GIAC CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

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

Interested in learning more?

Check out the list of upcoming events offering
"Introduction to Cyber Security (Security 301)"
at http://www.giac.org/registration/gisf

GIAC VENTURES
Securing a Small Business

© SANS Institute 2003, Author retains full rights.

GIAC ISO Certification
Version 1.2
Charles Hornat
February 27, 2003

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Table of Contents

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Abstract

The following paper discusses the infrastructure, business, technologies, policies and procedures that apply to GIAC Ventures. After one has read this paper, they will have a better understanding of what is recommended by SANS in terms of policy and procedure requirements. They will also learn that identifying the crown jewels first, will help focus efforts pertaining to security.

Assignment 1

A Description of the GIAC Enterprise

Who We Are

Formed at the start of the new millennium, GIAC Ventures focuses on investing in early-stage businesses that leverage emerging technologies. Through formal and informal networks that exist among a broad array of minority communities and women entrepreneurs, GIAC is able to access unique investment opportunities. Prior to its formation, the principals of GIAC successfully employed the firm' strategy, investing in 22 early-stage companies and achieving substantial returns for their investors. We are located in New York, NY. GIAC Ventures employs 50 people.

GIAC is often seen as a value-added, early stage capital. The firm frequently invests in companies in their early life cycle; funding companies after angels, friends and family have infused capital, but before some larger venture capitalist are prepared to consider investing. GIAC uses its network of portfolio companies and established strategic relationships to assist young companies grow and position themselves for future financing and ultimate liquidity events.

How We Work

The investment decision process involves answering numerous questions that arise during a due diligence process. This is the process where GIAC learns the potential client companies business plan, attitude and methodology. The core approach involves the following:

- Review of the company's business plan
- Reference checks of the management team
- Discussing the Company's required key hires, if any
- Examining the competitive landscape
- Understanding milestones
- Reviewing information regarding proprietary technology including patents, licenses or joint development agreements
- Understanding the Company's existing, potential and targeted key strategic partners and relationships
- Understanding the existing capitalization including all outstanding options and warrant
- Reviewing all material agreements including those with strategic partners, customers, or other contractual relationships.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

IT Infrastructure

Overview

GIAC's network is simple in design, but robust enough to provide all the advantages of today's top Financial Firms. The network, detailed below in Figure 1, consists of an internal network and a DMZ. The internal network includes a Microsoft Exchange Server, a Microsoft Windows 2000 File Server with additional functionality, and a Microsoft Windows 2000 Application Server. Terminal Services, Terminal Server License Sever and the Terminal Service Server functionality have been deployed as well. The DMZ consists of a VPN Appliance by Netilla Networks, Inc. ("Netilla"), www.netilla.com. Finally, this is all divided by a Firewall with Checkpoint NG ("Checkpoint") installed on a Solaris Ultra 20.

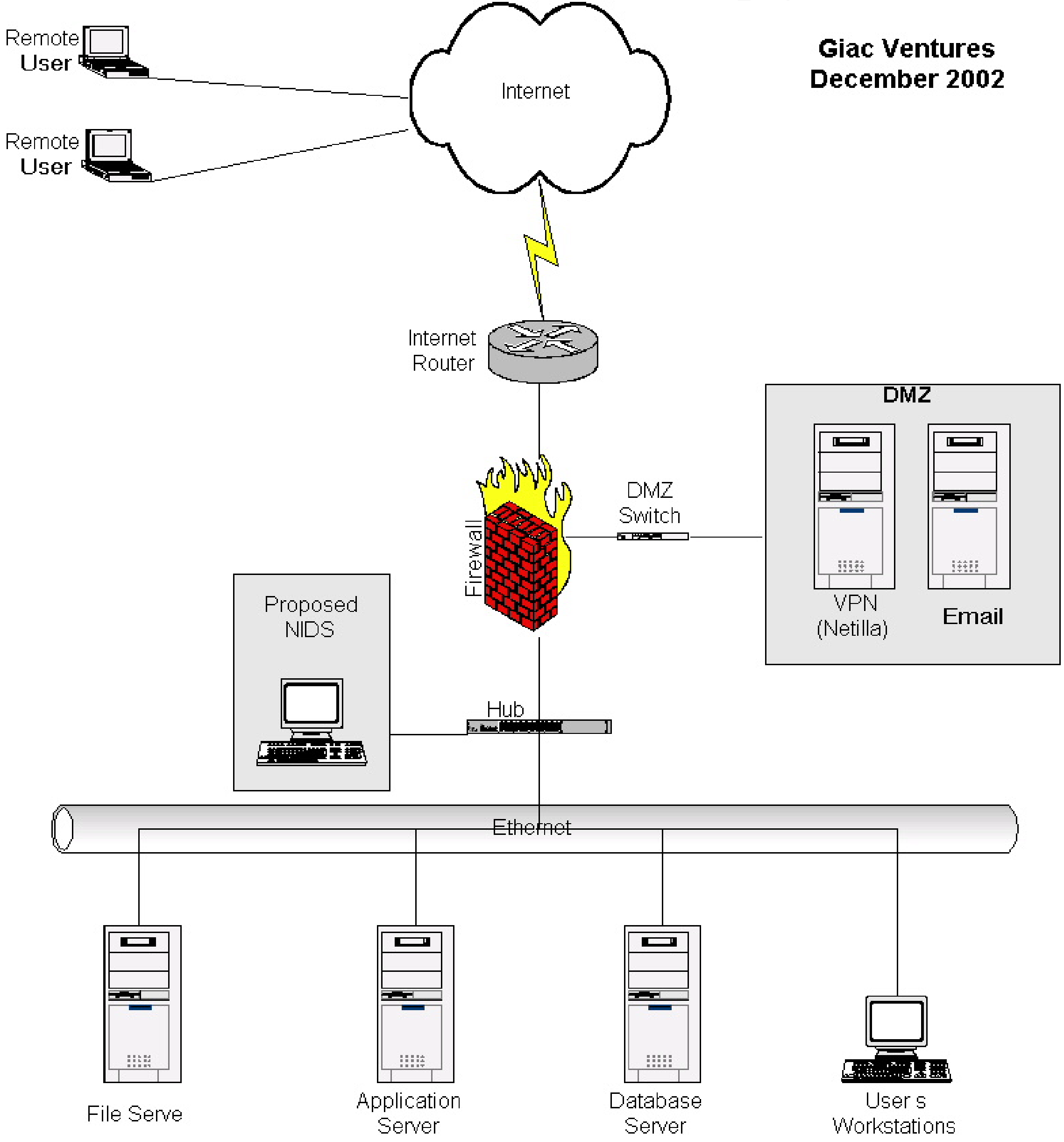

Figure 1:Network Diagram

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Systems

File Server

Since this is a small network with limited funding, some systems will have alternate roles. The first server that was setup was the File server. This system is a Rack mount Dell server with Raid 0 configuration and two 14 gig hard drives. The Operating System of choice was Windows 2000 with the latest service packs and security patches. This server is the Domain Controller and also hosts the following components for the Giac Infrastructure:

- McAfee Management Console e-Policy Orchestra ("McAfee")
- DHCP
- Print Server
- WINS Server
- Terminal Server (Administration Mode)
- Terminal Licensing Server
- Backup

Exchange Server

The Exchange server is a powerful Compaq server with tape backup built in. This server resides in the DMZ. A firewall rule set adds a layer of security between this server and the Internet and the internal network. Since this server can be accessed directly from the Internet, additional steps must be taken to harden this server. Additional steps include the removal of sample files and directories, using the NSA[1] guidelines for securing a server on the Internet, the Firewall rule set, and removing any unused or unnecessary services and applications that may be installed on this system. This server has two 14 gig hard drives and is configured with Raid 0. Backup of this server is performed via a built in tape backup solution.

