GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

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

Interested in learning more?

Check out the list of upcoming events offering
"Security Leadership Essentials for Managers (Cybersecurity Leadership 512)"
at http://www.giac.org/registration/gslc

GIAC REGIONAL SCHOOL DISTRICT
Securing a Public School System

GIAC ISO Certification

Version 1.3

Donald Borsay

11-Nov-03

© SANS Institute 2003, Author retains full rights.

ABSTRACT

The GIAC Regional School District does not have an established information security program. GIAC has no dedicated resources or focus on information security. This paper captures the nature of information found within the district, and sets a high-level plan of action on how that information should be secured. The security assessment will identify key risk areas, introduce information security policy, and formulate remediation plans to further risk reduction.

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

Table Of Contents

1. EXECUTIVE OVERVIEW 4
2. OVERVIEW OF THE GIAC SCHOOL DISTRICT 6
2.1 Description of Organization 6
2.2 IT Infrastructure 7
2.2.1 Perimeter 7
2.2.2 Enterprise WAN 11
2.2.3 Computers 12
2.2.4 Anti-viral Controls 14
2.2.5 Encryption and Use of Public Key Infrastructure 15
2.3 Business Operations 15
2.3.1 Sensitive Information 16
2.3.2 Applications and Core Services 17
3 RISKS 21
3.1 Areas of Risks 21
3.2 Prioritation and Selection 22
3.2.1 Risk 1: Viruses and other Malicous Code can and do exist. 22
3.2.2 Risk 2: Unauthorized users can use or steal an authorized user's identity 23
3.2.3 Risk 3: Compromised Public/ Semi-Public Servers can be used for an internal attack 24
4 EVALUATE AND REFINE SECURITY POLICY 26
4.1 Overview 26
4.2 Evaluate Policy 26
4.2.1 Section VI – Students – Internet Use Policy 26
4.3 Revise Security Policy 27
4.3.1 Section VIII– Information Security – The Vision 27
4.3.2 Section VIII –Information Security– Risk Assessment 28
4.3.3 Section VIII –Information Security– User Management 29
4.3.4 Section VIII –Information Security– Network Security 30
4.3.5 Section VIII –Information Security– Acceptable Use Policy 31
5 DEVELOP SECURITY APPROACH 32

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

5.1 Users Not Aware of Information Security Responsibilities 32
5.2 Poor or Unknown Qualities in Existing Passwords 33
5.3 Faculty/Staff Applications and Core Services Not Separated 34
5.4 Minimum Security Standards do not exist for Faculty/Staff Applications and Infrastructure 34
5.5 Risk Assessments Incomplete for Faculty/Staff Infrastructure.....35
5.6 Public Systems Not Separated and Isolated.....36
5.7 Student Infrastructure Not Separated and Isolated 37
APPENDIX.....39
INTERNET USE POLICY 39
Information Security: The Vision.....43
Information Security: Risk Assessment Policy.....44
REFERENCES 47

© SANS Institute 2003, Author retains full rights.

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

GIAC REGIONAL SCHOOL DISTRICT
Securing a Public School System

1. EXECUTIVE OVERVIEW

GIAC is in the business of public education, and services 4000 students, using 380 faculty and 200 staff employees. In the process of performing its business operations, GIAC has access to and needs to manage the following sensitive information:

- Basic and special education student information
- Employee information
- Accounting information
- Library asset information
- Public records
- Service information

This information is managed by applications and core network services which run within the district's technical infrastructure. The applications and core network services in use are:

- Powerschool & Powergrade
- Skools
- Proprietary Special Education Program
- Follett
- IIS Public Web Site
- Exchange Electronic Mail
- Windows File Share Services
- AWS Weather Station
- Mailing List Services

The school is faced with a number of challenges when attempting to protect this information and provide maximum services within its limited budget. Students do not cooperate, and attempt to circumvent the protections that are in place. Faculty and staff want the flexibility of working from home. The Technology Department does not have the resources or budget to implement the most basic form of security. Many risks exist. The following priority risk factors are present, and need to be managed in this plan.

- Viruses and other Malicious Code can and do exist.
- Unauthorized users can use or steal an authorized user's identity
- Compromised Public/ Semi-Public Servers can be used for an internal attack

Information Security Policy must provide governance so that these specific risks to information can be dealt with and sufficient direction can be set to handle the issues that may surface down the road. Managerial controls are demonstrated in

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

the district's charter, and its Policy and Procedure manual. All the GIAC policies were reviewed, but only the one defined below applied to these priority risks.

- Section VI – Students – Internet Use Policy

Information security was not the primary focus of any of these policies. A comprehensive set of policy does not exist to establish the checks and balances needed to ensure that information is protected. Further, the policy identified above was not comprehensive to all users of information and all areas of acceptable use. The following policies should be introduced to put the information security program on better footing. These policies are only a starting point. Additional policy, guidelines, standards, and procedures should evolve as risks are discovered, and management direction is further clarified. Note that a new section of in the district's Policy and Procedures manual is being recommended,

- Section VIII– Information Security – The Vision
- Section VIII –Information Security – Risk Assessment
- Section VIII –Information Security – User Management
- Section VIII –Information Security – Network Security
- Section VIII –Information Security – Acceptable Use Policy

Once the policies are put into place, they must be applied so that the existing risks can be reduced. Note that these steps assume budget limitations and prioritize security services on the most important information assets. The following high-level steps should be followed to provide the necessary information security transition at GIAC:

- All students, faculty, and staff should receive security awareness training, focusing on the importance of and their responsibilities to information security
- A more restrictive password policy should be put into effect, and all passwords should be changed.
- Business systems and core network resources in support of faculty and staff should be hosted on separate clients and servers. This infrastructure should reside on a separate managed virtual network (VLAN).
- Anti-virus protection should be purchased and maintained for all faculty/ staff infrastructure. Vulnerabilities should be accessed, and appropriate patches and vendor best practices should be applied.
- Risk assessments should be performed on faculty/staff applications and infrastructure. Priority should be given to continued risk reduction.
- Access to internal applications from the Internet should be eliminated. Public applications and core network services should be hosted on separate servers, and should reside on an isolated network managed by the firewall (DMZ).
- Applications and core network services in support of Students should be hosted on separate clients and servers. This infrastructure should reside on a separate managed virtual network (VLAN). The trust level of this

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

network should be lower, and access to the faculty/staff network should be prohibited.

2. OVERVIEW OF THE GIAC SCHOOL DISTRICT

2.1 Description of Organization

The GIAC Regional School District was originally formed in 1958 to fund the construction of, and subsequently support to, a regional High School. In 1986, the charter was broadened, and included funds to construct a Middle School, and integrate elementary education with secondary education. The district currently contains: 4 elementary schools, one Middle School, one High School, a vocational/technical school, and a school for high-risk students.

The district owns the property at the GIAC campus, containing the High School, Middle School, Career and Technical School, and Central Administration. Property is leased for the other schools from the neighboring towns of Mayberry, RagsToRiches, and Ghostown.

Approximately 4000 students are educated yearly within the 7 schools. Roughly 380 faculty and 200 staff personnel support those students through their academic and administrative activities.

The primary business is public education – a service to the community. Accounting of income and expenses determines the cost per student, which is used to calculate the school district taxpayer contribution to the budget. The vocational/technical school provides services to other communities, and has a different fee structure. Those towns that are out-of-district pay the normal cost per student, plus an additional surcharge of around $3000.

Even with a limited budget, the school system attempts to be innovative in its use of technology. Investments are made on a yearly basis. The Career and Technical School already has a high-technology focus, and provides training tracks that can lead to technical certifications. The other schools are also making computers an important tool in the educational process. Computers and technology provide a significant value to the school's educational offerings. The cost of having technology is not well understood, and as a result, the technology is not well maintained.

Additional business operations are also necessary for the district to carry out its primary mission. These include: student transportation, dining services, and administrative services.

IT software development and operations are managed by the Technology department. The department has a staff of four, which includes a Director, Network Administrator, and two PC Technicians. Support is provided

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

centrally from their office in the Career and Technical School. Infrastructure within the GIAC campus has good service levels. Those service levels are not maintained for infrastructure located at the remote locations.

2.2 IT Infrastructure

Technical infrastructure should be in place to support the business operations of the school in a safe and secure manner. Each component of the IT infrastructure needs to be reviewed from a security perspective. The threats, countermeasures, and vulnerabilities need to be identified at the component level of that architecture. Existing solutions will be identified as part of a general landscape of typical security architecture. The following sections correspond to key elements of that landscape.

Before going into each component assessment, the set of common exploits used by hackers, viruses, and worms will be summarized. These exploits are discussed in more detail in Hacking Exposed[1]. These threats challenge the design and construction detail of the GIAC IT infrastructure. By keeping these well-known threats in mind, vulnerabilities can be discovered and risks can be prioritized.

- Footprinting – gathering the information leakage
- Scanning – probing for network, system, operating system, and services
- Enumeration – probing for well known host configurations and software version vulnerabilities without need for authentication
- Penetration – logging in and operating as an authenticated user
- Denial-of-Service – disruption in services
- Privilege escalation – gaining administrative access after penetration or as a result of denial-of-service.
- Pilfering – gathering information as an authenticated user or administrator
- Covering tracks – using privilege and access to alter logs and system state
- Back doors – altering system security to provide a targeted approach to penetration and privilege escalation

2.2.1 Perimeter

The first line of defense for an IT infrastructure is the perimeter. Outsiders must penetrate the perimeter defense before any attack can be successful to the internal network and internal assets. The outside attack surface is limited to vulnerabilities on those servers and services which need to be served to the public network. The diagram below details the perimeter network, and the perimeter controls which come into play. Later in this section, the elements of the perimeter architecture are explored in depth.

