

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.

GIAC Institute for Basic Cellular Research

GIAC INFORMATION SECURITY OFFICER
GISO – Basic Practical Assignment
V1.2 (February 9, 2002)

Kay A. Cornwell
SANS Wash. DC
May 2002
Submitted Oct 16, 2002

© SANS Institute 2000 - 2002 Author retains full rights.

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

Abstract

The GIAC Institute for Basic Cellular Research (IBCR) is a component of the GIAC Federal Institutes of Health Services (FIHS) which is a branch of the Federal Government's Health Services Agency. The GIAC Institute for Basic Cellular Research (IBCR) supports basic biomedical research by funding grants that focus on basic cellular functions. The IBCR's operations depend heavily on staff processing information at a high level of sensitivity. The systems which provide access to grants information are considered to have a level 3 criticality meaning that availability is extremely important to the institute. Three risks to the protection of institute data and availability are identified; attack from the Internet or from within the IBCR's parent agency, server vulnerabilities and attack from within the IBCR, either intentional or unintentional. Each risk is discussed and mitigation steps are defined. A sample server security policy is evaluated and then revised to fit the needs of the institute in response to the sever vulnerability threat. In conclusion, a server installation procedure is developed to implement the server security policy.

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

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

TABLE OF CONTENTS

Description of GIAC Institute for Basic Cellular Research (IBCR) 5

IT Infrastructure 5

Relationship with FIHS 5

FIHS Infrastructure 6

IBCR Infrastructure 8

Business Operations 12

Identify Critical Risks 16

Levels of Data Sensitivity 16

Levels of Criticality 17

Risk – Attack from the Internet AND/OR from within the FIHS Network 18

The Threat 18

Significance 18

Impact Potential 19

Likelihood of Exploits 20

Mitigation Strategy 21

Risk – Server Vulnerabilities 24

The Threat 24

Significance 24

Impact Potential 25

Likelihood of Exploits 26

Mitigation Strategy 27

Risk – Protection against internal threats – unintentional or intentional 31

The Threat 31

Significance 31

Impact Potential 32

Likelihood of Exploits 33

Mitigation Strategy 34

Evaluate and Develop Security Policy 38

Server Security Policy 38

Evaluate Security Policy 39

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

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

Revise Security Policy....42
Develop Security Procedures....46
Server Security Installation Procedure....46
References **54**

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

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

Description of GIAC Institute for Basic Cellular Research (IBCR)

The GIAC Institute for Basic Cellular Research (IBCR) is a component of the GIAC Federal Institutes of Health Services (FIHS) which is a branch of the Federal Government's Health Services Agency. The GIAC Institute for Basic Cellular Research (IBCR) supports basic biomedical research. The IBCR does not perform research itself, rather it funds work that focuses on learning about the basic cellular functions that lead to advanced understanding of fundamental life processes and increases knowledge of the mechanisms involved in disease. The IBCR also supports training programs that provide opportunities and encourages students at all levels to pursue careers in biomedical research. Some of these training programs specifically target minority students to encourage them to pursue biomedical degrees. The IBCR's budget of $1.5 billion funds grants to university, medical school, hospital and research scientists. The IBCR funds approximately 4,000 research grants mainly supporting individual, investigator-initiated research grants.

IT Infrastructure

Relationship with FIHS

When discussing the IT infrastructure of the IBCR one must first look at where the institute fits within the entire GIAC Federal Institutes of Health Services. While the IBCR has its own congressional funding and devotes 4% of its budget to administrative functions, its IT infrastructure is tied closely with the GIAC Federal Institutes of Health Services (FIHS) infrastructure. FIHS' Information Technology Center (ITC) provides the network cabling infrastructure for the institute, they also provide the border routers, switches, firewalls and intrusion detection systems along with the skill set needed to monitor and maintain them. The IBCR has found it beneficial to buy into many of the solutions the ITC has provided for the FIHS campus WAN which includes 300 LANs supporting more than 20,000 PCs, Macs, and UNIX workstations. The FIHS has traditionally operated as close to an academic and research atmosphere as possible. Access and security, while following government guidelines, have been as open as if FIHS were a major university campus.

New security mandates from the FIHS' parent agency and the increase in attacks on the FIHS network has led the ITC, working in cooperation with all FIHS components, to provide overall security services rather than assisting each component separately. Policy and procedures put in place over the last two years have followed federal law or are best practices recommended by NIST, the National Institute of Standards and Technology and SANS. This situation has lead to an economy of scale and savings for the IBCR. The IBCR pays a minimal service fee into a general fund to benefit from the perimeter firewall and IDS systems. The IBCR is free to install its own equipment to achieve an even greater defense in depth. The institute has joined the ITC's program to place firewall and IDS products at all the FIHS component's perimeters. The ITC has provided the specifications for and will integrate the equipment into a new gigabit

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

router and switch upgrade occurring this fall. They will monitor the IDS and provide assistance with firewall rule sets. It is necessary to discuss the IBCR's relationship with FIHS and the FIHS infrastructure when considering a risk assessment as all packets that reach the IBCR network first travel through the FIHS network. The IBCR's risks and mitigation tactics depend largely on how good a job FIHS is doing on assessing and mitigating risk for the FIHS network as a whole. Due to FIHS' implementation of agency wide services the IBCR does not need to maintain or protect services such as DNS, WINS, and soon, Email servers.

The FIHS network structure utilizes defense in depth. Due to security concerns a detailed network structure diagram is not available to personnel at the individual component layer. The following is an overview of the FIHS infrastructure. The ITC provides and maintains an agency wide DNS service. A central Microsoft Exchange e-mail facility is utilized by many of the FIHS components. The IBCR is in the midst of migrating from its own Exchange server to this central service. This will eliminate the need for the institute to include the protection of an email server in its security plan. The ITC also maintains WINS services as well as a public, integrated web hosting service for the FIHS component's official web pages. The IBCR uses this service to host its official public web site which places the job of protecting the institute's official internet presence in the hands of the ITC. Since the IBCR does not have day to day technical responsibility for maintaining and protecting these services they will not be included in this risk assessment.

FIHS Infrastructure

The first layer of the FIHS infrastructure is the interface between the Internet and the FIHS and entities that utilize the FIHS network as an ISP. The FIHS' Internet connection to its provider, Genuity, is a redundant OC3 connection coming into a Cisco 7600 Gigabit router (see Figure 1). There are two other access points into the FIHS network. A Cisco 7500 Gigabit router connects to the Internet II and a Cisco 7500 Gigabit router isolates non-FIHS entities that had at one time shared the FIHS network space. These entities used the FIHS as their provider but for security reasons it was not appropriate to allow them behind the FIHS' firewall. Examples of such institutions are the County Public School system, Contractor facilities and other government agencies within the local area. All border routers perform IP filtering.

The FIHS Gigabit Ethernet backbone from the border routers down to the individual FIHS component's routers is duplicated for automatic failover. All individual components discussed have a backup product in place that steps in, in case of failure of the primary device. A Lucent gigabit firewall is the first layer of defense. The FIHS' initial firewall policy has been to allow all as default. As consensus between FIHS components is reached policy has been applied to close ports that are known as common vulnerabilities. Exceptions are made as needed. For example, to help alleviate HTTP attacks and defacements, all