The Exchange Server hosts the following services:

- Terminal Server (Administration Mode)
- Blackberry Server (BES 3.5)
- Backup Server via a local Tape drive

Application Server

This server hosts applications utilized by the VPN Appliance Netilla via a user connecting to Netilla in the DMZ. The Netilla device then initiates a terminal server window to the Application server using 2000 Domain credentials. Since applications on this server are accessed via Netilla, Terminal Services is set in Application Mode. This Terminal Server setup requires a licensing server, which must be a domain controller. Therefore, this server's Terminal Server Licensing server is the file server. This allows users to connect from anywhere on the Internet and have instant access to the following:

- Microsoft Word
- Microsoft Excel
- Microsoft Access – a shared database of investors, leads and deals.

[1] http://nsa2.www.conxion.com/index.html

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- QuickBooks 2002– used for accounting and often time access is required by GIAC's accountants from outside the firm.
- Remote file sharing – allow offsite users to upload and download files from the File Server
- Terminal Server (Application Mode)

Firewall Server
The Firewall Server is a Solaris Sparc Ultra 20 with two 9 gig hard drives that are mirrored and has Solaris 8 with the latest cluster patch installed as the underlying operating system. Checkpoint NG with the latest Feature Pack and Hotfixes are installed and configured and is the firms perimeter defense. This system has a quad card in it and is configured to be the primary router between the internal network, the DMZ and the Internet. Since this system is also acting as a router between the Internet, internal network and the DMZ, Checkpoint will also be performing NAT for the DMZ systems and the internal network.

Netilla (VPN) Server
The Netilla[2] Server is rack mounted and runs Redhat Linux 6.2 as the operating system. The appliance applications are all customized and run off a product called Tarantella. This system has two network Interface cards, one for direct connection to the Internet and one for connection to the internal network. The device utilizes built in IPChains Firewall that is managed and maintained through the Netilla front end Graphical user Interface (GUI). It also utilizes an SSL certificate for secure communications with the hosts.

Remote Access

Overview
Many of GIAC's employees travel often to visit potential investments and investors, as well as serve on the Board of Directors for Portfolio Companies about 70% of the time. The users are potentially out of the office for a few weeks at time while working. This puts an immediate need for a mobility solution. The users need access to their Email, Calendar, Contacts, Microsoft Word, Microsoft Excel, Microsoft PowerPoint and Microsoft Access. They also require a dial up client that has dial up access points throughout the United States where broadband is not an option. In order to achieve these requirements, multiple devices have to be used.

In order to ensure proper protection, GIAC has mitigated risk to an acceptable level by applying a layered security approach to remote access. This includes:

- securing clients with antivirus, firewalls, a hardened OS and user education
- Securing the DMZ and the communication passing through by requiring appropriate encryption levels and ACLs as well as hardening systems OS's and:
    - Monitoring logs automatically and manually
    - Developing processes and policies addressing monitoring, Includes:
        - Names and numbers of individuals

[2] http://www.netilla.com/ms_index.html

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

        - Escalation procedures
        - Response tactics
    - Development of an Incident Response Team
- Securing systems internally that will be accessed or contain information that will be accessed from the Internet by hardening their OS's, ACLs, and proper monitoring

Laptop
Each partner is outfitted with a Dell C400 laptop, because it is lightweight and reasonably priced. Each laptop runs Windows XP as the Operating System with Office XP for standard applications like Word and Excel. The primary email client installed and used is Microsoft Outlook.

A dial up client by United Online, Inc which provides value-priced internet access through NetZero is installed on each laptop. Sygate Personal Firewall is also installed to provide a layer of defense against attacks when the user is out of the office using their personal broadband solution or dial up. McAfee antivirus solution is installed to help protect against malicious code in web sites, antivirus security, and a layer to help protect against Trojans, spyware, worms and other known & unknown threats. Finally, user education is important. Users spend an hour and half upon receiving the laptop and taught best practices pertaining to security and the laptop. Both, physical and data security is discussed and users are permitted to ask question.

PDA
Research in Motion's Blackberry Wireless Handhelds are deployed to allow the users to receive and send emails when in a meeting or traveling and do not have Internet access for their laptop. A Blackberry server is installed and secured based on the white paper at Blackberry[3]. All users are required to carry this device when out of the office because the handhelds are designed to remain on and continuously connected to the wireless network, allowing the user to be notified as new email arrives. Furthermore, like the laptops, users are given a security overview of best practices pertaining to the PDA.

With any device that leaves the office, there is a concern about loss or theft. Important contact information and confidential deal information may be compromised if this occurs. Therefore, additional security to the device comes in the form of a small policy developed for Blackberry Enterprise Server (BES) 3.5. BES 3.5 allows an administrator to create a policy for groups and users of the device. There are overall about 40 items administrators can control centrally. Items include Minimum and Maximum password expiration, timeout and password requirements. To ensure proper security pertaining to this tool, an issue specific policy was created. Please see Appendix B for a copy of this policy.

Email Web Access
There are two methods in which users can check their email from outside of the office if they do not have their Blackberry or laptop with them. The first is a solution provided by

[3] http://www.blackberry.net/support/pdfs/bb_security_technical_wp_exchange_21.pdf

Microsoft and built into Exchange 2000 called Outlook Web Access (OWA). The second option is the built in portal solution in Netilla. Netilla has a more user friendly interface as a mail client and allows all the functionality of Outlook Web Access plus:

- Mail List
- Spell Check
- Company Email Directory Access

The only downfall of Netilla is that all subfolders in the users "in-box" have to be accessed separately. User education is also performed here as well. Users are not allowed to access their accounts from systems in Internet Café's or other public access points.

Printers

There will be four printers internally, a Xerox Document Centre 332ST black and white printer/copier, a Xerox Tektronix Phaser 850DP Color Printer, a HP 8550DP Color Printer and finally a HP 4550N black and white printer for small print jobs. The printers will be networked and managed via the built in print server functionality of Windows Server 2000.

Desktops

The operating system for all Desktops is Windows XP and are all members of the Domain. User accounts will be managed by Active Directory and Group Policy will be utilized. Users will not have administrative rights to their workstations to help cut down on potential problems caused by users installing foreign (non-approved and tested) software and making changes to the current configuration.

Applications

GIAC will utilize Office XP with the latest Service packs and security patches. The Application Server will be used in conjunction with the Netilla device to offer users of GIAC the ability to utilize applications out of the office. Applications to be shared and utilized out of the office are Microsoft Access for the shared company databases and Quickbooks for bookkeeping

The Backup software to be used is the built in Windows 2000 Server backup solution. This provides a simple and economical solution to backing up the user's files nightly on the server as well as the Exchange databases.

Business operations

GIAC Ventures receives numerous business plans from various companies on a daily basis and needs a method of tracking data pertaining to the companies, with comments, contact information, investors and financials. It also needs to manage the deal pipeline with the ability to initiate, track, and manage the lifecycle of deal opportunities.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Additionally, the investors who invested into the fund need to be tracked along with the amount invested and contact information.

GIAC Ventures is a small user environment that is comprised of investment professionals, support staff and a technology group. The company is located in a major US city. The investment professionals are all top executives who have left major Wall St. firms to begin their own business, GIAC Ventures. This sets precedence with their expectations as they are used to Blackberries, remote access and around the clock service. In their past environments, technology budgets were large, but now the technology budget is more limited and less expensive solutions and sharing of resources need to be sought out and implemented.