[1] Hacking Exposed – Network Security Secrets & Solutions; Osborne/McGraw-Hill, 2001

SANS Institute 2003 GIAC Practical Repository Author retains full rights

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

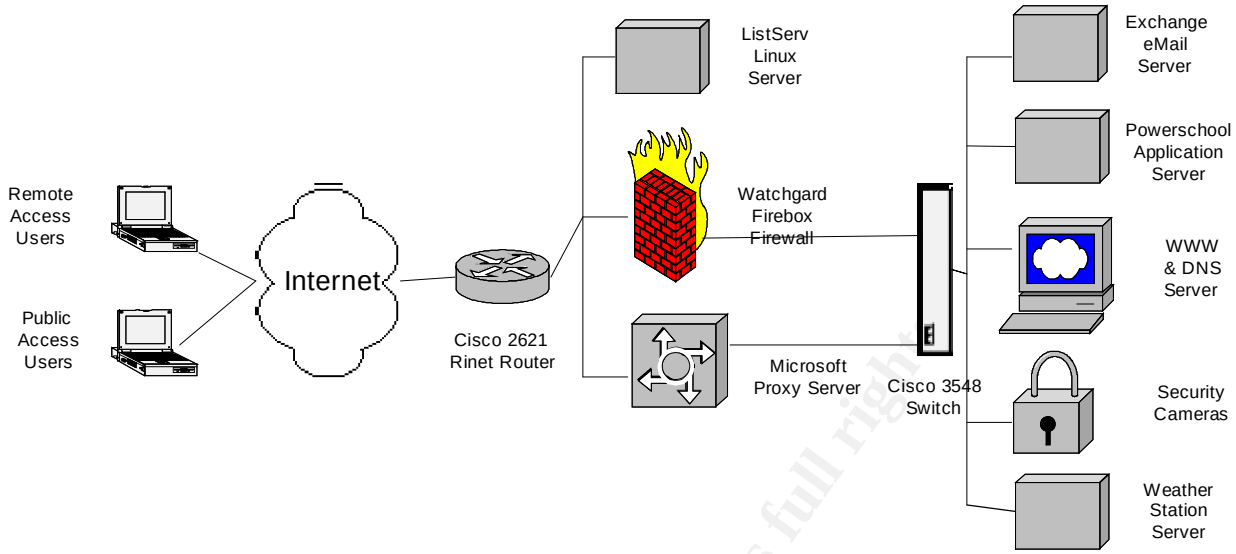

Figure 1 – GIAC Regional School District Perimeter Network

Border Controls

The district's IT infrastructure has only one perimeter, and one border edge router. The Cisco 2621 serves this purpose, and is administrated by the RInet, a local Internet Service Provider (ISP). Only one link and router exists, which represents a single point of failure for all services dependent to Internet access.

The ISP should be providing a service to the district in their management of this important element of infrastructure. This border control lacks any protocol filters that would limit the attack surface of the district's network from the Internet.

De-Militarized Zone

A De-Militarized Zone (DMZ) can be used to protect hosts and services from external threats, and further protect the GIAC network in the event that the host compromised. GIAC does not use the DNZ network model, and simply routes public connections to internal servers using the firewall.

The DMZ network model is typically used for email gateways, publicly accessible web servers, and external domain name services. Many of these services exist at GIAC, but have been implemented without the benefits of this security-in-depth design.

While much of the benefit of the DMZ model is network isolation, it does provide guidance on the rules for construction and the rules for on-going maintenance. DMZ hosts are typically stripped down to the needed services, and fortified to withstand constant attacks from the Internet.

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

Firewall Controls

At the time of this assessment, there are two different information flows to/from the perimeter network and the internal network. Outbound flows from web browsers are directed to the Microsoft Proxy Server using browser proxy settings. All other outbound flows are directed to the Firebox Firewall. Inbound flows destine to the Proxy Server complete web browser Internet session, and are thereby forwarded internally. All other inbound connections are only possible with addresses created through the firewall's Network Address Translation process. In those cases, inbound flows enter the Firebox, are filtered, and subsequently routed into the internal network.

The two forms of firewall controls do not provide any redundancy. Both implementations are single points of failure. Any services that depend on internet access will be impacted when the proxy or firewall are down. Failure does not create other vulnerabilities since down services guarantee network isolation.

The district does use non-routable addresses for all its internal servers and desktops. The use of non-routable internal addresses limits the possibility of unauthorized connections between internal devices and other third-party networks, like the Internet.

The Microsoft Proxy Server performs a limited set of firewall controls. Inbound connections are only served for dynamic ports still in service – those with live connections to internal web browser sessions. Outbound connections are allowed without filtering. One of the primary benefits of the proxy server is caching. Content is temporarily cached for possible re-use, limiting bandwidth consumption. This service is being phased out. Once transition is complete, all inbound and outbound flows will go through the Firebox Firewall.

The Watchguard Firebox Firewall is the primary defense to the internal network. It provides packet filtering in support of the district's public and semi-public applications. The following summarizes the rules that are defined in the Firebox:

- By default, all inbound connections are denied.
- By default, all outbound connections are allowed.
- Public access is provided to the school's Weather Station
- Public connections are allowed to the school's security cameras.
- Public domain name resolution is permitted using internal services.
- Public access to the school's public web server is allowed.
- Public access to the email system is allowed.
- Inbound and outbound Internet mail services are permitted.
- HP support team is allowed access to internal servers.
- Public access is permitted to the Powerschool application server.

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

- IT support staff and select administrators are allowed remote access to the internal network.
- Anyone can connect to the firewalls authentication services (used for remote access).

The liberal outbound connection policy needs to be revisited. Trojans or other malicious code could setup camp on the internal network, and easily integrate with other elements within the Internet.

Most proxy implementations are further supported by traditional packet filtering firewall. This bypass design is problematic, and weakens the border. The school has almost completed the plan to eliminate the bypass, thereby eliminating this issue.

Internal support for the firewall is limited. Only one staff member supports the firewall, and the level of training may not be appropriate to the importance of the firewall to the district.

Intrusion Detection

The internal network is not protected by an Intrusion Detection System. No automated monitor and response process has been implemented, and none are being planned.

At any point in the network, access control either allows the connection or not. The sequence of connections and overall activity is not a basis for the access control decision. Complex attacks may be launched to bypass the simplistic access control and probe further for infrastructure and application vulnerabilities. Worse case, the attacks will be successful, and generate information disclosure, modification, or destruction. IDS systems provide this additional activity monitoring, and integrate with automated security response mechanisms.

There are many consequences to providing access to the Internet from GIAC students, faculty, and staff. Outbound access can be monitored to limit impact to Internet services, and better support the Acceptable Use policy. The district monitors and automatically filters outbound HTTP access using the 8e6 third-party service. The service supports filtering rules based on pre-defined categories. The service periodically monitors the Internet and categorizes web sites. The site and category information become data to the product and service. The district is then allowed to set rules based on the vendor maintained categories. The district maintains some override information for sites to be allowed from a blocked category, or sites to be restricted from an allowed category.

The current outbound solution only manages HTTP, and simply blocks access to web sites. The complete benefits of IDS are not provided.

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

Internet attacks may be successfully launched from the GIAC network without detection and appropriate response.

Remote Access
The Firebox firewall provides remote access services to 6 staff personnel. Remote access users must install and configure the Microsoft Virtual Private Networking (VPN) client on their home PCs, Each user is given a unique account and password. Once authenticated, the remote access user is given unlimited access to the internal network. The password policy is not currently known.

The security state of these remote access clients is unknown. Vulnerabilities may exist which allow the client to be compromised, and be the launch point for internal attacks once the remote access client is connected. Security configuration standards should be made for these remote access clients. User rights to remote access services should be reserved to those who support these security standards.

Dialup Access
Dialup access is provided for faculty and staff through an Internet Service Provider. Dialup users have Internet access, and may access the internal network only if they are a remote access user. Otherwise, access is restricted to the Internet, and those public and semi-public services offered by the district.

2.2.2 Enterprise WAN

The internal network is a combination of six different networks. Each of the four elementary schools has a small local area network. The GIAC campus has a large local area network. These five sites are all connected using a Verizon frame relay network. The internal network connects to the perimeter network at the GIAC campus. The Verizon frame relay network provides that perimeter connection as well.

The district provides many competing services over its internal network. Some traffic separation is designed into the WAN. Each of the elementary schools has a dedicated pipe to the GIAC campus. Some virtual local area networks (VLANs) have been defined. A Voice over IP VLAN is being planned, but has not been implemented yet. As implemented, the VLANs simply manage flow, and do not filter traffic. Any node on the internal network can connect to any other node. The existing VLANs are:

- Administration Network
- Academic Network
- Security Cameras
- VLAN Management
- VLAN Trunking

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

At present, some infrastructure provides services to faculty, staff, and students. The implementation creates strong dependencies between the Administration and Academic Networks. Once some of these services are re-hosted, the faculty and staff should be serviced out of the Administration network and the students should be serviced out of the Academic network.