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

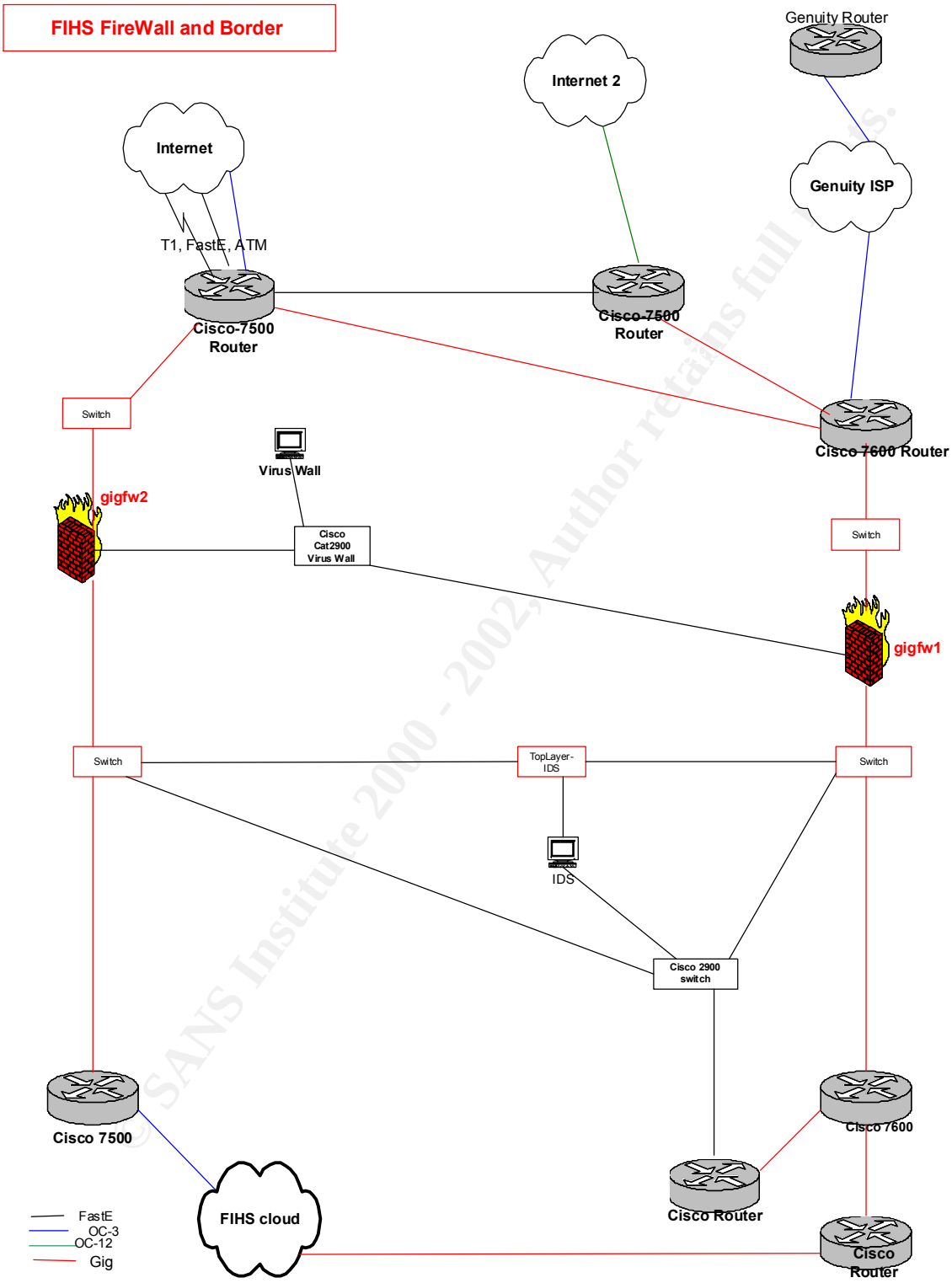


Figure 1. FIHS Network Diagram. Adapted from internal FIHS documentation.

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

components listed the IP address of web servers that needed to be open to the public. The firewall only passes port 80 traffic to these specified machines. Only the institute Information System Security Officer (ISSO) is allowed to modify their institute's list. This has lead to a marked decline in web compromises by simply limiting the number of web servers available from outside the firewall. Recent policy has been enacted to do the same for FTP servers and NetBIOS services. Future policy will address Internet Relay Chat and SQL access. While writing this paper the FIHS has experienced heavy activity at the firewall. The policy of allow all traffic has been changed to deny all expect that which is expressly allowed.

There is an IDS sensor behind the firewall. The sensor identifies any attacks that may have circumvented the firewall. It also identifies attacks that may be coming from within or some attacks between FIHS components. At this point an automatic block feature has been placed. In the event of an anomaly the IDS will automatically block traffic between the attacker and victim to prevent damage to FIHS resources or to prevent liability to FIHS in the event internal resources are compromised and used to stage attacks on other organizations.

IBCR Infrastructure

The next layer comprises the individual FIHS's component LANs. The IBCR maintains its LAN in a single location spread over 2 floors (see Figure 2). The IBCR LAN will be upgraded in the upcoming weeks. The IBCR LAN consists of a Cisco router and the following new equipment, two Lucent VPN Firewall Brick 1000s to create a DMZ for public services, two gigabit Cisco switches, and a blade IDS. The firewall, switches and routers are located in locked LAN closets. The Chief of IT Operations for the IBCR has one of two keys to these LAN closets. The remaining key is in the possession of the ITC's network infrastructure branch. The IBCR maintains a cipher locked and separate air conditioned LAN room which houses 40 Windows NT/2000 servers. Servers are a range of Compaq Proliant tower and rack mounted CPUs. Dell Optiplex GX 150, Precision 330 and 340 desktops run Windows 2000 server for single services such as help desk ticketing software, enterprise antivirus, and print servers. Two UPS provide conditioned electrical and backup power.

The IBCR maintains approximately 40 Windows NT/2000 and 2000 Advanced Servers. Immediate plans are to move to active directory within the next few months, upgrading the primary and backup domain controllers to Windows 2000 Advanced Server. All servers are running McAfee anti-virus in the background and are monitored from McAfee's E-Policy management console. Those servers that assist with security and those servers that are critical are listed below.

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

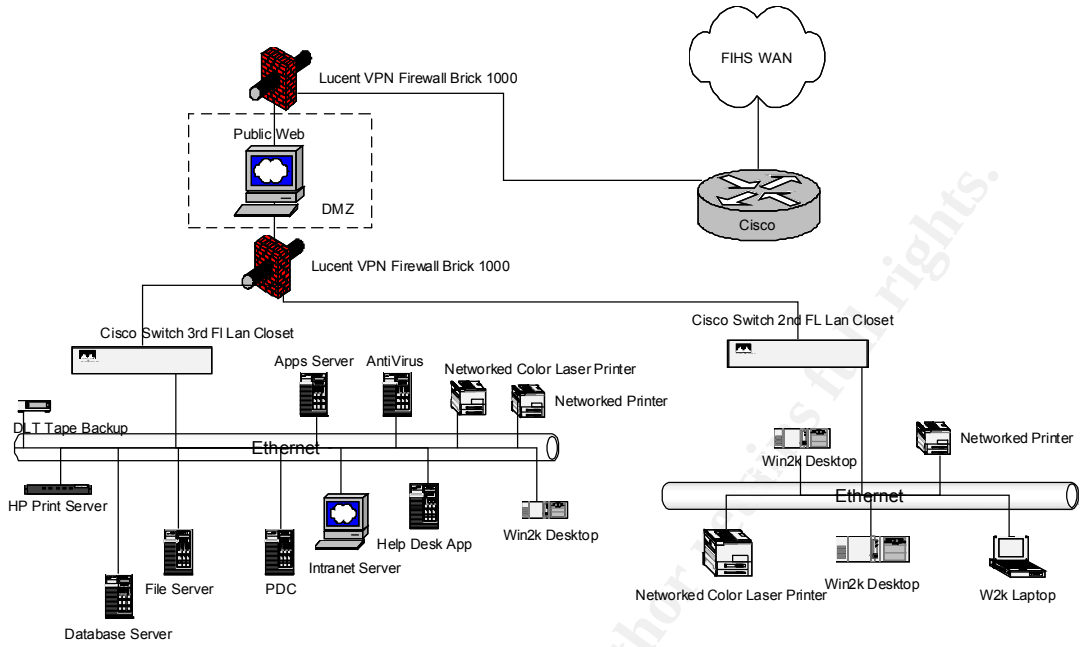


Figure 2. The IBCR Network

Critical Severs

Compaq Proliant Rack Mount Servers
All Proliant Servers have RAIDs with at least 45+ Gig
Proliant 3000
  App Server – All desktop applications housed here, NT
  Primary Domain Controller, NT
Proliant 4500
  Backup Domain Controller, NT
Proliant 5500
  Backup Server for non critical servers, W2k
  Microsoft SMS Server, W2k
  File Server - Users Home & Shared Directories, W2k
  Intranet Server, IIS 5.0, Cold Fusion, W2k
  Intranet Development, IIS 5.0, Cold Fusion, W2k
  Public Web Apps & FTP, IIS 5.0, Cold Fusion, W2K
  Actuate Server – Web interface for mainframe reports, IIS 5.0, W2K
Proliant 6500
  SQL Server, SQL 7.0, NT
Proliant DL380
  File Server - Users Home & Shared Directories, W2k
  Oracle Database Server – Production Server, W2k
  Oracle Database Server – Test server, W2k
  Oracle Database Server – Development Server, W2k

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

Dell Optiplex GX150, 1 GHz
Security Server – Security desktop, W2k – running:
St. Bernard's Update Expert – Patch Management
Test machine for Harris' STAT Analyzer – vulnerability scanner
Citadel Software's Hercules – vulnerability mitigation tool
McAfee EPolicy Orchestrator – central management of desktop anti-virus, W2k

Dell Optiplex Precision 340
Heat Application Server – Help desk ticket generator, W2k
Heat Asset Tracker – Help Desk Asset Management, W2k

Dell Optiplex Precision 330
Internet Development – IIS 5.0 Development for Institute Web pages, W2k

Compaq Deskpro
SNA Gateway – access to mainframe apps for travel, inventory, purchasing – will be replaced by Web Based Enterprise apps, W2k

Supporting Hardware
HP Print Server Appliance 4200 – to replace two desktops currently serving as print servers
Compaq SANS, Compaq Storageworks MSL 5026 Library – All critical servers attached directly to SANS for backup
Two APC Symmetra 16kVA, Input 208/240V UPS, Telnet control interface

The Cisco gigabit switch upgrade and implementation of two Lucent firewalls will allow the IBCR to deploy a DMZ for publicly accessible services. Initially, it will house a Microsoft IIS 5.0 web server running Cold Fusion applications and a non-anonymous FTP server. New requests for services currently being evaluated may indicate the need for an anonymous FTP service. These services currently sit behind the institute's Lucent brick firewall. This firewall has not had any rule sets implemented; it is logging traffic for review. The new IBCR firewalls will serve as components in a defense in depth strategy extending from the FIHS perimeter and will also serve to protect the institute from attack from within the FIHS network. The institute's perimeter has been a weak area and many institutes are starting to address the need for firewalls between FIHS components. While the ITC will maintain the new firewalls, there is a web-based interface available to the IBCR ISSO to audit logs and to change rule sets. If the ISSO does not feel comfortable with changing rule sets, the ITC will assist.