The heart of GIAC Ventures is the database kept in MS Access. This database acts as a collection of all clients, investors, their history and comments, deal pipeline, and etc. The database contains all critical information that is shared and used on a daily basis by most of GIAC's employees.

GIAC Ventures is staffed by several technologists. The Technology department is broken into three distinct groups:

- Server/Enterprise Application Team
- Desktop Support
- Remote computing

The Server/Enterprise Application team is responsible for the Exchange, File and Application Servers as well as backups and central management systems like Antivirus and the Personal Firewall. They also evaluate new solutions that could benefit GIAC, and analyze, design, and implement system changes.

The Desktop Support group provides daily upgrades and patches. They also assist end users to troubleshoot and solve technical problems on a daily basis. Additionally, they work with the Server/Enterprise team to recommend and investigate potential applications that could benefit the Enterprise. This group also administers, maintains, develops and implements policies and procedures for ensuring the security and integrity of the company database currently kept in Microsoft Access. This database is the Crown Jewel of the organization.

The Remote Computing group focuses on the tools that users use when off site, such as the VPN Portal solution Netilla and the Blackberries. They provide support and training on these products as well as plan, direct, and manage the daily operations of these devices. Establish department policies, procedures and explore ways to improve the remote computing experience for GIAC users.

The only group outside of GIAC employees who need remote access to the GIAC network are GIAC's accountants. They not only require access to Quickbooks each year to complete GIAC's taxes but also to track investments and expenditures quarterly to

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

report to firm investors. This is accomplished via the VPN Portal Netilla where Quickbooks is setup as a shared application.

In order to successfully identify risk, and offer mitigation techniques, we followed the following process:

1. Identify the Asset(s)
2. Identify Areas of Concern
3. Identify Threats to the Asset
4. Identify Impacts of Threats
5. Create a Risk Mitigation Plan

Using the outline described above, GIAC identified the following threats:

- Disclosure of confidential data to competitors or public
- Data destruction
- Data stored offsite and not protected by the GIAC security team

In order to get a better understanding of how GIAC responds to risk of an asset, let's walk through an example. GIAC identified the asset as the financial data that their accountants will access. This data is controlled by GIAC and they are responsible for it while in the GIAC infrastructure. However, the data is shared by GIAC management and their accountant's offsite. Since the accountants are off site, and the transmission of data is done over the Internet, this is a major security concern for GIAC as they have identified an interception of data transmission as a concern. Potential threats to the data could be competitors who are looking to gain an edge, internal employees who want to know their peers salaries or bonuses, or publications researching this type of information for public printing.

In each of the sample threats above, the impact to business by each threat could be as follows:

- If a competitor were to gain access to the financial records of GIAC Ventures, they could use that information against GIAC and gain a potential investors confidence by offering better services at a cheaper rate
- If an employee were to gain access, they could alter their pay, or review other employees salaries and bonuses
- If a publication were to gain access, they could print confidential information that could damage business relationships

Steps taken to help mitigate some of the risk include proper Access Control in the Active Directory as well as the file system and database containing the data, require proper authentication to access the data, require encryption for any transmission of data, proper storage of GIAC's data on any third party system, and third party agreements. Having the accounting firm sign a third party disclosure that states they are responsible for any damage done, whether it be the GIAC database while they are accessing or disclosure when data is stored in the accounting infrastructure, helps transfer some risk. For a high level overview of the Netilla security model, please see figure 2.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

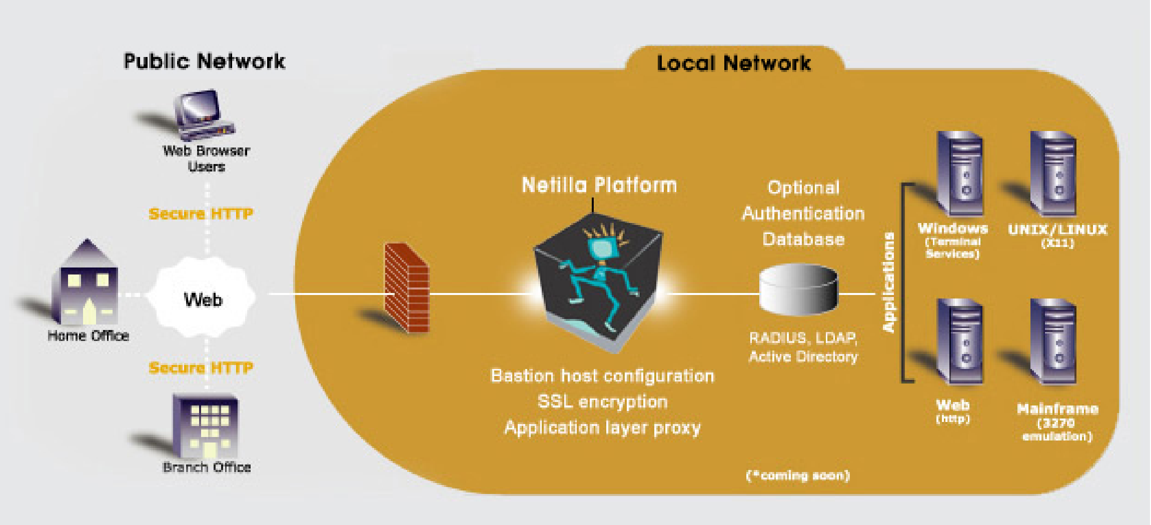

Figure 2:Netilla Security Overview
(http://www.netilla.com/images/subpageart/diagram_tech.jpg)

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Assignment 2

Identify Risks

Risk 1

Database

All Investment deals are kept in a central database. This information is considered the most crucial to the organization as it contains information pertaining to who made what investment, when was the investment made, how much was invested, what percentage of each investment is owned by a firm investor and etc. The information stored in the database is never removed. This is not a concern at this time since GIAC is a new company and disk space is reasonably priced. This also increases the level of concern over a compromise and disclosure of the data, as all data is located here.

Risk

Risk of data is determined via the Octave Model of managing Information Security Risk taught by CERT. Figure 2 outlines a generic chart to help outline risk.

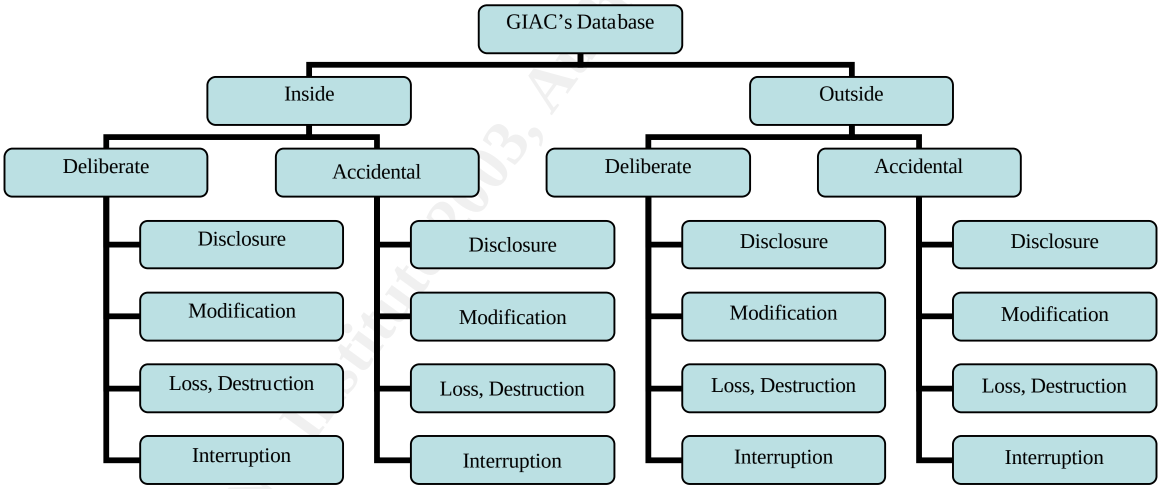

Figure 2:Risk Outline

By using the chart in figure 2, one can identify the type of risk that lies with GIAC's data in the database. The end-result of disclosure/modification/loss,destruction/Interuption would be considered the same whether an Inside or Outside attack occurs. Also, Deliberate and Accidental damage would be considered the same for this assessment.