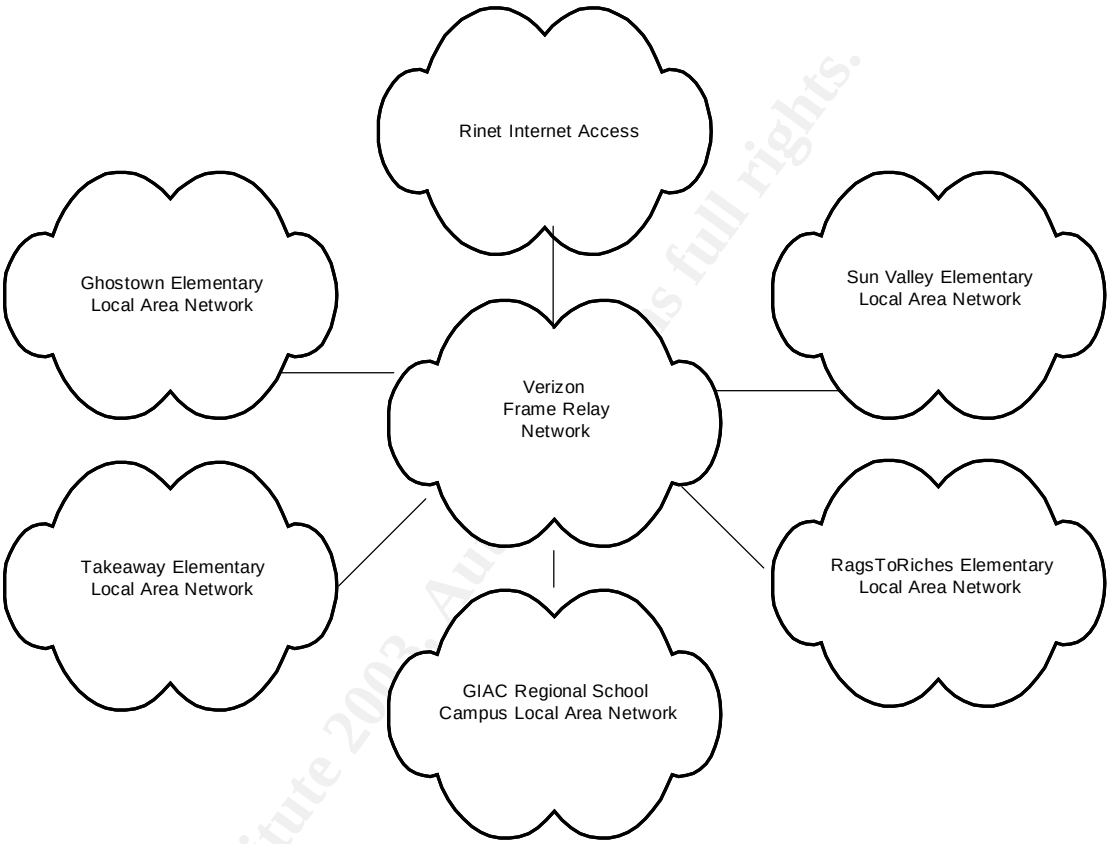

Figure 2 – GIAC School District Site Map

2.2.3 Computers

The computers that are resident on the GIAC network take the form of desktops, laptops, or servers. Each category of computer is detailed in its own section below.

While the staff recognizes the benefit of infrastructure standardization, it has to accept a mix of new and old computers, from a host of vendors. The mix of technology increases the burden on the staff. The older equipment has limited upgrade paths, and further constrains operating system upgrades, installation of patches, and installation of security software. System defaults are often applied and there is little time or training in computer hardening.

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

Client Computers

Approximately 800 desktop computers and 12 laptops can be found within the internal network. There are also 15 palm pilots that synchronize with Outlook, the desktop email client. The rough breakdown of operating systems is as follows:

- 640 Windows 95
- 80 Windows 98
- 80 Windows 2000

The desktop build is the vendor provided default. No "best practice" hardening of the desktop has been performed. Microsoft has placed Windows 95 and 98 into retirement. Available security patches have not been applied. Many vulnerabilities exist that can be exploited by viruses and other malware.

Desktop images and configurations are protected using the Fortres 101 and Clean Slate. Administrators manage this security configuration using Central Control.

Some of the administrators have dedicated PCs. Most desktops are allocated to classrooms, computer labs, and libraries, and are shared by everyone.

Only 80 of the 800 desktops have up-to-date Anti-Virus software. A few of the administrators have PCs with modems. No PCs are backed up, so recovery is through a re-imaging and rebuild process.

Servers

The district has 16 servers running a mix of operating systems. The breakdown is as follows:

- 6 Windows NT 4.0 (SP6a)
- 6 Windows 2000 (SP2 and SP3)
- 2 Linux Redhat (7.0 and 8.0)
- 1 HP-UX (11.0)

Server builds are the vendor provided default. No "best practice" hardening of the servers has been performed. The operating systems are modern, but available security patches have not been applied. Some vulnerabilities exist that can be exploited by viruses and other malicious activity.

Not all servers are backed up, and the backup schedule and retention varies from server to server. Backup software and tape drives are not available on all systems.

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

Unlike clients, servers are periodically monitored for performance and operational events.

2.2.4 Anti-viral Controls

A hit and miss anti-virus defense exists at GIAC. The implementation lacks anti-virus solutions in many places, and does lead to regular virus outbreaks and detections. Due to the gaps, virus eradication is almost impossible.

Many of the desktops and file servers are running out-of-date virus software. AV software contains an engine and data file component which would be updated regularly by the vendor. The engine is the programming for the software to handle the new types of viruses. The data provides information about the signatures that known viruses have had. When AV software is out of date, it does not get these updated engines and data files. New types and instances of viruses are not properly handled with out-of-date AV protection.

A mix of AV products and vendors exist within the district. The lack of standardization makes it difficult to assess the district's readiness for an Internet virus outbreak. A standard should be selected, and the gaps defined herein should be closed with investments in that standard product set.

A security-in-depth design has not been implemented. The core email system is Internet facing, and must defend the district from email virus threats. Viruses that are present in infected or malicious Internet web sites must be handled at the desktop or laptop. The mail (SMTP) and web (HTTP) information flows are not inspected for viruses by dedicated servers at the border of the network.

Desktops and Laptops

Roughly 640 of the 800 (80%) desktops do not have AV software. About another 10% have out of date AV software. That leaves around 80 of 800 desktops that have adequate AV protection. The six laptops have up-to-date virus software. The AV software which is on desktops and laptops came with the computer when it was purchased.

The desktops are the weakest link, and are causing viruses to be brought into the internal network. The internal network is not isolated from these infected desktops, and core services are prey to the virus payload.

File Servers

Some of the file servers are running out-of-date virus software. Viruses may be present in files stored on the servers with out-of-date AV

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

protection. Eradication will not be possible until all of these servers have the appropriate AV software.

Desktop AV software is used as a workaround to eradicate viruses located in file shares. File shares are successfully cleaned using the process, but are not further protected from re-infection.

File services are not provided from dedicated servers. The servers which provide file services also provide other critical services to the district. The other services provided are: domain authentication, IP dynamic address renewal, and applications. The virus payload can cause considerably more harm when activated on these mixed role servers.

Email Servers
The district has one email server, and that server does have up-to-date AV protection. Additionally, the email servers block the sending or receiving of executables, a common hiding place for viruses.

Web Content and Transmission
Internet web content may be infected with viruses or malicious in nature. The 8e6 third-party service does block some malicious web sites. The district does not block Internet web mail sites. Some of these sites may have AV protection. Many do not. The likely transmission of viruses to the desktop and laptops using HTTP further justifies the need for client AV protection.

Web proxies are often used to manage Internet web content flows and better integrate AV protections and other forms of content filtering. The district is retiring its Microsoft Proxy implementation. No plans exist for a replacement proxy service.

2.2.5 Encryption and Use of Public Key Infrastructure

No Public Key Infrastructure exists, and no encryption services have been implemented. Sensitive data, including network and application login credentials, are transmitted in clear text over the network.

Eavesdropping attacks can easily be launched allowing unauthorized users access to this sensitive data from the internal network.

2.3 Business Operations

In order for the district to carry forward its mission, it must gather, process, and further protect a number of information assets. In this section, the most sensitive information will be declared. The flows of information will then be presented, along with the applications and types of access which manage those flows.

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

2.3.1 Sensitive Information

Detailed below are the key information assets that the GIAC Regional School District has to protect.

Student Records

A full student record exists for each of the 5000 active students serviced, containing contact information, medical information, class assignments, attendance, grades, discipline, and historical information. Medicaid information exists for some special needs students, and is used to bill back for medical services rendered. Grades and other performance information must be maintained with high integrity. Most of the information is either private or confidential, with access limited on a need-to-know basis.

Administrators within each of the schools create the initial record for the student, and maintain most of the information not relevant to class performance. A number of business processes require administrators to read the student record. Teachers perform the update of grades and other classroom performance information. Access for students and parents is being considered, but is not currently implemented. Students and parents currently receive information contained in the student record using canned reports, such as Report Cards.

Special Education Information

When a student requests or is provided special education services, a student special education record maintained. Services are coordinated through district, state, and federal resources. Information is maintained on the interaction of these resources and the status of the services.

