20and%20Figures%20on%20data%20protection_Q4_02.pdf .
[27] PC World (14 September, 2004) http://www.pcworld.com/reviews/article/0,aid,112468,pg,3,00.asp .
[28] From Deloitte Touche Tohmatsu, 20 May, 2003, (26 pages) 2003 Global Security Survey.
[29] Ibid.
[30] Ibid.
[31] FIPS PUBS 191 page 7.
[32] FIPS PUBS 191 page 8.
[33] Pescatore, J. "Managed Security Services Provider Magic Quadrant." Gartner Research Note, 01 February 2002.
[34] http://www.cert.org/security-improvement/modules/omss/b.html Outsourcing Managed Security Services (12 October , 2004).

[35] King, Chris. "META Report: Are Managed Security Services Ready for Prime Time?" INT Media Group. July 13, 2001. Available at http://itmanagement.earthweb.com/secu/article/0,,11953_801181,00.html.
[36] CERT – CC Benefits of Engaging an MSS Provider (10 June, 2004) http://www.cert.org/security-improvement/modules/omss/c.html.
[37] Salary.com "Salary Wizard Basic Report" (10 September, 2004) http://swz.salary.com/salarywizard/layoutscripts/swzl_compresult.asp?zipcode=08618&metrocode=184&statecode=NJ&state=New+Jersey&metro=Trenton&city=Ewing&geo=Ewing%2C+NJ+08618&jobtitle=Security+Administrator&search=&narrowdesc=IT+--+All&narrowcode=IT03&r=salswz_swzttsbtn_psr&p=&s=salary&geocode=&jobcode=IT10000239 .
[38] Alner, Marie. "The Effects of Outsourcing on Information Security." *Information Systems Security*. Auerbach Publications, CRC Press LLC, May/June 2001.
[39] Darwin Magazine "Are You Practicing Safe Outsourcing? Some best practices and a cautionary case study" (10 November, 2004) http://www.darwinmag.com/read/040104/ponemon.html.
[40] Marianne Swanson, Nadya Bartol, John S (July 2003) "NIST Special Publication 800-55 Security Metrics Guide for Information Technology Systems".