Using the model in figure 2, we can accurately identify a risk and the associated threat. The result, with mitigation suggestions, would then be presented to management to determine if action should be taken.

Example

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

If GIAC's database were to become corrupt, we could use the chart in Figure 2 as follows:

- This would be considered an Inside threat
- The Actor would be the software failing
- The outcome would be potential loss or interruption (based on last successful backup)
- The impact would be to restore the database back to the last original known good state
- The Mitigation plan would be to require full backups on a regular schedule

To expand on the above sample, if a user at GIAC were to make a mistake and accidentally damaging the database, the information stored in this database could become in-accurate, corrupt and perhaps un-usable.

If the information were to become damaged or deleted, this would cause several severe problems for GIAC. The first is bookkeeping would become a problem. GIAC is required by law to keep account of taxes, and report this to the each investor so that they may file appropriately. This could in turn lead to legal problems for all investors.

An Additional concern would be the data stored in the database, we could conclude the following: If this information were disclosed to a competitor (outside), they could use it to coerce the investors or publish private information that would potentially harm GIAC's reputation and perhaps have legal ramifications. The attackers would have the contact information, banking information such as wiring instructions, how much was invested and key decisions made in meetings at the companies meetings. Additionally, GIAC Ventures credibility in the industry would fall, possibly causing them to go out of business. Only a handful of Investment firms specializing in technology today exist, and that makes the market that much more competitive.

Additionally, if a company is bought, sold or becomes bankrupt, GIAC needs to be able to identify the loss or gain for each investor into that company. They can then compensate or report the gain or loss. Finally, the database is used to store all communications that occurred with each company along with the quarterly financial information provided by the company. This helps determine if more funds have to be raise for the company, if the company will go public, if the company is being bought by a bigger franchise, etc…

Mitigation

Protecting the information in the database is crucial to GIAC. The philosophy of "Security in Depth" is applied here. The database is currently stored in a MYSQL database and is accessed via Microsoft Access. So first and foremost is assuring the latest security patches for the OS and MYSQL are applied to help mitigate risk of malware. Additionally, it is crucial to know when a new vulnerability is released so that the system can be patched almost immediately; this is done through subscribing to the

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

CERT[4] and VULNWATCH[5] list. If an alert is released, the administrators can react accordingly and shrink the window of opportunity for the attackers.

The next step is to assure the proper access rights are given on the database. MYSQL allows the administrator to assign specific user rights to tables thus helping eliminate the possibility of user error damaging the information. A backup is also made nightly to assure the possibility of a restore in such a scenario. The backup scheme requires a full restoration of the database back to original working order within 4 hours. Weekly backup tapes are sent offsite for a Disaster Recovery/Business Continuity situation.

The Quickbooks server resides in the internal LAN and also utilizes the Windows Rights and Permissions security structure. This allows GIAC to, at a different level, control who has access to what on that particular system.

© SANS Institute 2003, Author retains full rights.

[4] http://www.cert.org
[5] http://www.vulnwatch.org

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Risk 2

Information Security

The second risk that GIAC Ventures faces is securing the laptops of the partners as they contain a large amount of sensitive and confidential information. GIAC conducts much of its business out of the office and the partners all use laptops as their primary workstation. Items such as Virus protection, File security and central management are all concerns.

Threat

There are several concerns pertaining to mobility and several layers of defense that can be applied to help sooth those concerns. The primary concern is users will be working from many different networks, such as a dial up solution, their own personal broadband solution and hotel/remote companies they visit networks. As the user travels and exposes the system to these different networks, the risk of infection or remote attacks increases. Additionally, what type of data is stored on the laptop? Is it confidential or critical to GIAC and if so how do we protect it?

Using the same method of identifying risk as used for identifying risk with third party access, and offer mitigation techniques, the following steps will be reviewed:

1. Identify the Asset(s)
2. Identify Areas of Concern
3. Identify Threats to the Asset
4. Identify Impacts of Threats
5. Create a Risk Mitigation Plan

The Asset is defined as the data stored and communication between remote user hardware solutions and the GIAC Enterprise.

Primary areas of concern are:

- Disclosure of confidential or critical data
- Network compromise
- Denial of critical services such as remote access points or databases

Threats to the Assets

- Competitors
- Internal Staff
- Random attackers

Impact of Threats

- Disclosure could lead to a negative reputation
- Potential loss of clients
- Potential loss of investors
- Potential loss of business

Risk Mitigation Plan

- A personal firewall will be installed on all systems outside the company walls. Sygate is the personal firewall of choice as it not only provides standard firewall protection but also provides:

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

  - Firewall policies based on the user location
  - Central Management
  - An application based Intrusion Prevention Engine
  - Host integrity Enforcement providing Tripwire like security to the Operating System and applications on the system
- Encrypting File System (EFS) for data and file encryption. EFS is built in to the Windows XP and 2000 Operating System thus providing a price-friendly solution
- Hardening of the Operating System using solutions provided by the NSA[6] and SANS[7]
- Antivirus protection using McAfee and E-Orchestra. This provides:
  - Central management and reporting
  - Ease of deployment
  - Antivirus and other malware protection
- Ensuring that Critical or confidential data gets appropriate security by developing Information Security Policies that help users define how they should treat specific data

© SANS Institute 2003, Author retains full rights.

[6] http://www.nsa.gov/snac/index.html
[7] http://www.sans.org

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Risk 3

Network Security
Since GIAC Ventures is a small sized company, finances are limited. Therefore, the most effective strategy will be based on low cost solutions. Return on Investment is not going to be a deciding factor as the companies budget must be met one way or another. Currently GIAC only has a single Firewall on the perimeter protecting the internal network. GIAC lacks the ability to ensure data integrity using a Host Based Intrusion Detection tool (HIDS), a Network Intrusion Detection tool (NIDS) or antivirus solution.

Threat
The threat is significant as proper security is not implemented to protect against worms, Trojans or viruses on the servers. Additionally, if an intruder were to gain un-authorized access to the network, it would be near impossible to be aware of the intrusion, and recovery back to a known good state would require a complete rebuild of the servers and workstations.

If the network were compromised and this information become public, the company could suffer damages in reputation. GIAC is a venture capital company focused on technology, and many investors would wonder the competency of a company that invest in technology, yet does not secure their own network.

Mitigation
Using the GIAC Ventures method of identifying risk, the following steps will be reviewed:

1. Identify the Asset(s)
2. Identify Areas of Concern
3. Identify Threats to the Asset
4. Identify Impacts of Threats
5. Create a Risk Mitigation Plan

The Asset in this scenario is identified as the infrastructure. The term infrastructure, as used here, includes all systems (server, desktop, laptop, and PDA) that is utilized by employees for business reasons at GIAC, routers, switches, Email, data, databases, and etc.