The ITC will maintain and monitor the IDS installed with the new switches. Anomalies will be handled by the same procedures as those used for the perimeter IDS. Anomalies, along with their log entries and a description of the suspected attack will be emailed to the ISSO. The ISSO will determine if a breach has been successful. The ISSO may call upon the ITC incident response team for assistance if needed or may investigate herself. The ISSO must

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

respond within a reasonable amount of time to indicate the problem has been resolved. If the attack was successful details on how it occurred, what was done to clean up and what procedures where put in place to prevent a repeat are sent to the IRT.

Another important part of the IBCR infrastructure is data backup facilities. Veritas Backup Exec Version 8.6 is used to back-up the 40 Windows NT/2000 servers, including Oracle and SQL database servers. Fourteen critical servers are protected by Compaq's Storage Area Network product which is made up of two Compaq Fiber Channel Arbitrated Loop switches, a Compaq Modular Data Router, and a Compaq Super SLT Tape Library. This solution provides a separate fiber channel to provide dedicated bandwidth for backup, thus speeding the backup process. The Modular Data Router bridges between the SCSI drive of the server and the Fiber Channel device, allowing these critical servers to back-up directly to the tape device. The remaining servers use a traditional dedicated backup server method to the tape Library. A full backup of all devices occurs weekly, along with a daily incremental backup. As an alternative safeguard and to provide for offsite backup, critical data is sent nightly to the FIHS mainframe using the ADSTAR Distributed Storage Management (ADSM) service.

The remainder of the IBCR network consists of approximately 170 Dell Optiplex GX150, 1 GHz, Win2K desktop machines, used by staff, and approximately 30 networked B&W and Color Laser printers. Desktops are standardized and staff is not permitted to download or install software, although there is no facility to prevent this. The standard desktop contains the Microsoft Office XP suite, a browser, FTP client, and custom applications written by the IBCR database group to access grant information and financial systems. The desktop also provides access to FIHS tools providing access to agency wide grant processing software. All desktops have a centrally managed Antivirus program from McAfee that scans in the background during all web downloads, when opening email and attachments, inserting a floppy disk and on boot up. All machines are scanned weekly, upgrades and dat updates are managed from the central management console.

Division directors have permanent laptops for travel: Sony Vaio 600 MHz, Pentium 3, 128 MB RAM with W2k, and IBM ThinkPad T23, 1 GHz Pentium with 256 MB RAM and W2k. A loaner laptop pool is available for staff use when they travel; need to temporarily work at home, or for training. The ITC maintains a remote dial-up service for all FIHS staff for travel and telework. The IBCR IT staff configures all laptops to use this service, requiring all those needing remote access to apply for a remote account. The business need for remote access is reviewed yearly. This service provides the teleworker with an FIHS IP address and places them behind the FIHS firewall granting access to the Institute's services. This service eliminates the need for the IBCR to need modems on site with two exceptions. A server running Microsoft RAS has 5 modems for exclusive use of the IBCR's IT staff. Remote access policy implemented within the last year

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

necessitates that this service be retired. Also, as part of the Federal Government's accessibility programs hearing impaired staff utilize TTY services via NexTalk services. This service runs on a dedicated server which connects to a modem and allows TTY connections dialed from inside or outside the institute.

The FIHS has been piloting a VPN solution to secure high speed access to the FIHS network (see Figure 3). This solution consists of a Cisco VPN client for Windows 9X, 2000, XP, Apple OS X, Linux and Solaris and a Cisco VPN 3060 concentrator. When accessing the FIHS VPN, staff first connects to a remote access DMZ with a firewall, intrusion detection and email virus detection and removal. The Cisco client allows for a personal firewall to be pushed down to the client with policy control being in the hands of the ITC. As with the remote dial-up service, management must approve staff's need for an account. Both these services, the current remote dial in program and the soon to be implemented VPN program will become the only authorized way to remotely access the FIHS network.

The remaining products to discuss in the IBCR infrastructure include wireless devices. Division directors, upper management and critical IT staff carry Blackberry wireless devices to access Exchange email. There is a pool of loaner Blackberry devices available for staff that do not require a permanently assigned device. All Blackberry communications are encrypted. The ITC manages the Blackberry services, creating accounts for loaners and shutting them off when staff returns them. The IBCR help desk is responsible for syncing loaners on the desktop and training staff in Blackberry use. The institute will be purchasing wireless access points and in conjunction with the ITC installing wireless networking within the IBCR office space. Due to the hot debate over the security of wireless, the institute has decided to purchase products based on the ITC's recommendation. They will install the access points and the IBCR staff will closely follow all wireless policy and guidelines proposed by the ITC.

Business Operations

The IBCR's main mission is the support of research scientists who are working on basic cellular research. This is accomplished through the review of grant proposals submitted by single investigators or a group of investigators at universities and private research institutions; proposals to fund scientific meetings that support research or to provide training programs to assist students pursuing careers in biomedical research. The IBCR currently supports 19 different mechanisms for funding grants. The FIHS has a well established system for receiving and classifying grant proposals (see Figure 4). The Center for Scientific Review processes all incoming grants (over 40,000 a year), classifies them and assigns them to the appropriate component for review. An independent study section, staffed by up to 18 scientific experts identified by an FIHS Scientific Review Administrator, reviews each grant application. Members

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

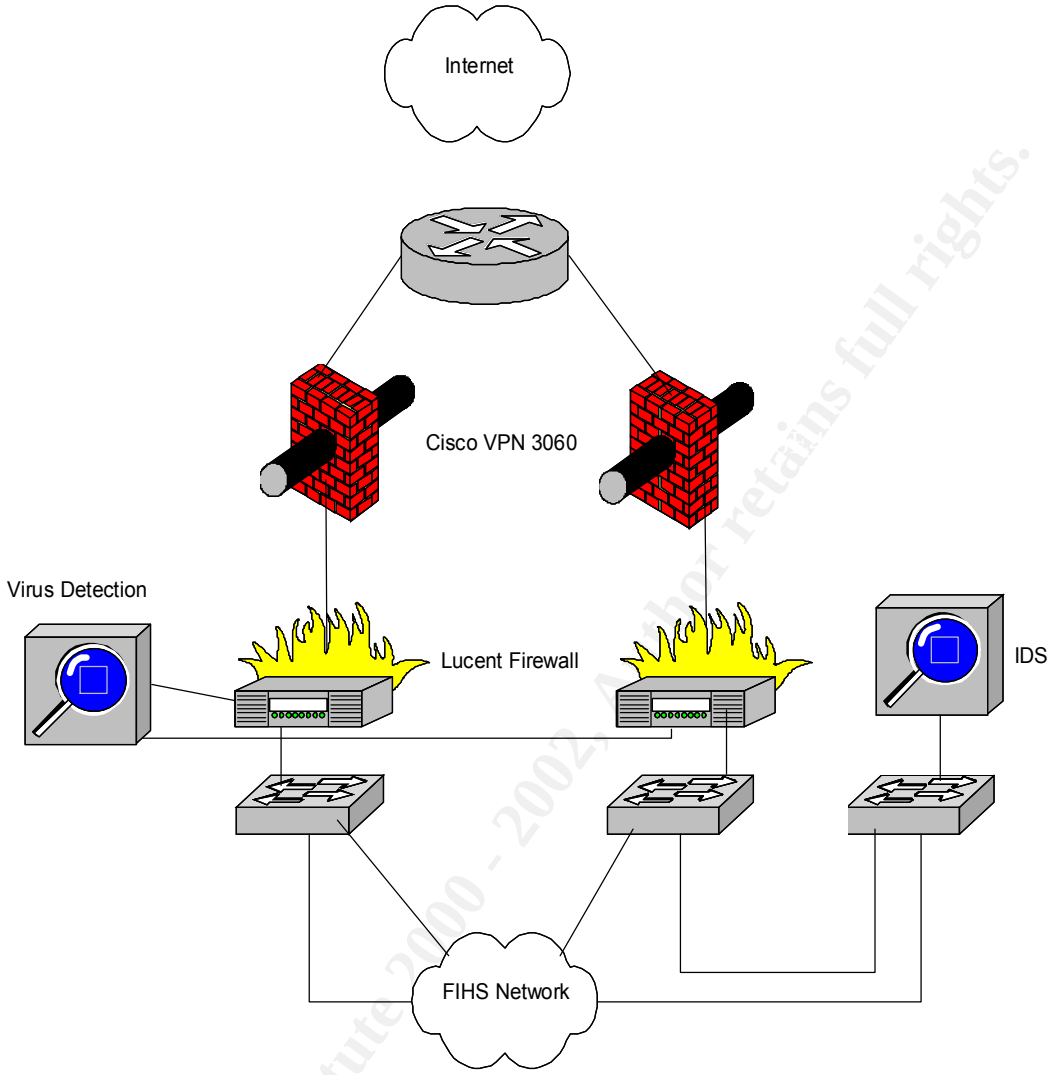


Figure 3. FIHS VPN Solution. Adapted from internal FIHS documentation.

prepare a written critique which is then discussed by the entire study section. The results of the review are collated into a Summary Statement and the application is given a score. The Summary Statements are discussed at each component's Advisory Committee Meeting. The Advisory Committee consists of members of the scientific community with knowledge in a component's specific scientific areas. This grants process runs on a three times a year funding cycle. Each component runs its own grant cycle, called Council, and maintains its own Advisory Committee. Council is a peer review process: during the entire application process all grants are judged or reviewed by peers from within and

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

without the FIHS community. Information is provided to reviewers and the Advisory Committee by FIHS developed web interfaces to grants databases, email, paper-based mailings and mailed CDs. Limitations on electronic means of sharing information is based on the wide range of platforms in use by non-FIHS personnel and the need to accommodate those of differing levels of comfort with computers.