Special education information must be of high integrity and limited to the students, parents, and administrators that will deliver or consume the program services.

Employee Records

The district employs approximately 580 faculty and staff. Each employee must be managed, and has a corresponding employee record containing: contact information, salary, medical information, performance information, and benefit information. To service automatic deposit, the employee's banking information may also be maintained. Salary and banking information must be maintained with high integrity. All personnel information is private or confidential, with access limited on a need-to-know

Administrators within the Central Office maintain employee records. Employees do not have access, and simply receive information from standard reports, such as Paychecks and W2s.

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

Accounting Records
Accounting is performed to manage the district's finances. The accounting process requires public disclosure so that taxpayers understand the school district's budget, and its impact to town taxes. Accounting records must be maintained with high integrity. Some information, such as employee salaries and bank account information are considered private or confidential, with access limited on a need-to-know basis.

Public Records
The district is required to disclose information to the public. Public records must be maintained with high integrity, and may need to be available when the public needs them. No private or otherwise confidential data element should be included within the public records. Only data of classification "public" should be included.

Much of the data that is made public is the outcome of internal processes which construct, review, and approve of its content. No uniform process or system manages this publishing. Content management should be considered.

Service Records
The district provides a number of services which may obtain or otherwise process sensitive information. Included below is a list of some of these services: Much of this information is considered private or confidential, with access limited on a need-to-know basis.

- Financial aid and other assistance
- HIV infection
- Substance abuse
- Pregnancy
- Sexual harassment
- Abused and neglected children
- Suicide and other crisis intervention
- Physical or mental impairment

2.3.2 Applications and Core Services

Detailed below are the applications and core services that enable business operations and information processing.

Powerschool and Powergrade
Student records are maintained using the Powerschool application by Apple Computer. The application is built as a Microsoft IIS Web service on the POWERSCHOOL Windows 2000 server. The application supports both Internet web browsers and the Powergrade desktop application. Each web user has a unique username and password. The password

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

policy for the application is weak. The password is short, based on user's SSN, and does not age. The Powergrade desktop application is installed with a connectivity key, which works like a password. The key enables access to a collection of Powerschool data without need of the web username/password login. The keys are assigned and installed by the Application Administrator.

Sensitive data is transmitted from the Powerschool application web service to the client in clear text. No encryption is used during application login or in the processing of private and confidential information.

The application is primarily used within the internal GIAC network. To allow administrators and teachers to work from home, the Powerschool application has been connected to the Internet.

Most usernames are public knowledge and the passwords are easily guessed. Methods are readily available to eavesdrop on the application login and other sensitive transactions. Using the exploit, unauthorized users may harvest valid user accounts and passwords. Any unattended and unlocked Powergrade desktop may be used to access student records without the need of a valid username and password.

Skools

Employee and accounting records are maintained by Keystone Information Systems Skools application. Skools is on server HP, running HP-UX. The application supports all payroll, personnel, general ledger, accounts payable, purchase requisitioning, and procurement functions needed within the district.

All faculty and staff can submit purchase requisitions. Building administrators are level-1 approvers for purchase requests. . Central office personnel are level-2 approvers, and also manage salaries.

Users must first initiate a terminal session with the HP server using the TELNET protocol. Each user is given a UNIX account and password, and must login to the server at the start of the terminal session. The password policy is unknown at this time. The character-cell application utilizes a secure menu system, and presents menu options based on the user's entitlement.

The TELNET session requires a username/password login sequence that is transmitted in clear text over the internal network. The TELNET login and any sensitive transaction are visible in clear text. Unauthorized users can eavesdrop on the login and transactions. Unauthorized users can harvest valid usernames and passwords.

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

Proprietary Special Education Program
Student Special Education processing is managed using a proprietary application, built as an extension to the Skools software package. Like Skools, the program runs on server HP, and utilizes HP-UX Unix user identifiers and passwords. The menu system manages access control to special education functions.

The issues of a weak UNIX password policy and clear-text TELNET session also apply here.

Follett
Library automation is managed by the FOLLETT application. Access is provided using a web browser or PC client software. Six separate installations of FOLLETT are used to manage the individual library inventories of each school. Each installation contains an application web server and a Farcona database server.

Web users get read access to the school's library. Some of the PC client software allows update capabilities, and is password protected.

The librarian maintains the library using the FOLLETT software and has the necessary program passwords. Students are the primary consumer and access the application anonymously. Since the library is considered a resource to the community, the Public Web Site allows the public to search for books of interest.

FOLLETT manages the asset inventory of books purchased or on loan to the school. Library records must be managed with high integrity.

Public Web Site
GIAC hosts a web site on the Internet for public access to its public records. The SUPERMARIO server services the web site, and runs Windows 2000 and Microsoft's IIS web service.

The site contains primarily static HTML and PDF content. Microsoft's Frontpage and Netscape's Composer allow web publishers to draft and preview content before it is implemented.

The site is broken up into a number of sub-webs. Individual webmasters manage their particular sub-web. A webmaster manages the root of the site, and is also a backup to the sub-web webmasters.

No standards or guidelines assist the webmasters in the maintenance of the web site. The rules governing content Integrity and the filtering of sensitive information are up to each webmaster. The Superintendent

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

does monitor the web site and provide feedback and recommendations to the webmasters.

The site contains names, phone numbers, and email addresses for faculty, staff, and parents. Some personal student information is also present. Information should be formally classified, and web publishing should only include content of type "public".

Electronic Mail Services

Each faculty and staff member gets a mailbox on the district's Exchange server. The mailbox allows for the individual composition and receipt of email, and access to directory and public folder services. The Exchange directory maintains the district contact information. Public folders support a number of applications, including: synchronization of contact information to hand-held PDAs, staff and faculty collaboration, administrative workflow and service requests, and a poor mans file share.

The Exchange mail server is configured to support MAPI, POP3, and IMAP mail client connections. Web browser users can also read and send mail by connecting to the Outlook Web Access web service (using HTTP). Services are primarily offered internally. To allow staff and faculty to perform work at home, the Exchange server also Internet facing.

The authentication source for Exchange is the Windows Domain. The domain has a weak password policy, which may allow unauthorized users access to district email. Additionally, potentially sensitive email is transmitted in clear text over untrusted networks. Man-in-the-middle eavesdropping is possible, violating the privacy and confidentiality of this information.

File Share Services

All faculty, staff, and students get a personal network file share. Students perform much of their school work using these services. Administrators and faculty use this area for ad-hoc tasks and activity.

The Windows Domain provides authentication services to file share access control. Due to the weak password policy in the domain, unauthorized users can access content on a user's file share.

Weather Station

GIAC is part of WeatherNet, and has a weather station connected to the Internet. The AWS web site performs the back-end integration to the weather station, and displays the weather related data in their web application,

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

The weather station is not directly visible to the general user. Its name and address are never seen through the AWS web site. The service runs as an appliance and utilizes a restricted port and protocol. Security is more than adequate given these safeguards.

Mail List Services

The district has created a number of mailing lists, and has an automated mailing list manager, also known as a Listserv. MailMan 2.0.10 provides the Listserv automation. Requests must be sent to the Technology Department to create new lists. Members can add or remove themselves from the mailing lists by sending mail and including commands.

Mail list services are hosted on the LISTSERV server. The server is outside the firewall, and is running an out of date version of Redhat Linux. Vulnerabilities do exist on the server, which can be easily exposed. As a result, the integrity and availability of mail list services can be compromised.

3 RISKS

Risk models narrow our focus on particular areas of our security-in-depth design. The weaknesses in these areas become the priority for risk improvements.

3.1 Areas of Risks

Given the nature of the business operations, there are a number of threats and risks that come with the territory, and are not reflective of vulnerabilities that may exist within applications or infrastructure. The threats will be grouped by type of user.

Students present the biggest insider threat. They may attempt to modify their own grades, disclose information about another student, teacher, or staff member, or tamper with security controls “just-for-fun”.

Employees have significant rights within the district’s applications, and may cause impact due to “accidents”. The more resilient the application, the less chance there is for employee accidents. Security awareness and training can increase their readiness and set clear expectations of their responsibilities.

Trusted third-parties have access to the internal network, and may have remote access through the Internet. Third-parties may not always act in the best interest of the district and may cause impact due to their access rights.

The general public has access to the district’s buildings, and may have access to computers and network connections. The public is made aware of the public web site and is encouraged to use it as a community service.

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

Most Internet attacks and virus outbreaks are blind to the organizations they impact. All that is needed is to open Internet ports and access to Internet-facing applications and services.

3.2 Prioritation and Selection

The review of technical infrastructure, applications, and core services has discovered numerous vulnerabilities that may be exposed. Some attack methods are more difficult than others. The probability that the attack will be launched is also a factor. High risks involve well known vulnerabilities.

3.2.1 Risk 1: Viruses and other Malicous Code can and do exist.

Rating

Risk is HIGH, due to a HIGH probability, LOW effort, and HIGH impact

Description

Viruses are imbedded programs written by malicious outsiders in an attempt to exploit vulnerabilities found in most organizations. Viruses are most often found in email, but can be elements of web content transmitted to the web browser or propagate over a network connection. When a virus is activated, it can propagate itself and compromise vulnerable services and applications. There is a high risk that viruses will impact GIAC services and applications, and could lead to breach in confidentiality, integrity, or availability of information assets.