Areas of Concern

- Network used in an attack or is a victim of an attack
- Disclosure of confidential or critical data
- Systems taken offline unauthorized
- Disruption of Internet and Email service

Threats to the Asset

- Outside Attackers
- Inside administrative mistakes
- Hardware failure

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- Malware – Worms, Trojans, and virus

Impacts of threats

- Disruption of data
- Modification of data
- The Financial Loss impacted by the following would be devastating:
    - Loss of customers
    - Loss of Investors
    - Loss of data
    - Disclosure of data

Risk Mitigation Plan

- Properly configured firewalls to ensure minimal exposure from mis-configured rule sets
- Operating System Hardening as defined by the NSA and SANS organizations
- Antivirus solutions on all servers, gateways, and clients to help mitigate the risk of key loggers, Trojans and other malicious ware.
- Access Control List that are properly defined and include policies and procedures on how a user would gain access to confidential or critical access
- Network Based Intrusion Detection (Proposed) to help detect malicious activity in the DMZ that bypassed the firewall
- Encryption of credentials during authentication and storage of those credentials in the domain
- Properly documented policies and procedures
- User Education and awareness programs designed to reduce risk of user error
- Monitoring of system and security logs, done both by scripts and manual
- Patch Update Policy defining when and how security patches should be applied to systems in GIAC
- An additional firewall to protect the internal network in the DMZ architecture

Let's review an example of the proposed Network Based Intrusion Detection (NIDS) and the antivirus management solution implementation and benefits. NIDS is not in production yet, but an older Pentium 2 workstation will be dedicated to this task in 4-6 weeks.

First, a low cost workstation will be equipped with Redhat Linux 8.0. The box will be secured using SANS securing Linux[8] documentation. IP Tables will be enabled to only allow specific traffic to and form this system. SNORT will be installed on this system and will monitor the connection from the Firewall to the internal switch. This will help identify malicious traffic that may have surpassed the firewall coming into the network, or detect malicious traffic as it leaves the internal network, identifying potential compromised systems. Snort will have the latest signatures and be updated weekly.

[8] http://www.sans.org/projects/bastille_linux.htm

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Additionally, SNORT will be configured to alert specific technologist in the event of a trigger of specific alerts.

Additionally, GIAC will purchase other components of McAfee E-Orchestra that will help monitor and protect the Email server, File server, and application server. This will help cut down the possibility of worms and malicious ware distributed via email.

Assignment 3

Evaluate and Develop a Security Policy

Overview

Security Policy # 3 can be found in Appendix A. This policy should be one of the first and most important policies in any organization. Most organizations have proprietary or confidential information that they want to protect, and this policy will clearly define the roles and responsibilities that will protect the information assets of GIAC Enterprises.

In the three areas of Risk identified above, they identified the data that was being communicated as the primary asset. Therefore, the following policy is dedicated to classifying that data and setting guidelines that the organization should follow. This would also tie into the user training as this is policy pertains to people and actions they would take.

Examples of concern over data security were outlined in Risk 1 and Risk 2. After identifying the assets and the potential threats to those assets, the outcome of disclosure of confidential data could lead to potential losses of investors and clients leading to financial loss.

Security Policy #3 was taken from former employment. In this section, a review and discussion of policy improvement will be discussed. The sample policy is derived from a previous employer.

Review

According to the GIAC standards, the policy should contain the following:

- Purpose
- Background
- Scope
- Policy Statement
- Responsibilities, and
- Action

Purpose

Security Policy #3 was established to protect the Information assets of GIAC Enterprises. The objective of Security Policy #3 as stated in the policy is to "ensure the integrity, confidentiality and availability of GIAC Enterprise Information." As stated earlier, the

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

primary asset of GIAC is the information that they have pertaining to clients and potential companies GIAC may invest in. Additionally, many times, GIAC will have exclusive insight into the future of particular companies. This information may be desired by others in the industry and needs appropriate security measures to protect it as well as policies guiding those who have access to this information.

Given the information above, this section is adequately covered for GIAC's requirements.

Background
GIAC Information Security Policy does not have a defined "Background" section. However, was implemented due to a personal experience at a previous employer. A few years ago, a senior manager requested a copy of the company's database and customer info be made on recordable CD's so that he may work from outside of the office. The unusual request was made on a weekend when no one else was around, and the network team was performing upgrades to the network. The network team notified their management that the request was made and requested actions to be taken.

Permission was granted and the CD's containing proprietary and confidential information was created. The next day, the manager who made the request and several other people from that company quit, to start a competitive company. This request was made, and there were no guidelines or policies to help determine or protect the information that was given. The entire decision pertaining to the company jewels was left up to a senior manager on the weekend. One individual should not be solely responsible for, nor make decisions for an entire companies Information and if more management were involved with this decision, perhaps they would have collectively seen that this employee was organizing this.

Due to the experience above, this policy was created for GIAC Enterprises to help minimize the risk of allowing a mistake like that to occur again.

Scope
Information Security Policy #3 clearly defines the scope of the policy by clarifying who is included in the policy as well as additional parties who have responsibility. The scope also describes who it is trying to protect and whom should get involved in special situations. The content provided here is adequate to the policy.

Responsibility
The policy has a well articulated Roles and Responsibilities section. The section is divided up by the different departments and their roles. This is a very critical piece so that everyone is clear in what is expected of them in this policy.

There is one area of improvement that would be recommended, a section for ex-employees. A section for ex-employees should include a non-disclosure, and a non-compete statement that outlines the responsibilities one assumes when leaving the GIAC organization. This will be added in the re-write.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Policy statements are missing and should be added. It is important to define specific level of interaction of this policy amongst employees of different levels. Additionally, the policy doesn't describe how it helps mitigate risk in the GIAC organization. The policy should include a description of the benefits it provides, and that will in return help define the goal.

Additionally, it would help to understand how this policy applies to the risk identified in assignment 2. Each of the risks identified relate to the identified asset and the access control that pertains to it: data. It is this reason that this policy was chosen as a representation of a critical policy to the GIAC organization. This policy will help outline protecting this asset.

Action
The action statement of Information Security Policy #3 is contained in section 3.2 labeled "Disciplinary Action". The item defines what will happen if an employee fails to comply. Additionally, it states that the disciplinary action to taken by GIAC will be determined by the seriousness of the breach. This policy is not clearly defined in terms of actions, but does make it clear that it will be considered seriously. A small description of what actions would be taken and when would they be taken will be added in the re-write.

Policy Maintenance
One additional item that is contained in this policy worth mentioning is the policy maintenance section. As organizations and technology grows and adapts, so should our policies. This section simply states that this policy should be reviewed regularly and adjusted as needed. It also defines who should be involved and what their roles are if a change should occur.

This was added based on experience. A policy was created about 8 years ago that stated that there would be no inbound connections. This meant that there could be no connection originating from the Internet allowed to enter the internal network. This was fine 8 years ago, until the adoption of VPN. Once VPN was considered by the organization, the policy had to be reviewed and changed as VPN connections would originate from the Internet, and require access to the internal network. This section is acceptable to the organization and provides appropriate information.

Exceptions to the Policy
Finally, Information Policy #3 did not contain a section on exceptions to this policy. The exception piece should describe what needs to occur and who needs to be involved in order to be granted an exception to this policy.

You might ask "Why would one need an exception to this policy?" The answer is, we don't know. If we knew what exceptions would be required, there is a good chance we would have included it in the policy or structured the policy to provide a secure method for that exception. The simple fact is, one cannot always predict what the future may

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

bring, or what our business might require, therefore a solution should be provided for all those items unseen.