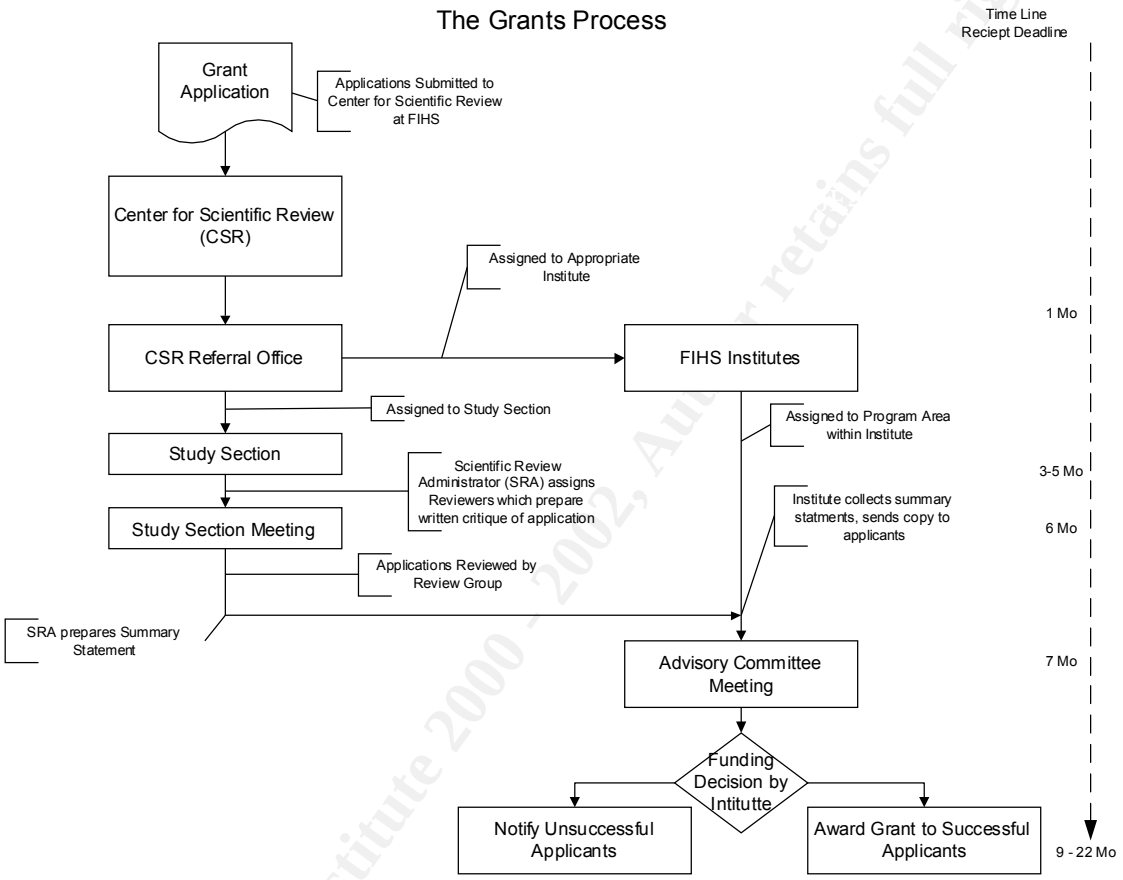


Figure 4. The Grants Process. Taken from internal FIHS documentation.

The bulk of approximately 170 IBCR staff process grants by serving in one of three areas: as a Health Science Administrator or support person, Grants Management Staff or Office of Scientific Review staff. The remaining institute staff works in administrative support positions such as budget, personnel, IT, public liaison and management. Administrative staff demands availability to FIHS developed resources such as personnel systems, financial systems, and administrative office systems such as procurement, travel, and inventory. Email is a necessity with high availability being extremely important. The Ph.D. scientists who manage the institute's program areas and assist the Advisory Committee with funding decisions are called Health Science Administrators (HSA). They spend the bulk of their time studying grant applications, considering which are worth funding along with monitoring grantees' research progress and assisting prospective grantees through the grants application process. Their

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

mission is communication with the applicants to assist investigators through the complex grant writing process as well as to provide support and report on the research during the life of the grant. The FIHS provides a web-based interface to the agency wide database that contains the grant application and summary statement data. Each FIHS component has its own Council process and operational procedures. In order to assist the HSA, the IBCR IT staff has customized views of the grants data by copying the data to a local Oracle database, creating a customized schema and custom interfaces that fit the institute's culture and needs. The HSA needs high availability to email, file space and FIHS and IBCR developed applications for access to grant information. HSAs must also keep up with scientific development and make heavy use of the internet and web resources.

Grants Management staff assist the HSA with the financial side of grants. They track grant funding and disbursement of funds utilizing FIHS-wide applications. Grants Management staff rely heavily on Microsoft Excel and email for communication with grantees along with access to FIHS developed interfaces to financial and grant databases. The Office of Scientific Review relies heavily on FIHS-provided access to the review process, portable laptops for travel and support at review meetings, email and Microsoft Word. Virus protection is important as staff accept reviews in the form of email and floppy disks. Scientific Review staff travel often making reliable and secure remote access to IBCR resources imperative. The single most important aspect of IT in the IBCR is high availability of resources, as most of the core business processes requires access to electronic information. Even a few minutes of down time for a critical application, file server or email is met with an instant telephone barrage. The information processed within the institute is classified as either public or confidential. A particular difficulty in this environment is clearly determining what is public or confidential information, in order to ensure appropriate measures are taken to protect confidentiality.

The IT staff is divided into Operations and Development. Development staff, besides building, maintaining, and providing customized interfaces to the FIHS grants database provides application development for financial applications, intranet application development and other database development. The Operations staff has responsibility for network configuration, implementation, support, security, maintenance and network backup as well as the help desk function supporting all aspects of desktop computing for all IBCR staff. Operations maintain user accounts and provides training and support for office applications and common peripherals such as printers, scanners, video conferencing, laptops, and Blackberries. Upper management has mandated that support be hands-on, therefore most support consists of desktop, face-to-face assistance. Software development or purchases are driven by staff need, federal mandate, FIHS operations, or IT staff looking for ways to enhance processes. Competitive outsourcing mandates have led IT to staff heavily with contractors rather than federal employees. This year the IBCR has run out of office space to

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

house contractors working on IT projects. This will be the first time that it has become necessary to allow contract staff to work on IT systems off-site. Contract staff will provide support; work on applications and databases off site while needing to have online access to IT resources. Traditional remote access has been used mainly to access email and transfer files. Dial-up access is not well suited due to speed issues and the data stream is not encrypted. The IBCR ISSO has suggested the use of the FIHS VPN system to meet this need.

Identify Critical Risks

When discussing risks, the IBCR has clear guidelines defined by the FIHS' parent agency in its Automated Information Systems Security Program Handbook. Security level requirements are based on the sensitivity of data and the impact of unavailability of computing systems. The IBCR processes data of sensitivity levels 1 – 3.

Levels of Data Sensitivity

Level 1 (Low) – Level one data requires minimal protection. Disclosure of level one information would not have an adverse impact (low need for confidentiality) as most of it is considered public data, but it should be protected from unintentional alteration or destruction (protect data integrity). Examples of this type of data are the staff listings on the IBCR Internet web page.

Level 2 (Moderate) – Information of moderate sensitivity must be protected from malicious attacks (protect data integrity). Data confidentiality is considered a lower priority as disclosure of level two data would not cause significant impact as this type of data is usually collected for analytical reasons. Examples of level two data are personnel staffing and workload data, correspondence and documents that have controlled distribution within the organization. This type of data usually has value such that it must be protected from modification but in time most of this data will be publicly released in some format. Privacy act data is included at this level as unauthorized disclosure could cause discomfort or embarrassment to an individual.