Justification

According to MessageLabs, one out of every 29 email messages contains a virus.[2] Viruses are the top form of security attack detected at most organizations.[3] GIAC has a hit or miss anti-virus defense. Virus outbreaks are occurring. Through many avenues, viruses can be downloaded to desktops and stored in file shares. Activation can occur from any of these places, and impact any service or application which is on the internal network. The lack of outbound Internet firewall filtering allows viruses to take the form of Trojans, and connect out to the Internet for more instructions and integration with more complex attacks.

Possible Impacts

Viruses and other malicious code can impact the confidentiality, integrity, and availability of most of the district's information assets.

When viruses are activated by a user, the virus runs with the user's rights and can impact any resource the user has access to. Since desktop anti-virus protection is so weak, any user at GIAC may activate a virus, and

[2] MessageLabs Intelligence, August 2003.
[3] 2003 CSI/FBI Computer Crime and Security Survey, page 10.

SANS Institute 2003 GIAC Practical Repository Author retains full rights

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

any network resource can be impacted. GIAC network resources include: electronic mail, file share services, and content management for the public web site.

Viruses often probe for the services within the network the user has access to. Well known and published vulnerabilities exist on most servers. Any of these servers can be compromised, and therefore impact the information serviced and protected on them.

The W32/BugBear.B virus, for instance, installs a key-logging Trojan, permitting the attacker to obtain a file of the user's keystrokes. Sensitive data exchanges, such as network and application login, or credit card information, may be captured and later used.

Recommendations
Any form of technical infrastructure that can receive or store a virus must either have up-to-date virus protection, or be removed from the internal network.

Servers or services that allow connections from unprotected infrastructure should have up-to-date patches, be stripped of unnecessary services, and be sufficiently hardened.

Users of unprotected systems must be notified that the system cannot be trusted, and to use more protected systems when dealing with sensitive data. Faculty and staff need infrastructure with AV protection.

3.2.2 Risk 2: Unauthorized users can use or steal an authorized user's identity

Rating
Risk is HIGH, due to a HIGH probability, LOW effort, and HIGH impact

Description
Restricted information is supported by authorization controls that understand a user's identity and entitlement, and grant access only when appropriate. Authorization depends on authentication to establish clear identity before providing access. Weak authentication controls have been implemented, and can easily be manipulated to allow an unauthorized user to run with an authorized user's identity.

Justification
In almost all cases, authentication controls rely on a user identification using a single-factor shared secret called a password. The user's username may be very easy for an unauthorized user to determine. The default settings in Microsoft Windows allow an anonymous user to

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

enumerate all usernames within a domain[4] Password policy typically guarantees the secrecy of a user's password. The password policy used at GIAC does little to guarantee the secrecy, and instead enables the password to be calculated for most users. A convention exists to use a small portion of the user's SSN as the password. Both the minimal length and use of a convention makes it highly probable that unauthorized users can determine a password of another user.

Users within the district do not manage their password well either. They allow their account to be freely used by others, and do share their password. Once the password is shared, the user looses control of the password, and further disclosure may occur without the knowledge of the user.

Since the password is static, and the user does not obtain any audit of account usage, an unauthorized user may be using their account indefinitely without detection.

Possible Impacts
All network and application services trust the user's identification after a successful authentication and provide access. Any asset that the original user is entitled to is fair game for the unauthorized user. Disclosure, modification, and destruction of information assets may result.

Recommendations
The network and application password policy should define rules for password complexity, length, aging, and history to help maintain the secrecy of a user's password. A compound password, such as a multi-word or mix of letters and numbers, should be used. A minimum password length of 6, and password expiration of 90 days or less should be implemented. The system should maintain knowledge of the last 5 passwords, and prohibit the user from using any of these recent passwords.

Users should be given the responsibility for their password, and given consequences when the user inappropriately shares their account with other users.

Periodic auditing of the existing passwords should be performed to guarantee compliance with password policy. Causes for non-compliance should be researched, and appropriate action should be taken.

3.2.3 Risk 3: Compromised Public/ Semi-Public Servers can be used for an internal attack

[4] Hacking Exposed – Network Security Secrets & Solutions; Osborne/McGraw-Hill, 2001

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

Rating
Risk is MEDIUM, due to a HIGH probability, MEDIUM effort, and HIGH impact

Description
The GIAC public and semi-public services are delivered using internal servers and filtered external connections. If these servers are compromised by an external user, those servers can be used as a launch point for attacks on the internal network.

Justification
Connectivity within the internal network is not filtered. Any internal network device can connect to any other internal network device using a number of network transports and ports.

Almost all network devices and services are installed with vendor defaults, and have known software and configuration vulnerabilities that can be easily exposed by viruses, spy ware, and other forms of malicious code.

No outbound (egress) filtering of Internet connections for the internal network is performed. A compromised server can be easily integrated with Internet-based malicious infrastructure.

Possible Impacts
These systems provide public and semi-public services. They will be exposed to threats that other internal systems will not. This will be a risk inherent in their function.

The real impact to this risk is from the placement of these servers inside the internal network. These servers are trusted in the internal network, and when compromised, allows an attacker to further impact any and all assets that may be exposed from that trust.

The extent of the trust of the public and semi-public servers to the rest of the internal network is not known at this time. The network is wide open, however. Any exploit code which is installed on a compromised public and semi-public server can easily identify vulnerabilities that exist on other internal servers, and target those serves for further attacks.

Recommendations
The primary audience for semi-public services is internal users, namely staff and faculty. Electronic mail access and Powerschool application access are provided over an unprotected and unsecured Internet. These services should be limited to the internal network

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

Remote users may need access to these services when at home or on the road. Expanded access to remote access services should be considered to provide access to the services after they are isolated to the internal network. Remote clients must be resilient to these outsider threats, and must not be in a compromised state at the time of remote access to the internal network.

The Firebox firewall should be configured to support an isolated DMZ network. Public servers should be moved to that network. One obvious candidate for the DMZ is Supermario, which hosts the district's public web site and external DNS services.

The working assumption is that the Weather Station and security cameras are sufficiently hardened and isolated, and may not need to be transitioned to the DMZ at this time.

4 EVALUATE AND REFINE SECURITY POLICY

4.1 Overview

Existing policies are owned and approved within the School Committee. Policies must be made public by district charter, and any exceptions to policy must be approved by the majority of the School Committee.

Policies are published in sections that correspond to functional areas of the school's organization. There is not currently a section that includes policy that targets all users and all functional areas.

The Superintendent is the assigned the responsibility of running the school, and implementing the policies.

4.2 Evaluate Policy

Most of the GIAC policies and procedures target requirements for critical functions that must exist within the school system. In that context, behavior and the protection of certain sensitive information is discussed. Only one policy deals with the risks defined above, and will be evaluated in the following section.

4.2.1 Section VI – Students – Internet Use Policy

Description

The Internet Use Policy defines the terms and conditions for acceptable use of Internet services and technology. It is targeted for students, and must be signed by each student annually. Students are reminded of their responsibilities, and are given consequences for potential violations of the policy. The existing policy is included in its entirety in the Appendix of this assessment.

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

Support to Risks
GIAC has a weak password policy and other infrastructure vulnerabilities that could be the target of unacceptable behavior or accidents. This policy attempts to deal with such abuse.

Internal users present a medium threat to the risks identified above. This policy defines responsibilities and establishes consequences when students are found to abuse their access. The process which distributes the policy and obtains signage is an annual reminder of this mandate.

The policy helps to set the stage for Acceptable Use. It provides a basis for the requirements for all users of the district's assets.

Gap
The scope of the policy should be changed from Internet Use to Acceptable Use, and should contain Internet Usage as one section of the overall policy. The following changes should be applied.

- Audience should be expanded to all internal and external users.
- Usage should be restricted to the user's authorization and entitlement.
- Should limit use of electronic mail to district business.
- Should define need for license compliance.
- Should mandate due diligence.
- Should have stronger penalties.
- Should mandate that breaches be reported.

4.3 Revise Security Policy

No information security function or vision has been defined as part of the school's charter. No policies dictate the set of protective, detective, or reactive controls that must exist to manage risks to the district's sensitive information. The existence of formal Policy and Procedure reflects the district's interest in a set of managerial controls in support of district operations. Policies do place constraints on a number of functional areas. In most case, the policies are combined with procedures to define, at a level of measurement, the activities of functions in dealing with sensitive information.

This section will introduce policy elements that will clarify the goals for information security. The application of these policies will evolve a set of security configuration standards and maintenance procedures. Those standards and procedures will provide the managerial controls necessary to manage the risks to information assets.

4.3.1 Section VIII– Information Security – The Vision

Description

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

The Information Security Vision sets forth the elements necessary for risks to be known and properly managed. Each of the functional areas within the district seeks to maximize services while living within their chartered responsibilities. Some functions do manage sensitive information, and apply diligence in their processes. The focus to clarify risk and properly manage risk extends support beyond discrete functional areas.

Support to Risks
The Information Security Vision makes it everyone's business to secure sensitive information. The policies as written provide little separation of duties to ensure that information is secure. This vision statement and its family of program policies provide the checks and balances so that risks are dealt with.

The district charter and existing policies and procedures define the primary functions and responsibilities for each user in the organization. By creating a separate policy section and documented vision for information security, all users can see clearly their secondary responsibilities. Existing policy and procedure can then be revised with information security in mind, and provide additional measurement and managerial control.