Policy Rewrite

Overview

Overall, the policy above is comprehensive and compliments the SANS policy guidelines. However, some changes and additions were made to help better define the policy. The policy did grow due to the fact that some new sections were added that weren't present and add to the value of the policy.

© SANS Institute 2003, Author retains full rights.

GIAC Enterprise (Rewrite)
Policy #3

Information Security

January 2003

Change History
February 2003 – added change History

January 2003 – expanded on the roles and responsibilities and disciplinary measures sections

December 2003 – added a change management section

November 2003 – Added a Policy Maintenance section

1.1 Introduction
The GIAC Enterprise Companies' ("GIAC" or the "Corporation") employees and business partners have a responsibility to protect the information assets of GIAC. This Policy addresses the security of information belonging to and/or in the possession or control of GIAC, including information about products, services, customers, and employees.

All communications and information accessed, transmitted, received, and stored by the GIAC Enterprise, or contained in GIAC's information systems, are covered by this Policy. The Policy applies to information owned by GIAC Enterprise as well as information licensed by GIAC Enterprise from third parties. The Policy applies to information that is accessed and used internally within as well as information distributed outside of GIAC. It applies to all such information regardless of media and origin, and all hardware, software, and networks that receive, store, distribute (either internally or externally) or process such information. Note that additional contractual or legal obligations may apply to third party information. All of this information is collectively referred to as the "**Information**" in this Policy. Access to, and the use of, GIAC

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Enterprise Information and systems are to be provided as required by business needs and are only to be used as authorized and intended.

The integrity, confidentiality and availability of this Information must be secured at a level outlined in the “Data Classification” procedure while meeting the needs of GIAC’s strategic objectives. As such, security measures must be employed regardless of the methods by which Information is moved or distributed, the systems that process it, or the media on which it is stored.

The Information Security Policy 3 requirements will be supported by standards, guidelines, and procedures, as well as compliance monitoring, education, awareness, and enforcement programs.

1.2 Objective
The objective of this Information Security Policy (the "Policy") is to ensure the integrity, confidentiality and availability of GIAC Enterprise Information.

To ensure that the use of such Information is consistent with GIAC’s legitimate business interest, authorized representatives of GIAC Enterprise may monitor the use of this Information and related information systems, review information and messages on such systems, and maintain recordings of such use. Any attempt to block the authorized monitoring or protection of GIAC’s Information assets and systems is prohibited.

It is GIAC Enterprises policy to ensure that security risks to the Corporation are identified, assessed, and managed. Necessary and required measures will be taken to protect the tangible and intangible assets of the Corporation, the business operations of GIAC Enterprise and associated customers, vendors, suppliers, business partners, and staff, from loss, damage or impairment.

Please refer to the “Issue Specific Procedures” for specific data access processes.

1.3 Scope
The Information Security Policy applies to all business units and corporate staff departments, both domestic and international, within GIAC. It applies to employees regardless of the type or length of relationship with the Corporation (collectively, "**Employees**").

The Policy is also intended to protect the security of our Information when it is accessed by customers, vendors, distributors, consultants, business partners and other third parties (collectively, "**Third Parties**"). Issues relating to the security and terms governing the use of this Information must also be addressed in agreements with Third Parties having access to our Information. The Legal Department can assist with the preparation of appropriate agreements for this purpose.

2. Key Roles and Responsibilities

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The following describes the roles and responsibilities related to Information Security at GIAC.

2.1 Corporate Information Risk Management
Responsible for the protection of GIAC Enterprise Information from threats to its confidentiality, availability, and integrity by establishing policies, standards, and guidelines to protect GIAC's shareholder value and its business processes by supporting risk management processes and procedures.

2.2 Corporate Information Security Organization
Responsible for the identification and reduction of risk exposures by providing advice and support to Corporate Information Risk Management, Segment/Corporate Management, Systems Management, and Employees. The Corporate Information Security Organization has primary responsibility for the development, planning, and communication of the GIAC Enterprise Corporate Information Security program. The Corporate Information Security Organization and Business Units/Segments have joint responsibility in deployment and maintenance of the program, as applicable.

2.3 Corporate Audit
Responsible for periodically reviewing and assessing security risk management practices to identify ineffective or non-functioning safeguards, and identifying significant changes in the risk environment that may indicate the need to update the risk analysis or the related internal controls. Corporate Audit will periodically review approved exceptions to this Policy to ensure corporate objectives are achieved.

2.4 Management
GIAC Enterprise management in all business organizations and at all levels is accountable for information security in their respective areas of responsibility. This includes the implementation of policies, standards, guidelines, and supporting programs to ensure that the requirements of this Policy are implemented and supported. Management should ensure that all Employees receive and acknowledge understanding of this Policy and related documents, and that timely information security education is provided to their respective staffs. Additionally, management must ensure, with assistance from the Legal Department where appropriate, that all contracts with Third Party users comply with GIAC Enterprise security policies, standards, and guidelines. Management is responsible for defining the ownership and protection requirements of the Information assets belonging to its business operations. Management is also responsible for assessing change and taking appropriate action as well as ensuring information security risk assessments is periodically carried out.

2.5 Employees
Employees using GIAC Enterprise Information assets are responsible for complying with the security policies, standards and guidelines established by the Corporation and implemented by management. Employees should report information security issues to the appropriate GIAC Enterprise security personnel and promote security awareness and

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

education. Employees should consult with the Issue Specific Policies 2 and 3 for specific peer data access.

2.5.1 Former Employees

When an employee begins employment, they are required to sign a non-disclosure agreement that defines any information, materials, and ideas or any other information pertaining to GIAC company not is disclosed to any other competitor or third party. The assets of the company are owned and regulated by the organization. If an ex employee discloses any critical or confidential information to a third party, they are subject to legal actions deemed appropriate by GIAC. Should a former employee have questions about disclosing, they should contact GIAC's legal department.

3.1 Policy Maintenance

This Policy and its supporting standards, guidelines, and procedures will be periodically reviewed and updated to accommodate an ever changing environment.

- Corporate Information Risk Management will collect all information and comments from management at all levels and Corporate Audit related to changing business needs.
- Corporate Information Security will provide life cycle maintenance for Corporate Policy, standards, and guidelines. When significant changes occur, as when a section is added, deleted, or rewritten, a revision notice will be sent to all appropriate Employees.
- Corporate Audit will report audit findings and recommendations to Corporate Information Risk Management, Corporate Information Security and other appropriate members of management for consideration.
- Management at all levels will notify Corporate Information Risk Management, and specifically Corporate Information Security, of their changing business needs and new requirements.

3.2 Policy Exceptions

Exceptions to Policy are to be considered on an individual basis. Where appropriate, a risk assessment will be performed to evaluate the threats, countermeasures, and extenuating circumstances associated with the exception, and the impact of the exception on GIAC Enterprise resources and business processes.

Management will be responsible for ensuring that objectives, risks and related internal controls are documented. Management is also responsible for analyzing the risks affecting their area of responsibility. If business requirements dictate potentially serious risks, management should review the situation with the appropriate corporate officer to discuss risk transfer. An exception affecting more than one business unit will require the coordinated acceptance of risk from the management of each affected business unit.

Requests for exceptions will be made in writing to Corporate Information Security for evaluation, to ensure that management fully understands the risks involved, and that

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

appropriate action can be taken. All approved exceptions must be reviewed periodically to ensure their continued validity.