Level 3 (High) – Requires protection against unauthorized disclosure (confidentiality) and against modification (data integrity). Examples of this type of information processed by the IBCR is proprietary information contained in grant applications and summary statements, research findings, financial data for authorizing payments to individuals or organizations, grant application review data, and any automated systems of records (a database) that falls under the Privacy act (a collection of personal information) of which disclosure could lead to an invasion of personal privacy.

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

Levels of Criticality

The Automated Information Systems Security Program Handbook (FIHS parent agency) also defines levels of criticality which measure the impact of an interruption or loss of availability of an automated information system, computer or network or the level of impact if the system, computer or network became the victim of fraud or abuse.

Level 1 (Low) – System requires minimal precautions to protect. Failure, alteration of the system or loss of availability would have a minimal impact on the organization's ability to continue. Information could be replaced with minimum staff time and expense.

Level 2 (Moderate) – System processing at this level is important but not imperative to the institutes' operations. An extended period of unavailability of a level two system would not have a devastating impact on the institute.

Level 3 (High) – If a level three system, computer or network is unavailable for even a short period it can have a severe impact on the organization. Examples are FIHS-wide network systems or applications that affect a large number of employees in the various components. Central systems such as e-mail and mainframe services are considered level three. For the IBCR itself, a network failure that denied access to the MS office suite or email would be at this level.

The security level designations outlined above determine the minimum security safeguards the IBCR must have in place. Since the bulk of the IBCR system processes at all levels of data sensitivity and management has indicated that availability is extremely important, IT staff consider the "crown jewels," the critical systems such as file servers, production Oracle database server, help desk application, e-mail server (which is being handed over to the ITC), and the applications server to have level three criticality. The "crown jewels" are more than the grants and financial data as most are contained in databases that the institute itself does not control. The critical information is the various supporting information generated by HSAs and the ability to process grants, financial and administrative data when it is needed. Individual desktops would also be considered to have level three criticality and are replaced immediately if they cannot be fixed as they are necessary for the processing of grants data. IT staff must protect the institute's proprietary or intellectual information resources generated by HSAs and train staff to prevent unauthorized disclosure and inadvertent or malicious modification of data while ensuring a high degree of availability.

In determining risks, threats must be identified. A threat, as defined by NIST's Special Publication 800-30, Risk Management Guide for Information Technology Systems is, "the potential for a threat-source to exercise

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

(accidentally trigger or intentionally exploit) a specific vulnerability." (Stoneburner, Goguen and Feringa 12). The authors go on to define a threat-source as "Either (1) intent and method targeted at the intentional exploitation of a vulnerability or (2) a situation and method that may accidentally trigger a vulnerability." (Stoneburner, Goguen and Feringa 12). One way to determine overall risk is to attempt to quantify threats and vulnerabilities by placing them in Peter Tippett's Risk Equation. "Risk = Threat x Vulnerability x Cost" ("Risk Equation" Tippett) Common threats can be from natural, environmental or human sources. The IBCR considers human threat to be the most critical to the security mission of protecting resources from unavailability and modification. It is important to note that a threat can be intentional or accidental.

The top three critical risk areas for the IBCR are attack of IBCR resources from the Internet AND from within the FIHS network; managing server vulnerabilities caused by configuration error or software vulnerabilities and the protection of resources from internal attack, unintentional or intentional.

Risk – Attack from the Internet AND/OR from within the FIHS Network

The Threat

Government entities are favorite targets for hackers and script kiddies. The press will report failing grades for security in government agencies giving the perception that all agencies are easy pickings (Tillett). This often attracts hackers wishing to test their skills. Political events can lead to government agencies being the target of hackers from other countries in retaliation for specific events or ideologies. With the current war on terrorism, cyber warfare is a concern for all government networks. These types of attacks are probably the biggest threat to the FIHS network. Another attack possibility could be espionage. Scientists from rival universities, corporations, or even other countries might target the FIHS network in attempts to steal research results or patent information. Those first to market a drug or patent a process stand to benefit financially. Bioterrorism is the hot topic of today and all of the Federal Government's health agencies will be participating in bioterrorism research, this could also make the FIHS network a target for other countries.

Significance

A "threat is the frequency of potentially adverse events" (Tippett). The ITC's internet response team provides a weekly chart of attacks on the FIHS network to institute ISSOs. In 2001 there were approximately 18,500,000 events or possible undesired activity recorded. Any of these events might have lead to a possible intrusion. Approximately 4,500 alerts were sent to FIHS ISSOs. Approximately 500 incidents were identified and less than 100 compromises reported. In the case of the IBCR, proactive security is a new tactic. A full time security position was instituted in January 2002. Since then the ISSO has been attending training and evaluating products to help implement proactive security strategies. The IT staff has no tools in place to determine if an alert has led to a

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

compromise, there are currently no active firewall policies in place or IDS to protect the IBCR perimeter.

Reports claim that cyber attacks are on the rise, so FIHS attack numbers are expected to rise for 2002 (Hulme). At this time, the institute has no facility to determine how many attacks are targeted at the IBCR network. Looking at a recent weekly report (see Table 1), approximately 20,000 FIHS hosts were targeted. The FIHS network supports over 20,000 machines. The obvious assumption is that the entire IP range of the FIHS network is being probed for vulnerabilities. The data would seem to indicate that the FIHS firewall and IDS are doing an exceptional job at protecting the network. But new vulnerabilities are discovered daily and it would be dangerous to assume that the small number of compromises from 2001 indicates that there is little to worry about. The practice of defense in depth teaches the concept that multiple layers of protection are important. It would be a mistake for the institute to assume that the FIHS firewall and sensors alone will reduce the risk of attack to an acceptable level. With only three IRT alerts this year the ISSO must not be complacent, for not only is there danger from outside attack but there is a danger of attacks between FIHS components. A compromise of an FIHS component that does not filter outgoing traffic could lead to attacks on the IBCR network. Since the firewall at the institute perimeter currently passes all traffic there is no protection from attacks coming from other components within the FIHS network. The current set up means that any compromise of a machine within the FIHS network could be a potential danger for the IBCR network.

Denial of Service	5,000
Unauthorized Access	42,000
Probes	7,000
Suspicious Activity Abnormal network traffic, may indicate undesired activity	132,000
Protocol Decodes network activity that could be used in undesired methods such as DOS, probes, etc. May or may not indicate undesirable activity.	790,000
FIHS hosts targeted	20,000
Unique Sources	15,000
Anti-Virus detections	38,000
Total Events	1,039,000

Table 1. Sample Weekly Incident Report

Impact Potential

If the IBCR network was breached by an external attack or attack from within the FIHS network the possibilities could range from unauthorized disclosure of data, the alteration of data, to denial of service. All levels of data are processed on the IBCR network. The institute has operated as an open system in that there has been little effort to practice the principle of least privilege, especially in regards to network file access. Staff has access to shared directories even when it is not needed to perform their duties. Configuration

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

mistakes have led to staff having write access to application directories. These problems mean that the compromise of one machine on the IBCR network could lead to compromises of critical servers and possibly to the collection of accounts and passwords that might allow an attacker to access critical databases. An attacker with a user account could access files on file servers, perhaps disclosing information that might pose a threat or embarrassment to a grantee. Alteration of spreadsheets that are used to pay grants could lead to a loss of confidence in the system and loss of credibility for the institute, not to mention causing problems for the investigator in lost opportunities or time spent to fix financial errors. Loss of credibility within the scientific community and with the public could impact biomedical research and future advances. Denial of service could be problematic as high availability of critical services is a management mandate. A malicious denial of service attack which resulted in the alteration of important operating system files would require time to detect and then return the computer to service. Even if the procedure is to simply wipe the machine and rebuild it from back-up there will be some interruption, loss of processing, and possibly permanent loss of data. The IBCR has a limited number of backup machines, making it difficult to take the time to attempt to determine the how of an attack if more than a few machines were brought down by such a denial of service. A big concern would be a compromise that might lead to the alteration of data contained on the FIHS grants databases. Once again, a loss of confidence by the scientific community if grant scores where changed resulting in grants not being funded or grants being funded that might not represent the best science could be devastating.

Likelihood of Exploits

Vulnerability "is the likelihood of success of a particular threat category" (Tippet). As discussed above the FIHS network is the target of thousands of events per day. There is no information available to indicate that the IBCR network is not a target of some of these attacks. While the FIHS firewall and sensors do a very good job of protecting the institute from incoming malicious packets, a compromise in another FIHS component could be a threat because the IBCR does not currently employ firewall rules to protect its perimeter, nor does it employ firewall rules to prevent its network from attacking others. The IBCR does not currently practice an effective process of least privilege which leaves connected services vulnerable to the compromise of a single machine. For the last few months the ISSO has been involved in the study of patch management and vulnerability scanners looking to purchase vulnerability scanning tools. During the testing phase candidate programs identified a number of vulnerabilities per machine. These software holes can allow a hacker to gain access to the network by exploiting software flaws. Until a vulnerability identification and mitigation program is put in place, servers are vulnerable as patches are difficult to install quickly. The IT staff must schedule downtime to test and deploy patches but with new patches and vulnerabilities being identified every day this can prove at odds with management's desire to have a 24 x7 network. All patches need to be tested and then deployed on multiple machines. The IBCR doesn't have the facilities to have an extensive test network so

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

patches would have to be tested on less critical machines with time budgeted to recover from any problems. The entire IBCR network is entirely Windows based, an operating system that is known for its vulnerabilities and ease of exploits unless express care is taken to harden all machines. All desktops have an internet routable IP which makes each desktop a possible target. Institute staff has the typical view of security as being in the way and security awareness training for staff has not been a priority. Users share passwords, leave them posted on their machines and goodness knows how they protect access when on the road. What's the likelihood of an exploit? The old adage is that it is only a matter of time, and it's not if but when would be appropriate. With new exploits appearing almost daily and with hackers from all countries targeting the FIHS network the only assumption the ISSO can afford to have is that it is imperative to protect the IBCR network from outside exploit and from compromises that may come from within the FIHS network. The risk is high due to a high threat probability x the known vulnerabilities; no internal firewall rules, behind in server patches x the cost of lost of public trust and confidence.