The vision is the highest level of requirements for information security. This policy establishes a broad mandate, and allows other policies to focus on critical areas as the need arises.

Recommendation
A Vision statement should be created to state the district's value for information and its mandate that information be secure. The proposed vision statement is included in the appendix.

4.3.2 Section VIII –Information Security– Risk Assessment

Description
Risks must be known before risks can be managed. The knowledge of risk comes from the testing of security controls. The Risk Assessment policy establishes the requirements for this testing, and provides the key areas of testing results needed to understand risk. Risk decisions are made based on the results of a risk assessment. Managerial and technical controls evolve from decisions to invest in security.

Support to Risks
Risk Assessments provide clarity in risk. Without risk assessments, risks will be unknown and not be managed. By detailing the requirements for risk assessments, uniform definition for risks can be achieved, and consistency in risk decisions can be provided.

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

The state of the district's technical infrastructure and applications suggest that risk has not been a key element in the decision-making. By creating clear policy on the need for risk information, the "costs" of progressive use of technology and the Internet can be balanced with the benefits.

This security proposal provides a high-level assessment of the security at the GIAC Regional School District. Risks have been identified. These policy and procedure recommendations provide the next steps to risk remediation. This assessment has only scratched the surface. Continued application of the Risk Assessment policy will detail additional areas for risk improvement.

Recommendation
A policy should be created to establish when, where, and how to assess for risks. The relative value of the information being protected must be known. The probable threats to those assets must be identified. The strength of any countermeasures to those threats must be assessed. Through assessment, vulnerabilities are discovered. Thresholds for vulnerabilities need to be declared using a minimum security baseline. Assessments must recommend additional safeguards when the baseline is exceeded.

A proposed policy can be found in the appendix.

4.3.3 Section VIII –Information Security– User Management

Description
Users must identify themselves uniquely to the system so that access control and auditing can properly manage their entitlement and track their activities. Unauthorized users can be denied access to the system only when authentication credentials for authorized users are not known by others and not easily guessed. The User Management policy establishes the requirements for creation, maintenance, and removal of user accounts.

Support to Risks
Access control and auditing have little value if users are not properly managed. The User Management policy establishes mandates so that users are properly managed.

The district has taken a simplified approach to user management. This approach has made the control ineffective. By making it easy for the users and administrators to know their password, unauthorized users can exercise guessing attacks, and gain access to sensitive information. This policy will force a change, and provide guarantees that access is only being provided on a "need-to-know" basis.

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

Recommendation

The User Management policy must be created to define the rules for password complexity, length, aging, and history in order to help maintain the secrecy of a user's password. A compound password, such as a multi-word or mix of letters and numbers, will be recommended. A minimum password length of 6, and password expiration of 90 days or less must be used. The system should maintain knowledge of the last 5 passwords, and prohibit the user from using any of their recent passwords.

All users must be given the responsibility for their password, and given consequences when the user inappropriately shares their account with other users.

Periodic auditing of the existing passwords must be performed to guarantee compliance with password policy. Causes for non-compliance should be researched, and appropriate action must be taken.

4.3.4 Section VIII –Information Security– Network Security

Description

The district has a complex wide area network, integrating internal and external users and services. The access to the extended network is outside the control of the district, and introduces threats to the district's operations and information assets. The district also has insider threats to information assets. These threats and risks can only be managed when security is applied within its network services. The Network Security policy mandates elements in the network design and operations.

Support to Risks

Client and servers within the GIAC internal network have high-risk vulnerabilities. Network Security will provide safeguards that unauthorized users cannot access these systems, and therefore, not exploit the vulnerabilities.

Two of the three risks identified in this security proposal can be reduced by advancements in network security. Viruses enter the district by transmission through the network. Network security can contain or filter these transmissions. Internet services are provided by internal hosts. Network security can isolate these hosts in the event that they are compromised.

The district lacks sufficient resources to strengthen security at all elements of its infrastructure and applications. This policy sets a priority for network security solutions as a means to reduce risks. The internal network may need to be segmented so that risks and threats can be isolated, and the security of sensitive information can be ensured.

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

Recommendation

The Network Security Policy must value information assets and control access based on the trust of the systems and users. The internal network must be modeled as isolated zones of trust with network controls managing the flows between the zones. Activity should be allowed within a zone, or from zone of higher trust to a zone of lower trust.

The Internet must be the "least-trusted" zone. A firewall must manage any connections from/to the Internet and the internal network.

Some internal infrastructure and applications protect sensitive information and meet minimum security standards. These systems must be trusted and should be connected to the same zone. These trusted clients and servers can communicate freely with each other without restriction. A firewall must manage any inbound connections from any less trusted zone to this trusted zone.

Other internal infrastructure and applications may not meet minimum security standards. An intermediate level of trust is appropriate for these systems. These clients and servers must be less trusted, and can freely communicate with each other. A firewall must restrict any connections from this semi-trusted zone to the trusted zone.

4.3.5 Section VIII –Information Security– Acceptable Use Policy

Description

The Internet Use policy is published in the Students section of the district's policy and procedure manual. As identified in the policy assessment section, this policy has many gaps when reviewed against the information security vision statement. A more suitable replacement would target Acceptable Use to all kinds of GIAC information asset users.

Appropriate use needs to be mandated to all users, including students, staff, faculty, and third-parties. The policy must apply to the use of any networked computer, and should not be tied to Internet usage.

Support to Risks

All users of GIAC information assets have a distinct role and set of responsibilities. When these roles and responsibilities are clearly defined, appropriate activity can be monitored for, and violations can be detected and responded to.

As compared to the original Internet Use policy, the risks for use by staff, faculty, and third parties will now be discussed and dealt with. All forms of users will now provide better support to the information being protected.

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

All functions which introduce sensitive assets to users can now set expectations for acceptable use, and introduce monitoring elements that will trigger information security incident response.

Recommendation
The exiting Internet Usage policy should be removed, and a new policy entitled "Acceptable Use" should be created. All areas detailed in the original policy's assessment gap should be included. See Section 4.2.1 for more details.

All users of the district's information and systems have responsibilities and must conform to acceptable usage. The revised policy must broaden the scope of users to third-parties and all forms of internal users. Parents, town residents, and vendors need to be included. Faculty, staff, and volunteers need to be included.

The activities for users must be restricted to district business and the user's authorization and entitlement. Any vulnerability that provides additional access must not be exploited, and any vulnerability or security breach must be reported.

All users must respect the rights of vendors and comply with contract and licensing terms and conditions. Licensing violations must be reported.

5 DEVELOP SECURITY APPROACH

Once the policies are put into place, they must be applied so that the existing risks can be reduced. Note that these steps assume budget limitations and prioritize security services on the most important information assets. The following high-level issues remain which must be addressed:

5.1 Users Not Aware of Information Security Responsibilities

Issue
Many of the existing uses of technology involve bad practices which directly challenge the direction of information security outlined in this assessment. Without proper education, these bad practices will continue, and will diminish the value of the program.

Action
The Technology Department should develop and administer a security awareness session for all faculty and staff. Each faculty member should then be instructed to reinforce the information security message in their educational application of technology.

As part of the annual acceptable use acknowledgement process, all users should read an informational brochure on information security, and

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

acknowledge their awareness and willingness to abide by the acceptable use policy.

Benefits
The training will provide a uniform understanding of what is expected. It will allow for clarification and acknowledged awareness before compliance monitoring would begin.

A number of other changes will be necessary to improve security at GIAC. This training session can also support information sharing on the changes that are coming, and help minimize any impact due to the change.

Measurement
Security incident handling will assess awareness and determine if users are familiar with their roles and responsibilities and the information security policy that mandates them.

Periodic audits can also be performed to identify gaps in security awareness.

5.2 Poor or Unknown Qualities in Existing Passwords

Issue
As outlined in this assessment, a poor password policy exists on many of the critical applications and core network services. The User Management policy mandates a stronger use of passwords. The requirements in that policy have not been applied. Compromised passwords may exist and may need to be strengthened.

Action
Where possible, force an appropriate password length, complexity, and age. Document any exceptions along with justification for non-compliance. Either reset the passwords, or force them to expire. Where transmission of passwords is necessary, communicate them discretely. Reinforce the user's responsibility to maintain secrecy of the password.

Benefits
Individual accountability can only exist when users know their responsibilities, and activities on the network can be associated to their identity. Strong password controls are necessary to achieve this accountability.

Measurement
Password change history will indicate that passwords are aging, and users are being required to create new passwords. Password settings can be reviewed against the policy to determine the rules for new passwords.

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

Period assessments of the password file can be performed by password cracking tools to identify weak passwords, and policy non-compliance.

5.3 Faculty/Staff Applications and Core Services Not Separated

Issue

Virus outbreaks and other destructive activity exist on the internal network. Vulnerabilities exist within the critical applications and network infrastructure. The lack of separation places the most sensitive of applications and data at risk. Faculty and staff applications and core network services need to be isolated from these threats.

Action

The Technology Department must establish physical separation for network services in support of faculty and staff. Dedicated infrastructure (clients and servers) must be restricted for use by faculty and staff.

Benefits

Faculty/staff applications and core network services have a business priority, and relate to sensitive information assets that must be protected. Separation will minimize threats to the security implemented, minimize the effort to assess for risks, and limit the costs of security improvements.