3.3 Disciplinary Measures
This GIAC Enterprise Corporate Information Security Policy cannot be effective without the cooperation of every individual using GIAC Enterprise Information. It is imperative that all Employees be made aware of and fully comply with this Policy and subsequent security standards and guidelines based on this Policy. Failure to comply with the standards and guidelines, without previous approval from management and Corporate Information Security, will be treated as a breach of corporate Policy. Action may be taken against violators in accordance with existing GIAC Enterprise corrective action procedures, as applicable, and commensurate with the seriousness of the breach, including loss of employment and legal liability. Any breach of critical or confidential information will be dealt with seriously and full financial loss will be sought to be recovered, and full prosecution of the law will be aspired.

Assignment 4

Develop Security Procedures

Overview

Since we GIAC identified data as one of its most important asset, the following access control policies were chosen for this assignment. This section lays out the procedures and details for accessing both: current staff systems and data and employees who have left the companies data and systems.

These procedures where developed to guide the GIAC organization (Support Services, Management, and employees) on what steps to take to gain access to current and former employee data and systems. It was developed to help protect user rights. This turned out to be a good marketing tool for the security team and raised employee moral when thinking about security. These procedures are not about technical specifications of GIAC or what employees can and cannot do, but ensuring them that management or peers would not be granted access to their systems and data with a simple request. It also kept management in line by not allowing an abuse of power. There are checks and balances worked into these procedures to ensure everyone is in line.

Right to Privacy

The right to privacy is an important statement when a company decides how to handle data access in the United States. The right to privacy is the expectation an employee has about his or her privacy and ownership of the data on their work systems. In the US, employers own the data that is within their organization. If an employee downloads 10 gigs of MP3's they did not purchase, and stores that information on their computer at work, the organization will be held liable, not the employee. The same concept can be applied to all data stored on an employee's computer. Therefore, the corporation has the right to monitor, review and remove any data within their infrastructure.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

When discussing the right to privacy, it is very important to set the users expectations. The best way is to let the employees know that they do not have the right to privacy and that the corporation will monitor and log all activities. This should be explained to all employees on a yearly basis and the employees should sign off on an acknowledgment. A suggestion as to when this could be done is during review time, or when employees receive their bonuses or raises.

History

The following 2 policies were developed because of situations that arose early on in GIAC's beginning. Both procedures were developed to guide the support staff (Helpdesk), management and staff under stand the processes that need to occur when requesting access to employee email.

The first procedure was developed after a peer requested information to another users inbox, who was on vacation at that time, to look for a specific email pertaining to a business deal that was about to close. Access was granted and the deal was closed. However, when the employee who's inbox was granted access to returned, the problems began. In the end, the one employee who requested access should not have been involved with the deal.

The second procedure was developed to address request for access to an ex-employee's data and system. This was developed to ensure only proper access to critical or confidential data was given. However, the concern about the sales team not able to continue business had to be addressed. For example, when a member of the sales team left the company, that person's contacts and deals needed to be followed up with. The Issue Specific Policy #3 helps define the actions that need to occur in order for this to happen.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Issue Specific Procedure #2

Access to a current employee's Email/systems

Creation Date: August 23, 2001
Modification Date: August 23, 2001

ISSUE: Managers and employees want access to other employees Email and files that are still employed in the organization.

RESPONSIBILITIES: The requestor is responsible for gathering the appropriate authorization. Human Resources and the Business Unit Management are responsible for reviewing and approving or denying request. The Helpdesk is responsible for ensuring all requirements have been met, giving access if appropriate, and retaining the authorization.

ACTION: Develop a written procedure to be followed when a manager or employee calls to gain access to another employee's email or files. This written procedure will help minimize some of the risk factor of social engineering and un-authorized access to Email and files.

1. The requestor must obtain, in writing, either:
   a. Both of the following:
      i. Approval from Human Resources with an explanation of what they are requesting, and
      ii. Approval from the Business Unit's Management with an explanation of what they are requesting,
   b. Or, the employee's approval.
2. The Requestor will then contact the helpdesk in writing and supply the authorization to have the account password reset and/or gain share rights to the employee's directories.
3. The helpdesk will retain the written request/authorization for a period of 12 months.

BENEFITS: This process will help minimize the potential threat abuse by management and peers of violating user rights. If at anytime, the helpdesk suspects some unauthorized attempts to gain access to the user account, they should not reset the password or grant access to the requesting party. They should inform the user's manager of the policy and instruct them to get the required authorization as outlined above and notify the appropriate people responsible for Information Security in the Business Unit.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Issue Specific Procedure #3

Access to Ex-Employee Email/Systems

Creation Date: January 23, 2001
Modification Date: January 23, 2001

ISSUE: Managers and key department people want access to a former employees Email and files. The purpose of this procedure is to help identify who should have access, the requirements, and the process of granting access. This policy is designed to that business can continue to function after an employee leaves the organization.

ACTION: Develop a written procedure to be followed when a request is made to gain access to a past employees email. This written procedure will help minimize some of the risk factor of social engineering and un-authorized access to Email and files.

1. When an employee leaves, their account is disabled on that day. The account is then archived to tape backup and deleted from the server which it resided on after 30 days.
2. The next level manager of the departed employee must submit in writing or email a request to have access to the data and systems.
3. If the request is within the 30 day period, the helpdesk will grant access for 60 additional days form the date of the request. All calls and timelines must be entered in the Remedy database for tracking purposes.
4. If the request comes in after the initial 30 day period, the Helpdesk must put in a formal request with the Operations Department to attain the backup tape from the offsite archiving center. The 60 day extension will begin when the account has been restored from the tape backup.
5. Access is granted in the following ways
   a. If access is required for a system, a new random password must be assigned to the account and left on the requesting managers voicemail
   b. If access to data is only requested, supply a mapped drive to the data via the requestors network profile
   c. For access to email, share the email account, and grant access to the requestors email profile
6. The manager has 60 days to copy, print or email any information they require.
7. At the end of 60 days, the account will be disabled, backed up, and removed from the server.
8. All backed up user data must exist for 6 months.

BENEFITS: This process will help business continuity when an employee leaves the organization. It is left up to the business manager's discretion on dispensing of the former employees data to other employees. If at anytime, the helpdesk suspects some unauthorized attempts to gain access to the user account, they should not unlock the account. They should inform the former user's manager of the account that was asked to be unlocked and notify the appropriate people responsible for Information Security in the Business Unit.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

References

Alberts, Christopher and Dorofoe, Audrey. Managing Information Security Risks: The Octave Approach. Addison Wesley Professional. 2003

CERT Coordination Center. http://www.cert.org/

The Vulnerability Disclosure List. http://www.vulnwatch.org

Baele, Jay and Lasser, Jon. “Bastille-Linux Scripts to Secure Linux and HP-UX” SANS. 2002. http://www.sans.org/projects/bastille_linux.htm

“Security Recommendation Guides” NSA. November 25, 2002. http://www.nsa.gov/snac/index.html

“Technical White Paper Blackberry Security” Research in Motion. 2002 http://www.blackberry.net/support/pdfs/bb_security_technical_wp_exchange_21.pdf

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Appendix A

GIAC Enterprise

Policy #3

Information Security

January 2003

1.4 Introduction
The GIAC Enterprise Companies' ("GIAC" or the "Corporation") employees and business partners have a responsibility to protect the information assets of GIAC. This Policy addresses the security of information belonging to and/or in the possession or control of GIAC, including information about products, services, customers, and employees.