Mitigation Strategy

In a risk assessment the threats, vulnerabilities and costs are computed to determine overall risk. Risks usually have multiple mitigation strategies and different risks may share specific mitigation strategies. In the three critical risks discussed for the IBCR some mitigation strategies can be shared across the three risks.

Implement Institute Perimeter Firewall

Plans for mitigation are to extend the defense in depth practice to the IBCR perimeter. The purchase of two Lucent firewalls to create a DMZ and application of firewalls rules is an important step. With the assistance of the ITC the ISSO will implement many of the same rules used at the FIHS perimeter. In some cases the IBCR firewall rules will be more restrictive as some services that may be required for FIHS components are not needed for institute operations. The ISSO is developing rules compiled from information gathered in SANS courses and the SANS Firewall Checklist (Naidu). Best practices dictate that services that are not required have their ports closed at the firewall. For example, some components of the FIHS may require the use of IRC or instant messaging. The IBCR currently has no business need for these services. The institute firewall can block these services while the FIHS firewall may not be able to be so restrictive. In this way the IBCR network defense in depth practice can mitigate risks that the FIHS network has to accept.

Each desktop has an internet routable IP address which makes it vulnerable to probes from the internet. There is no reason to access the IBCR desktop from outside the institute. The firewall should block all access to desktops. With a firewall at the IBCR perimeter network assets can be protected against threats that might get by the levels of protection maintained by the ITC. Another benefit of the firewall will be the ability to respond quickly to new

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

vulnerabilities. For example, the SQL attacks that occurred a few months ago hit late on a Friday evening. The ITC sent out alerts and mitigation methods but most of the IT staff had gone for the evening. Being able to set firewall rules to block these attacks to provide IT staff time to correct vulnerabilities will be beneficial.

Implement Principle of Least Privilege

Compromises can be amplified by the fact that the principle of least privilege is not practiced. As part of a security plan for the institute it is imperative to standardize on and determine procedures to decide who needs access to what information. The IBCR is purchasing Net IQ's Security Administration Suite to help standardize the process of administration of user accounts. This will provide support for authorization processes that are not currently practiced because they are difficult, require manual intervention or require a non-IT approval process.

Install Network Intrusion Detection System

The inclusion of an IDS into the institute's defense in depth program will allow the ITC to notify the ISSO if attackers find their way through the FIHS perimeter firewall or if another FIHS component has been compromised and is acting as a stepping off point for further exploration. The IDS will also monitor the internal network to ensure that a compromise from within the institute is not allowed to attack other machines on the FIHS network or other outside agencies. The IDS will give IT management a better view of how many and what types of attacks are being targeted at the network. This can be used in future risk assessments.

Install Host-Based Intrusion Detection

A major problem with the current network setup is the lack of tools to ensure a server or desktop has not been compromised when an IRT notice indicates that an attempt to penetrate the network has been made. IT management has approved the purchase of the host-based intrusion detection product Tripwire[1]. Tripwire will allow critical server's files to be monitored for alterations. This tool will help the ISSO to determine if a breach was successful. It is important to remember that a firewall, or even multiple firewalls and other defense in depth layers, do not guarantee that an attack will not make it through. Net IQ's Security Management and Administration[2] tool is also on order. It has its own host-based intrusion detection capability and monitors security event logs to provide automatic response to stop security breaches. Net IQ detects trojan horse applications and can shut down processes that are not supposed to be running on a server.

[1] For information on Tripwire see http://www.tripwire.com/products/servers/.
[2] For information on Net IQ Security Management and Administration solution see http://www.netiq.com/solutions/security/default.asp

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

Install Vulnerability Scanner

Risk is the result of a threat and a vulnerability the threat can exploit. The Windows operating system is noted for its high number of vulnerabilities. A vulnerability scanner will assist the ISSO in identifying, prioritizing and patching vulnerabilities. Management has approved the purchase of tools to help in this area. St. Bernard's Update Expert[3] identifies Microsoft operating system and application vulnerabilities and allows patches to be managed from a central location. This product will be used as a quick fix to implement top priority patches and as backup to double check STAT Analyzer's and Hercules' remediation process. Harris Corporation's STAT Analyzer[4] is designed to automate network security assessments. It goes beyond a simple patch assessment product like Update Expert as it checks for patches, compliance to security policy, and for common vulnerabilities such as blank passwords and open shares. STAT Analyzer takes input from some of the best commercial scanners such as Harris' own STAT Scanner, Nessus, ISS Internet Scanner, and Network Associate's Cybercop. IT management has decided upon STAT Scanner. During testing it proved to be fast, generated a minimum number of false positives, and had good reporting capabilities not to mention that it is incorporated into STAT Analyzer and saves the institute money. STAT Analyzer uses the input from STAT Scanner to compare results to the organization's security policy. It helps prioritize a mitigation strategy by looking at multiple vulnerabilities that separately may only equal a low vulnerability but together indicates a highly possible exploit path. The IBCR has also approved purchase of Citadel Software's Hercules[5] product. Hercules takes input from STAT Analyzer and automates the remediation process. Hercules remediates unnecessary services by turning them off in the registry; it can disable insecure accounts and identify backdoors and misconfigurations. Hercules provides details on each solution for those who wish to fix vulnerabilities by hand or Hercules can automatically perform the fix.

Ensure Data Backup Process Protects Resources

As discussed in the IBCR infrastructure section, IT staff has implemented a Compaq Storage Area Network to speed backup of critical servers. The storage area network interfaces directly to the drive cards of these servers providing separate, high speed bandwidth for backup. This shortens what had become a lengthy backup time lasting almost the entire weekend. It will also speed up recovery of files or entire servers if needed. The separate backup path also ensures that backups are successful. A reliable backup procedure is important to recovering from attacks and preventing extended downtime.

[3] For information on St. Bernard's Update Expert see http://www.stbernard.com/products/updateexpert/products_updateexpert.asp.
[4] For information on Harris Corporation's STAT Analyzer see http://www.statonline.com/solutions/sec_policy/index.asp.
[5] For information on Citadel Software's Hercules see http://www.citadel.com/Hercules.asp.

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

Risk – Server Vulnerabilities

The Threat

Server software, applications and operating systems are often the source of vulnerabilities in the risk equation. The threat of outside attack needs a vulnerability to exploit and often that is misconfiguration of software by staff or the vulnerabilities, programming errors and holes that seem to plague all software. Operating Systems and large applications like the Microsoft Office Suite, Oracle databases, Internet Explorer and even home grown applications are very complex programs. It has become a major challenge for developers to test code for every possibility and patch all software holes. In some instances the motivation of being first to market and capturing market share has led developers to cut corners to rush their application to the store shelves. These facts together mean the simple installation of software without a process to include a thorough exam of security implications will often leave an organization vulnerable.

Significance

In a small organization such as the IBCR, the fast moving IT industry poses unique problems. IT management has been tasked with providing the infrastructure needed to perform the day to day duties of the institute while also accommodating new requests for processing capabilities as often as possible. Institute management often takes advantage of new technology as it becomes available. IT staff are asked to implement new services and install software often without adequate time to become thoroughly familiar with its use or without time to adequately test configurations. IT staff do not always have time to keep up with technology via training or conferences. At times, new services have been brought in under contract with a limited time for implementation. Contractors rush through installation and IT staff don't have time to check for possible errors introduced by the contractor's unfamiliarity with institute systems. Staff may have to follow behind contractors and fix compatibility problems while not having any training or knowledge of the system. Currently there are over 40 servers which need to be maintained. There has been little time to worry about security concerns as most of network staff time is devoted to ensuring the continued uptime of equipment. The IBCR has sufficient budget that often new equipment is applied to house new services rather than attempting to run multiple services on a single server. This prevents conflicts from bringing down current services but also increases the complexity of the environment by adding another server to be maintained.