Measurement

Security incident handling can identify the infrastructure involved, and determine how the isolated faculty/staff infrastructure is performing.

An audit can be performed of all clients, servers, and applications. Those physical components can be associated with the network design, and the portion of that design specific to Faculty/Staff activity. Access control policy for infrastructure located within the Faculty/Staff network can be reviewed. A random sample of Faculty and Staff can be interviewed, and usage of infrastructure located outside of the Faculty/Staff network can be identified.

5.4 Minimum Security Standards do not exist for Faculty/Staff Applications and Infrastructure

Issue

Faculty/Staff applications and services are critical to the district and must be protected. Well known vulnerabilities exist and are not being managed. The goals for infrastructure and application security have not been established. AV protection, for instance, is not being mandated.

Action

The Technology Department must define and apply security configuration standards to critical application and infrastructure. As a business priority, standards will be defined for Faculty/Staff applications and infrastructure.

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

Security components, like AV protection, need to be mandated. Service levels must be defined for the remediation of high risk vulnerabilities.

Establish minimum security standards for the Faculty/Staff computers, including mandatory AV protection, up-to-date security patches, and best practice security configurations. Apply the standards to the existing infrastructure. Make sure that the standard evolves as new technologies are pursued, or as the application of technology broadens.

Benefits
A number of tangible costs are incurred when sensitive information is compromised. Minimum security standards establish the appropriate level of safeguards to the threats that lead to information compromise. Risks can only be clarified and managed when standards are defined, and implementations are measured.

Measurement
Formal and ad-hoc processes can be created to review the Faculty/Staff applications and core network infrastructure. Implementations can be audited for compliance to standards. Incident response can be triggered for standards non-compliance, and appropriate action can be taken.

Tools can be used to perform periodic assessment of vulnerabilities. Discoveries can be investigated, and non-compliance to standards can be identified.

5.5 Risk Assessments Incomplete for Faculty/Staff Infrastructure

Issue
Due to time constraints, the breath and depth of this assessment was limited. The author did not have hands-on access to the infrastructure or applications. Limited resources from GIAC were provided and only resources from the Technology Department were involved.

Gaps may exist in the high-level action planned contained within this assessment. The development and measurement to Minimum security standards may not go far enough to get at these risks. Critical applications and network services may have unknown and unmanaged high-risk vulnerabilities.

Action
Review this entire assessment. Identify sensitive information assets or critical applications which were not a target of this assessment. Review the vulnerabilities for areas that were covered in this assessment. Identify any high-risk vulnerability that was not presented. Refine the assessment based on those discoveries.

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

Use vulnerability assessment tools to target specific infrastructure or application vulnerabilities. Use password cracking tools to target change in weak passwords.

Perform a physical inventory of the dependent infrastructure. Establish an inventory system which will help manage change and ensure that the standards and other actions apply to all candidate configurations.

Benefits
Information security solutions blend people resources, process development, and evolving technology. Investments in security architecture must be justified through proposed resolution to high-risk vulnerabilities.

By revising this assessment, the breath of change can be appropriately adjusted. By using tools and a manual inventory process, the depth of change to specific configurations can be prioritized.

Measurement
When the risk assessment process is complete and faithful, all information asset custodians and decision-makers have clarity and consensus on the vulnerabilities that exist, and the priority risk actions that need to be taken.

This assessment identifies a set of sensitive information assets. Conduct interviews of the stake-holders of those assets, and identify issues that have led to loss of confidentiality, integrity, or availability of these assets. Identity the root cause for these incidents, and compare the vulnerabilities discovered with those developed through the risk assessment process.

5.6 Public Systems Not Separated and Isolated

Issue
Internal assets have increased threat from the hosting of public systems and services from within the internal network. The protection of internal information assets is not appropriate for all forms of Internet-based attacks.

Action
Access to internal applications from the Internet should be eliminated. Public applications and core network services should be hosted on separate servers, and should reside on an isolated network managed by the firewall (DMZ).

Benefits
Faculty/Staff applications and network services have a business priority, and directly manage the most sensitive information assets. Protection can be ensured when the risk model to those assets is simplified, and specific risk actions are taken within that model.

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

The risk model for Internet-based services is quite complex. By limiting the assets contained within that model to those that have business priority, specific security investments can be made so that those exposed assets are not compromised. By isolating those information asset systems, the risks of doing business on the Internet can be reduced to the values of those assets.

Measurement
Security incident handling can identify the infrastructure involved, and determine how the DMZ infrastructure is performing.

An audit can be performed of all clients, servers, and applications. Those physical components can be associated with the network design, and the portion of that design specific to DMZ activity. Access control policy for infrastructure located within the DMZ network can be reviewed.

5.7 Student Infrastructure Not Separated and Isolated

Issue
Internal assets have increased threat from student access and activities. Section 5.3 addresses the separation of Faculty/Staff applications and network services from the rest of the internal network. The primary consumer that remains is students. Student applications and infrastructure will therefore be isolated.

Action
The Technology Department must establish physical separation for network services in support of students. Client computers must be reserved for students, and hosted on a separate network. Student applications and network services must either be hosted within this isolated network, or hosted within the Public network. Student computers must not have access to Faculty/Staff applications or network services.

Benefits
Students present a more significant insider threat than faculty or staff. Students require limited access to sensitive information. By limiting the assets and containing the threat, the risk model is targeted, and clear expectations can be set.

Budget limitations will more than likely limit the protections that can be applied within the student infrastructure and applications. Incidents will be expected, but will be contained.

Measurement
Security incident handling can identify the infrastructure involved, and determine how the isolated faculty/staff infrastructure is performing. As

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

stated above, limited protections may be available, so certain kinds of incidents, like virus outbreaks, should be expected.

An audit can be performed of all clients, servers, and applications. Those physical components can be associated with the network design, and the portion of that design specific to Student activity. Access control policy for infrastructure located within the Student network can be reviewed. A random sample of Students can be interviewed, and usage of infrastructure located outside of the Student network can be identified.

© SANS Institute 2003, Author retains full rights.

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

APPENDIX

INTERNET USE POLICY

The GIAC Regional School District realizes the value of access to the internet. It also recognizes the potential for abuse. In an effort to prevent such abuse, the following document must be completed by the indicated parties on an annual basis for all students in grades 5-12. Students in grades 5-12 who enter GIAC during the school year shall be required to complete the form. Students at lower grades will be required to complete the form on an "as needed" basis.

Please read the following carefully before signing this document. This is a legally binding document.

Internet access is now available to students and teachers in the GIAC Regional School District. We are very pleased to bring this access to the District and believe the Internet offers vast, diverse and unique resources to both students and teachers. Our goal in providing this service to teachers and students is to promote educational excellence in the District's schools by facilitating resource sharing, innovation and communication.

The Internet is an electronic highway connecting thousands of computers all over the world and millions of individual subscribers. Students and teachers have access to:

1. electronic mail communication with people all over the world;
2. information and news from world-wide sources as well as the opportunity to correspond with the scientists at NASA and other educational/research institutions;
3. public domain software and graphics of all types for school use;
4. discussion groups on a plethora of topics ranging from Chinese culture to the environment to music to politics;
5. access to many university library catalogs, the Library of Congress, and ERIC, a large collection of relevant information to educators and students;
6. graphical access to the World Wide Web, the newest and most exciting access tool on the Internet.

With access to computers and people all over the world also comes the availability of material that may not be considered to be of educational value in the context of the school setting. The GIAC Regional School District will insure that precautions are taken to restrict access to controversial materials. However, on a global network it is impossible to control all materials and an industrious user may discover controversial information. We (the GIAC Regional School District) firmly believe that the valuable information and interaction available on this world-wide network far outweighs the possibility that users may procure material that is not consistent with the education goals of the District.

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

Internet access is coordinated through a complex association of government agencies, and regional and state networks. In addition, the smooth operation of the network relies upon the proper conduct of the end users who must adhere to strict guidelines. These guidelines are provided here so that you are aware of the responsibilities you are about to acquire. In general this requires efficient, ethical and legal utilization of the network resources. If a GIAC Regional School District user violates any of these provisions, his or her account will be terminated and future access could possibly be denied.
The signatures at the end of this document are legally binding and indicate the parties who signed have read the terms and conditions carefully and understand their significance.

INTERNET - TERMS AND CONDITIONS OF USE

1. Acceptable Use - The purpose of the backbone networks making up the Internet is to support research and education in and among academic institutions by providing access to unique resources and the opportunity for collaborative work. The use of your account must be in support of education and research and consistent with the educational objectives of the GIAC Regional School District. Use of other organization's network or computing resources must comply with the rules appropriate for that network. Transmission of any material in violation of any national or state regulation is prohibited. This includes, but not limited to: copyrighted material, threatening or obscene material, or material protected by trade secret.
2. Privileges - The use of the Internet is a privilege, not a right, and inappropriate use will result in a cancellation of those privileges. (Each student or teacher who receives an account will be part of a discussion with a District staff member pertaining to the proper use of the network. The system administrators will deem what is inappropriate use and their decision is final. Also, the system administrators may close an account at any time as required. The administration, faculty, and staff of the GIAC Regional School District may request the system administrator to deny, revoke, or suspend specific user accounts.
3. Network Etiquette - You are expected to abide by the generally accepted rules of network etiquette. These include (but are not limited to) the following:
    a. Be polite. Do not get abusive in your messages to others.
    b. Use appropriate language. Do not swear, use vulgarities or any other inappropriate language. Illegal activities are strictly forbidden.
    c. Do not reveal your personal address or phone number, or the address or phone number of students or colleagues.
    d. Note that electronic mail (email) is not guaranteed to be private: People who operate the system do have access to all mail. Messages relating to or in support of illegal activities may be reported to the authorities.