All communications and information accessed, transmitted, received, and stored by the GIAC Enterprise, or contained in GIAC's information systems, are covered by this Policy. The Policy applies to information owned by GIAC Enterprise as well as information licensed by GIAC Enterprise from third parties. The Policy applies to information that is accessed and used internally within as well as information distributed outside of GIAC. It applies to all such information regardless of media and origin, and all hardware, software, and networks that receive, store, distribute (either internally or externally) or process such information. Note that additional contractual or legal obligations may apply to third party information. All of this information is collectively referred to as the "**Information**" in this Policy. Access to, and the use of, GIAC Enterprise Information and systems are to be provided as required by business needs and are only to be used as authorized and intended.

The integrity, confidentiality and availability of this Information must be secured at a level outlined in the “Data Classification” procedure while meeting the needs of GIAC’s strategic objectives. As such, security measures must be employed regardless of the methods by which Information is moved or distributed, the systems that process it, or the media on which it is stored.

The Information Security Policy 3 requirements will be supported by standards, guidelines, and procedures, as well as compliance monitoring, education, awareness, and enforcement programs.

1.5 Objective
The objective of this Information Security Policy (the "Policy") is to ensure the integrity, confidentiality and availability of GIAC Enterprise Information.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

To ensure that the use of such Information is consistent with GIAC's legitimate business interest, authorized representatives of GIAC Enterprise may monitor the use of this Information and related information systems, review information and messages on such systems, and maintain recordings of such use. Any attempt to block the authorized monitoring or protection of GIAC's Information assets and systems is prohibited.

It is GIAC Enterprises policy to ensure that security risks to the Corporation are identified, assessed, and managed. Necessary and required measures will be taken to protect the tangible and intangible assets of the Corporation, the business operations of GIAC Enterprise and associated customers, vendors, suppliers, business partners, and staff, from loss, damage or impairment.

Please refer to the "Issue Specific Procedures" for specific data access processes.

1.6 Scope

The Information Security Policy applies to all business units and corporate staff departments, both domestic and international, within GIAC. It applies to employees regardless of the type or length of relationship with the Corporation (collectively, "**Employees**").

The Policy is also intended to protect the security of our Information when it is accessed by customers, vendors, distributors, consultants, business partners and other third parties (collectively, "**Third Parties**"). Issues relating to the security and terms governing the use of this Information must also be addressed in agreements with Third Parties having access to our Information. The Legal Department can assist with the preparation of appropriate agreements for this purpose.

2. Key Roles and Responsibilities

The following describes the roles and responsibilities related to Information Security at GIAC.

2.1 Corporate Information Risk Management

Responsible for the protection of GIAC Enterprise Information from threats to its confidentiality, availability, and integrity by establishing policies, standards, and guidelines to protect GIAC's shareholder value and its business processes by supporting risk management processes and procedures.

2.2 Corporate Information Security Organization

Responsible for the identification and reduction of risk exposures by providing advice and support to Corporate Information Risk Management, Segment/Corporate Management, Systems Management, and Employees. The Corporate Information Security Organization has primary responsibility for the development, planning, and communication of the GIAC Enterprise Corporate Information Security program. The Corporate Information Security Organization and Business Units/Segments have joint responsibility in deployment and maintenance of the program, as applicable.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

2.3 Corporate Audit

Responsible for periodically reviewing and assessing security risk management practices to identify ineffective or non-functioning safeguards, and identifying significant changes in the risk environment that may indicate the need to update the risk analysis or the related internal controls. Corporate Audit will periodically review approved exceptions to this Policy to ensure corporate objectives are achieved.

2.4 Management

GIAC Enterprise management in all business organizations and at all levels is accountable for information security in their respective areas of responsibility. This includes the implementation of policies, standards, guidelines, and supporting programs to ensure that the requirements of this Policy are implemented and supported. Management should ensure that all Employees receive and acknowledge understanding of this Policy and related documents, and that timely information security education is provided to their respective staffs. Additionally, management must ensure, with assistance from the Legal Department where appropriate, that all contracts with Third Party users comply with GIAC Enterprise security policies, standards, and guidelines. Management is responsible for defining the ownership and protection requirements of the Information assets belonging to its business operations. Management is also responsible for assessing change and taking appropriate action as well as ensuring information security risk assessments is periodically carried out.

2.5 Employees

Employees using GIAC Enterprise Information assets are responsible for complying with the security policies, standards and guidelines established by the Corporation and implemented by management. Employees should report information security issues to the appropriate GIAC Enterprise security personnel and promote security awareness and education. Employees should consult with the Issue Specific Policies 2 and 3 for specific peer data access.

3.1 Policy Maintenance

This Policy and its supporting standards, guidelines, and procedures will be periodically reviewed and updated to accommodate an ever changing environment.

- Corporate Information Risk Management will collect all information and comments from management at all levels and Corporate Audit related to changing business needs.
- Corporate Information Security will provide life cycle maintenance for Corporate Policy, standards, and guidelines. When significant changes occur, as when a section is added, deleted, or rewritten, a revision notice will be sent to all appropriate Employees.
- Corporate Audit will report audit findings and recommendations to Corporate Information Risk Management, Corporate Information Security and other appropriate members of management for consideration.
- Management at all levels will notify Corporate Information Risk Management, and specifically Corporate Information Security, of their changing business needs and new requirements.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

3.2 Disciplinary Measures

This GIAC Enterprise Corporate Information Security Policy cannot be effective without the cooperation of every individual using GIAC Enterprise Information. It is imperative that all Employees be made aware of and fully comply with this Policy and subsequent security standards and guidelines based on this Policy. Failure to comply with the standards and guidelines, without previous approval from management and Corporate Information Security, will be treated as a breach of corporate Policy. Action may be taken against violators in accordance with existing GIAC Enterprise corrective action procedures, as applicable, and commensurate with the seriousness of the breach, including loss of employment and legal liability.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Appendix B

Issue Specific Policy #1

Blackberry security

Creation Date: January 7, 2002
Modification Date: February 3, 2002

ISSUE: Provide a detailed set of security requirements for deploying the Blackberry PDA with BES 3.5.

Roles: This policy applies to all staff who utilize the Blackberry PDA. It is the responsibility of the remote computing technology staff to ensure the following policy is defined in the Blackberry user "IT Policy" feature of the Blackberry Enterprise Server.

ACTION: The following steps outlined below must be taken in order to ensure maximum security on the Blackberry PDA device using the Blackberry Enterprise Server version 3.5. This written procedure will help minimize some of the risk factor of compromised information.

1. Blackberry Enterprise Server version 3.5 must be used.
   a. The server that BES 3.5 will be installed on must be built to company standards build documentation and requirements
2. IT Security policies must be applied to all users. This can be found at:
   b. Right clicking on the blackberry server in the administrative console
   c. Selecting "IT Policy"
   d. Click either "Edit Policy" or "Create Policy" and follow the guidelines below.
   e. The following guidelines must be enabled in the policy:
      i. Long Term Timeout Enabled
      ii. MaxPasswordAgeInDays – set to 90
      iii. MaxSecurityTimeout – set to 10
      iv. MinPasswordLength – set to 4
      v. PasswordPatternChecks – set to 1
      vi. PasswordRequired
   f. Disable the following options:
      i. UserCanChangeTimeout
      ii. UserCanDisablePassword
3. If a Blackberry device is lost, the device should be remotely wiped clean within 2 hours of reported loss during East Coast Business hours. If this occurs off hours, then this item must occur the next business morning.
4. The BES administrator account should have the least required privileges needed. Please see BES 3.5 documentation provided by the vendor.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

5. The Exchange and domain user and service accounts must be configured to the least required privileges needed. Please see BES 3.5 documentation provided by the vendor.

BENEFITS: This process is designed to help secure the deployment and usage of a Blackberry Enterprise solution. This helps minimize the potential risk of system and email compromise as well as potential message compromise.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.