Services provided to the institute have grown over the years with a maximum of four staff responsible for the installation and maintenance of servers. In the past there was little time devoted to documentation as staff time was often taken up with fixing problems or installing new applications. From 1990 through 1999 the four staff responsible for the network also served as the help desk. This provided little time to document, create standards or think about security issues. In the last three years four contract staff has been added to provide the help desk component. Contract help desk staff has become involved

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

in the basic installation of desktops and servers without written documentation to assist them. This lack of documentation and standardization has meant that everyone does installations in their own way. As staff have increased communication of unwritten standards has broken down. It has even been difficult at times to ensure that basic requirements are communicated.

The basic point is that services have grown faster than time has been allowed to properly secure them. Until 2000 security was not a high priority at the FIHS, in the last year it has moved to the forefront. Many of the current services were installed with little consideration for security. There have been few attempts to document procedures to create standards, much less security standards. The need for baselining, auditing and implementation of tools assisting in the creation, maintenance and compliance testing of standards are now recognized as an important part of the processes that need to be put in place. Most IT staff has not had training in IT security issues. While the network administrators are aware of basic security needs, demands of management often push security to the background such that it is not a high priority.

The IBCR has its work cut out for it in that it must assess all current services for security holes and put in place procedures to ensure new services are installed following security best practices. Besides defining best practices, staff must be trained to follow new, more restrictive procedures they are not used to and which may be seen as a hindrance. All IT staff need to be trained to recognize that security is very important and how to make decisions with security in mind. This behavior modification will probably be the biggest challenge for the IT staff.

Along with the staff's weak stance on security, products purchased and installed out of the box make the institute vulnerable. It's a highly publicized fact that Microsoft products usually need patching before they can be considered safe for use. The IBCR is a Microsoft shop. All servers run various flavors of Microsoft's operating system, along with the desktop. The office suite is Microsoft Office XP; web servers use IIS 5.0, along with SQL server, Project Central and some Access databases. If Microsoft products are vulnerable then the IBCR is vulnerable. Microsoft vulnerabilities are so numerous at least three patch products have appeared on the market to help administrators discover and implement patches exclusively for Microsoft software. These problems; staff knowledge of servers, applications and security, the lack of attention paid during software installation which could lead to configuration errors, the weaknesses inherent in the software itself, or exposure caused by the interaction of software can lead to a serious vulnerability problem for the institute.

Impact Potential

Server misconfigurations, lack of knowledge of server applications and vulnerability in the software can impact the institute in two ways. First, even with defense in depth, attacks could find their way through or a compromise in

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

another component could lead to an attack on institute resources. These attacks could mean the lost of confidentiality by allowing an attacker to gain access to a server, allowing them to collect data and distribute it for their own purposes or perhaps alter data and cause the institute to question the integrity of data in its grant or financial databases. An attacker could also perform a denial of service, locking up a server or crashing it. It would take time to discover the attack and to clean up and place the server back in operation or restore missing or altered data. If an attacker altered operating system files the server might have to be recovered from backup, possibly leading to the loss of data and availability of the services.

These types of attacks can lead to embarrassment, the defacing of web pages for example or loss of confidence by grantees if their data was lost. In the current political climate any successful attack on a government network often leads to publicity and a general public feeling that the government does not have a good handle on security.

Server misconfigurations can play a role in opening vulnerabilities that can be exploited by outside attackers. Misconfigurations can also lead to degraded processing and introduce errors into data integrity; such as incorrect grant amounts or consider the impact of an incorrect score on a grant. Misconfigurations can cause downtime or unavailability. Misconfiguration errors can be very hard to trouble shoot, especially on systems that network staff may not have installed themselves or have little knowledge of. Misconfigurations can cause intermittent glitches that are difficult to diagnose and lead to frustration for IT staff and users alike. If institute staff doesn't have confidence in IT and its infrastructure they might begin to go around them or seek alternative means to do their work which could lead to security problems.

Likelihood of Exploits

The likelihood of an exploit can be calculated with the risk equation. Risk = Threat x Vulnerability x Cost. Past experience has taught the security community that vulnerabilities in Microsoft and other products can be serious. Code Red, Nimda and more recently the Bugbear email worm have shown that vulnerabilities among common platforms can be used to wreak havoc across the Internet. Since Windows operating systems are commonly in use, along with Outlook being a common email client, exploits are passed along from organization to organization effecting hundreds, thousands to hundreds of thousands of users. The security community has often lamented that many of these vulnerabilities are well known and patches have been available for long periods of time. For example, patches that would prevent infection by the current email worm threat, Bugbear, have been available for over a year. Organizations are not keeping up with vulnerability mitigation, putting them at risk. The ITC has negotiated site licenses for Microsoft operating systems and products. These products are in common use across the FIHS; compromise of one component can quickly spread to others within the FIHS. Knowing that the institute IT staff,

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

like many other organizations, have many duties, that it has been searching for tools to help manage numerous vulnerabilities and considering the number of attacks on the FIHS network the likelihood of an exploit must be considered as high. The threat is clearly there and the ISSO knows that vulnerability mitigation is a very important priority that must be addressed.

Mitigation Strategy

The mitigation of risks posed by server compromise is heavily dependent upon the attention staff pays during installation and maintenance of servers. A commitment to a standardized, security minded procedure will go a long way in reducing the chances of misconfiguration and ensure potential vulnerabilities are addressed as soon as possible. The IT staff will put the following procedures in place.

Implement IT Security Training for All IT Staff

Staff needs to understand the reasons for IT security and the overall picture of how it protects the institute's resources. Each staff member must be aware that security begins and ends with them and that procedure must be followed to the letter as they are in place to help standardize the installation process using best practices. If there is a question or a suggestion to make a process more efficient or more secure, staff must not take it upon themselves to implement it but discuss changes with management. To ensure that staff takes security seriously the ISSO suggests that a security element be placed in all IT staff's performance reviews as well as in performance reviews for contractor. The FIHS is developing a security awareness course targeted at IT staff; the ISSO recommends that it be mandatory for all institute IT staff, along with a yearly review. The ISSO also strongly suggests that network administration staff and contractors take basic security courses. A decision on which course has not been made at this time, perhaps the new Fundamentals of Network Security course by Microsoft or introductory SANS courses.

Write Policy and Procedures for Server Installation

The ISSO, Chief of IT Operations, and network administrators will work together to create a standard procedure for the installation of all servers. The procedure will define the specific steps required to install Windows 2000 servers, Windows 2000 Advanced server, Web servers and database servers. The ITC has released security guidelines for hardening servers and desktops. The IBCR procedures will build on these guidelines and will include sections that cover the removal of unnecessary services, running a vulnerability scanner against the server and using benchmarking tools such as GFiLANguard Network Security Scanner[6]. Network Security Scanner takes a snapshot of a machine's configuration including open ports, network shares, services, accounts and indicates potential problems. Reports can be archived and then compared to later reports making them suitable for auditing changes to the servers. A similar

[6] For more information about GFILANguard Network Security Scanner see http://www.gfi.com/lannetscan/index.htm.

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

tool, Active Network Monitor[7] reports on the applications installed and also allows reports to be generated and compared against later ones. These reports will be saved on the network and later snapshots compared on a monthly basis.

When a Windows 2000 Server and Advanced Server Gold template is released from the Center for Internet Security (CIS) it will become part of the server installation procedure. IT staff will customize the template to fit the IBCR environment and then apply it to various servers. The CIS scoring tool[8] will be used to benchmark the security settings of each server. All software upgrades and even patches will be followed by a vulnerability scan and scans by the CIS scoring tool. Tripwire will be implemented on critical servers to monitor the operating system and important files for changes. This will require any valid changes by administrators to be documented so that file changes can be incorporated into Tripwire's reporting. A similar install procedure for Windows 2000 desktops is currently under development. Once the desktop procedure is complete, the server procedure should be easy to develop as the process is similar. These installation procedures will be followed by all IT staff and contractors. Temporary contractors, those brought in expressly to install a system will be required to review their install procedures with the ISSO and network administration staff to ensure that it follows all guidelines of the server install procedure.

Institute Auditing Tools and Procedures

Once servers are installed and put into place they need to be routinely audited for compliance to security policy. The tools mentioned to gather reports during server configuration can be used periodically to compare against current snapshots. Unexpected changes will be reviewed for possible compromise or as indication that staff is not following policy. Security, application and system logs will be reviewed for errors to indicate configuration problems or possible security compromises. Management has approved the purchase of Net IQ's Security Management and Administration Suite. Its Security Manager[9] application consolidates event logs. This will assist the ISSO and network administrators in checking for events that may indicate configuration problems across the enterprise. Security Manager also monitors security configurations and enforces configuration compliance. In conjunction with Microsoft's Security Configuration Manager the security policy is pushed out to servers and then audited for compliance. Changes made by the installation of patches, software or changes by staff will be noted and if vulnerabilities are introduced they can be quickly fixed before there is a chance of them being exploited.

[7] For more information on Active Network Monitor see http://www.protect-me.com/anm/.
[8] For information about Windows 2000 security benchmarks and the CIS scoring tool see http://www.cisecurity.org/.
[9] For more information on Net IQ's Security Manager see http://www.netiq.com/products/sm/default.asp.