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

   e. Do not use the network in such a way that you would disrupt the use of the network by other users.
   f. All communications and information accessible via the network should be assumed to be private property.
4. GIAC Regional School District makes no warranties of any kind, whether expressed or implied, for the service it is providing. GIAC Regional School District will not be responsible for any damages you suffer. This includes loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions caused by its own negligence or your errors or omissions. Use of any information obtained via the Internet is at your own risk. GIAC Regional School District specifically denies any responsibility for the accuracy or quality of information obtained through its services.
5. Security - Security on any computer system is a high priority, especially when the system involves many users. If you feel you can identify a security problem on the Internet, you must notify a system administrator or the GIAC Regional School District Technology Coordinator. Do not demonstrate the problem to other users. Do not use another individual's account. Attempts to logon to the Internet as a system administrator will result in cancellation of user privileges. Any user identified as a security risk may be denied access to the Internet.
6. Vandalism - Vandalism will result in cancellation of privileges. Vandalism is defined as any malicious attempt to harm or destroy data of another user, Internet, or any of the above listed agencies or other networks that are connected to any of the Internet backbones. This includes, but not limited to, the uploading or creation of computer viruses.

SCHOOL DISTRICT INTERNET USE AGREEMENT
STUDENT
I understand and will abide by the above Internet Use Agreement. I further understand that any violation of the regulations above is unethical and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked, school disciplinary action may be taken, and/or appropriate legal action.
User's Full Name: _____
User's Signature: _____
Date: _____

PARENT OR GUARDIAN
As the parent or guardian of this student, I have read the Internet Use Agreement. I understand that this access is designed for educational purposes. GIAC Regional School District has taken precautions to eliminate controversial material. However, I also recognize it is impossible for the District to restrict access to all controversial materials and I will not hold them responsible for materials acquired on the network. Further, I accept full responsibility for supervision if and when my child's use is not in a school setting. I hereby give

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

permission to issue an account and certify that the information contained on this form is correct.
Parent or Guardian's Name (please print) _____
Parent or Guardian's Signature _____
Date: _____

SPONSORING TEACHER
(Must be signed if the applicant is a student.)
I have read the Internet Use Agreement and agree to promote THIS agreement with the student. Because the student may use the network for individual work or in the context of another class, I cannot be held responsible for the student use of the network. As the sponsoring teacher, I do agree to instruct the student on acceptable use of the network and proper network etiquette.
Teacher's Name (please print) _____
Teacher's Signature _____
Date: _____

© SANS Institute 2003, Author retains full rights.

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

Information Security: The Vision

GOAL
In order to provide a balanced approach to the use of technology and the Internet, the GIAC Regional School district must focus on the security surrounding information access. Information Security will define the diligence to understand the value of information while identifying and properly managing the risks to digital access to that information.

Protection of information assets is a key component in the management of risks. The public places their trust in the district to maintain the confidentiality, integrity and availability of its information assets. The GIAC Information Security Policy is the foundation by which requirements for protecting information assets are established.

CRITERIA
Information, whether valued as its own proprietary intellectual property or held in trust for the purpose of providing educational services, is an important asset. Unauthorized disclosure, modification, misuse, destruction, or lack of availability creates real costs to the district. The extent of information security must be based on its value and these potential costs. The strength of information protection is determined from its guarantees toward maintaining the information's confidentiality, integrity, and availability.

Responsibility for the protection of information assets rests with all users of the district's information assets, through the adoption of this Policy into Information Security procedures and standards.

© SANS Institute 2003 Author retains full rights.

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

Information Security: Risk Assessment Policy

Objective
This Policy defines requirements for conducting risk assessments in order to identify weaknesses and target additional protection against legitimate threats to the GIAC Regional School District Information Assets. The risk assessment must calculate the risk corresponding to all information assets and the effects produced if threats are realized.

Scope
This Policy applies to all information assets operated by the district or those contracted with third parties used by the district regardless of geographic location. The term "information asset" defines electronic and non-electronic assets and includes, but it is not limited to all documentation, business processes, products, hardware and software.

Description
A risk assessment examines security of GIAC Information Assets and estimates the impact on a business group due to loss or degradation or misuse of these information assets.

LIMITING THE ANALYSIS
The scope of the risk assessment process must be identified according to the environments that are part of the analysis. Relevant factors include the importance of the environment to district and business operations, and the environment's perceived threats and vulnerabilities. This risk assessment policy suggests ways of measuring levels of information vulnerability to various threats and the means of determining the effectiveness of proposed controls in reducing these risks.

IDENTIFYING THE ASSETS
Once the scope of the risk assessment process has been determined, the assets belonging to each environment must be identified to ensure that the subsequent assessment steps address the environment as a whole. The total asset value of the environment includes the information present within the environment and all the entities therein that contain it, utilize it and facilitate its transfer into and out of the environment itself. Specifically, this means all the environment's information assets (hardware, software, telecommunications, data etc.) as well as the facility which houses it must be identified and submitted for security analysis. The managers of the environment under review (e.g., the building manager for physical security, the network or systems manager for logical security of the information) are responsible for identifying all the assets to the risk assessment team so that they can perform a comprehensive risk evaluation.

ASSET PRIORITIZATION AND VALUE STATEMENT
Once the relevant assets have been identified, the value of these assets to school operation must be defined to determine the impact of their potential loss due to threats and vulnerabilities. The loss impact is a key factor in determining the proper risk reduction strategy to adopt in the last phase of the assessment. The rule must be that the

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

cost of applying risk reduction procedures must not outweigh the value of the assets to the Information Owner and GIAC. This value can be quantitative or qualitative.

IDENTIFY THREATS AND VULNERABILITIES

Once the environment assets and their values have been identified, specific corresponding threats which could cause loss of asset availability, integrity, and confidentiality (in the case of information assets) must be determined along with the likelihood of their occurrence. Likewise, the vulnerability of assets to these threats must be understood in light of existing environmental controls and available countermeasures. To achieve this, information inherent to the information asset environment must be collected and examined to determine the current security state of the area. During the examination, the threat presence, probability and the information assets susceptibility to the threat must be taken into consideration. Threats considered must be natural and man-made.

CALCULATING THE RISK

Threat and asset vulnerability identification must be coupled with the probability of threat occurrence in an equation to arrive at the appropriate risk determination for the asset evaluated. An established risk evaluation formula must be utilized to determine the level of risk. Threats are realized when vulnerabilities are attacked. The effort of an attack and the probability of an attack define the probability of the threat occurrence. An impact is realized during a threat occurrence. The data and asset value of an environment defines the severity of impact. Risk is calculated by combining the threat probability with the impact value. Risks for the exposure areas will be described as low, medium, or high risk values for ease of interpretation and targeting for risk reduction strategy.

THRESHOLDS FOR RISK REDUCTION ACTION

Minimum standards must be established for each environment, defining the tolerance for risk. Risk reduction plans must be created and activated when these minimum thresholds are exceeded.

ELEMEMTNS OF A RISK REDUCTION PLAN

A list of recommendations to reduce risk values which exceed district security baseline standards and allowances must be developed. The recommendations will address the medium to high risk exposures and fall under one of these four categories:

- Preventative safeguards must reduce the cost of risk to zero by preventing the risk event from occurring.
- Mitigating safeguards must reduce the cost and impact of the event occurrence.
- Detective safeguards must detect risk events.
- Recovery safeguards must help recover from the event in a way which reduces overall cost.

Compliance Requirements

Compliance with GIAC Risk Assessment Policy is mandatory.

Waiver Criteria

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

Requested waivers must be submitted to the Office of the Superintendent, including justification and benefits attributed to the waiver, and must be approved by the appropriate information owners. The waiver should only be used in exceptional situations when communicating non-compliance with the policy for a specific period of time (refer to the policy Waiver Request Form). The policy Waiver Request Form must be used when communicating exceptions to this policy.

Maintenance
All change requests of this policy must be submitted in writing to the Office of the Superintendent. The "policy sponsor" is responsible for reviewing and approving all change requests.

Responsibility for Ensuring Compliance
Periodic reviews of activity associated with this Policy will be held by Internal Audit. GIAC managers must ensure continuous compliance monitoring within their organizations.

© SANS Institute 2003, Author retains full rights

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

REFERENCES

"MessageLabs Intelligence – August 2003", MessageLabs, August 2003, URL: http://www.messagelabs.com/news/pressreleases/detail/default.asp?contentItemId=557&region=

Richardson, Robert, "2003 CSI/FBI Computer Crime and Security Survey", Computer Security Institute, 2003, URL: http://www.gocsi.com/awareness/fbi.jhtml

McClure, Stuart; Scambray, Joel; Kurtz, George; Hacking Exposed Network Security Secrets & Solutions, Third Edition, Berkley, California, Osborne/McGraw-Hill, 2001.

© SANS Institute 2003, Author retains full rights.

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