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

Install Institute Perimeter Firewall

The firewall installed at the IBCR perimeter will aid in defense in depth to help prevent the initial compromise of servers. Common ports and vulnerabilities identified by SANS can be blocked for all servers. When CERT notices report that potential vulnerabilities are being exploited a firewall rule can be put in place to prevent access to those ports to provide time for IT staff to repair vulnerabilities. As part of server hardening all unnecessary services should be disabled. With large applications and operating systems it can be very difficult to know what services are necessary. Upon installation of a new application staff needs to know what services were running to determine what new services may have been installed. In the event that a service is overlooked or for older machines which have no previous configuration information, implementing the firewall principle of denying all except that expressly approved will help ensure that any entry port to these overlooked services will be blocked at the firewall.

Install Host-Based Intrusion Detection

Why would host-based intrusion detection be a mitigation tool for server misconfiguration? Depending on how host-based intrusion applications are developed and implemented they can be used to point out configuration changes as well as possible compromises. The host-based intrusion detection application Tripwire monitors the operating system and other important server files. If the server is updated or changed without notifying the administrator or ISSO, Tripwire will send an alert. Network staff can research the change and ensure compliance to security policy by investigating why the change was not reported and documented. This alert procedure can prevent malicious acts by IT staff or contractors while providing a feedback mechanism that can be used to train network staff on the importance of documenting and planning configuration changes. It will be a challenge for the IT staff to move from a loose operating environment to a more restrictive, policy guided environment. Host-based intrusion tools point out configuration changes and allow management to council staff on proper procedure without having to wait for a possible disaster to reveal configuration problems.

Net IQ's Security Management and Administration tool allows the ISSO to create security rules and enforce compliance. It automatically enforces policy and helps prevent configuration mistakes. This assists staff in the difficult job of server configuration and maintenance. The Security Manager assists by providing security expertise via a knowledge base in which the ISSO can input specific security knowledge for and about the institute's network. This creates a personalized knowledge base that can be used by network staff to deal with security incidents.

Install Vulnerability Scanner

Once a server is configured and put into place there are things to worry about other than hardware malfunction and software upgrades. Vulnerabilities are discovered every day in Microsoft applications and the operating system.

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

Holes must be continuously plugged by installing software patches released by the developer. The ISSO tested and selected a vulnerability scanner and vulnerability mitigation tool to assist the institute in keeping up with software holes, Trojans, patches, and misconfigurations. The two products work in conjunction with each other to provide scanning and then automatic mitigation.

Harris Corporation's STAT Analyzer scans the entire network for needed patches, compliance to security policy, and for common vulnerabilities. STAT Analyzer uses its own STAT Scanner to quickly scan machines, and then Analyzer attempts to minimize false positives. It compares results to a chosen security policy and helps prioritize vulnerabilities to bring those which need to be mitigated first to the forefront. Citadel Software's Hercules takes the vulnerability results from STAT Analyzer and automates the remediation process. Hercules can turn off unnecessary services by making registry changes; it can add passwords or disable accounts that are insecure and it identifies backdoors and misconfigurations. Hercules provides detailed solutions for mitigation of all listed vulnerabilities. Hercules can roll back patches and other fixes and will release a version by the end of this year that can roll back registry fixes. If a problem occurs due to mitigation, simply roll back the fix and research the problem. These two tools will give the ISSO a fighting chance to mitigate the current vulnerabilities that are the result of years of installations with little consideration for security. They will also help the ISSO respond quickly to CERT notices of new vulnerabilities as all servers can be repaired from a single console at the same time. During testing of these products over 4,000 vulnerabilities were identified on a small representative number of servers. These tools will be imperative in bringing the institute up to date on patches.

In addition to STAT Analyzer and Hercules, the IBCR has implemented St. Bernard's Update Expert which is a patch management program. It identifies missing patches in Microsoft operating systems, SQL, Exchange, Internet Explorer, Office and Outlook products. Update Expert allows patches to be rolled out to all machines from a central location. This product will be used as a quick fix for top priority patches and as backup to double check Hercules remediation. It can deploy a patch quickly when the specific patch is known, rather than having to run Analyzer to scan machines which can take some time. With these tools, the institute can manage the flaws in software that lead to exploits thereby securing the servers and preventing downtime, denial of service, data alterations and disclosure of information. Hopefully, this will allow the network administrators more time to concentrate on preventing hardware malfunctions.

Ensure Data Backup Process Protects Resources

A reliable backup procedure is important to prevent extended downtime in the event a server is compromised. The Compaq storage area network protects critical servers. A more traditional system protects the remainder of the servers. If a server fails it can be reinstalled from backup usually within an hour. A quick

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

and flexible backup system can also be used to backup a compromised system to save it for forensic investigation while restoring services to the institute.

Risk – Protection against internal threats – unintentional or intentional

The Threat

While IT security spends much of its time securing the organization's networks from outside threats it is important to remember the threat that may come from inside. Before the Internet most compromises came from the inside or from traditional forms of espionage. As the popularity of the internet has grown the spotlight has been turned outward to the hacker. The media's reporting of hacker's activities has led many to believe they are the biggest threat to security. Management does not want to believe that employees would harm the organization but new research from PricewaterhouseCoopers, the U.S. Chamber of Commerce and the American Society for Industrial Security indicates that insiders may still be the biggest threat to an organization (Perez).

The insider threat can be intentional; a disgruntled employee, contractor or vendor or corporate espionage by paying an employee or contractor for information or infiltration by a rival company or vendor. The insider threat can come from any one that is allowed access to the network either on a permanent or temporary basis. An unintentional threat can be a careless or untrained employee, temporary employee or a vendor installing test software to demonstrate a product. The IBCR has run out of space for needed contract employees which will necessitate allowing contractors to remotely access institute resources. Remote access adds another dimension to insider threats by extending the network to unknown environments. One serious insider threat is the untrained network administrator or IT employee with access to network resources.

Significance

The IBCR prides itself on its family-like work environment and management would find it difficult to believe that an employee would attempt to harm its resources. Nevertheless, every day employees download software when the IBCR policy clearly indicates they are NOT to install software on their desktops from home or from the Internet. While employees are not intentionally trying to destroy or disclose information they are putting the network at risk of virus infection, Trojans or denial of service. Employees have also been asked not to read private email from web clients such as Yahoo or Hotmail as this bypasses virus filters placed at the email gateway and the email server leaving only the desktop virus program to prevent an infection. Web-based email circumvents the defense in depth process for email. There is also the occasional employee who feels they are computer knowledgeable that may try to tweak desktop settings, create shares to access the hard drive from an Institute laptop or may use

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

services such as GoToMyPC[10] to access the desktop from home. The employee is usually trying to make their job easier and is often unaware of the security implications of these actions.

The IBCR has made use of onsite contractors for years. As IT has become more important to the institute's day to day activities contractors have been added until the IT office space has reached capacity. This year new contract staff will be added that will be working offsite and will need access to network resources. Some of these contractors will be supporting databases and providing network support which will require administrative access to critical servers. Along with contractor's need for remote access the government is beginning to push telecommuting. This means staff will need access to network resources from home just as if they where on site. Telecommuting staff pose problems when considering they may be using their own, possibly compromised computers. Their family may have access to the computer and introduce viruses or trojans. In some instances, staff has been known to use FIHS provided internet access as their private service and allow family members to use the PC just as if they were on AOL.

As discussed when covering server vulnerabilities, IT staff have often had to quickly install new applications with little time to become familiar with their operation. Untrained staff can be a danger if mistakes lead to exploitable vulnerabilities. Once again this is often unintentional. The staff person that normally works on a server may be unavailable when there is a problem and someone else may be directed to fix it but their lack of knowledge of the system leads to a misconfiguration. Junior staff may not be fully aware of all the steps required to install or upgrade an application and introduce configuration errors because they made assumptions and did not ask for assistance. Senior staff may feel they don't need to read manuals, they know it all already. The IT staff has seen each of these scenarios, if not actually participated in them. Management and IT staff hope there are no intentional threats. The only precedence is the theft of desktop computers and laptops which were likely perpetrated by service personnel such as movers, cleaning staff or construction crews or someone posing as one. In all likelihood these thefts were specifically to profit on the hardware but its possible that access to data could have been a motive or could be an unintentional outcome.

Impact Potential

An insider threat could lead to intentional or unintentional disclosure of data by releasing information to unauthorized personnel or by installing software that may lead to vulnerabilities. A disgruntled employee could change or delete data. An intentional change in grants data could give a grantee an unfair advantage, perhaps increasing the score of an application or the score of an

[10] GoToMyPC is a remote access service similar to PC Anywhere. The connection is initiated by the corporate desktop, thereby bypassing the firewall which does not perform egress filtering. For more information on GoToMyPC see https://www.gotomypc.com/.

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

application could be reduced. Grants information may contain proprietary or patent information that might be worth cash in the scientific community. Disclosure of privacy act information could cause embarrassment or perhaps allow identify theft. Contractors could gain access to statements of work that would give them inside information and provide an unfair advantage when responding to requests for proposals. Contractors could prolong time and material work by sabotaging their work. Any of these events being reported in the press would lead to embarrassment to the institute and further public mistrust of the government. If the event was serious enough it could lead to congressional inquiry. In the last few years stories such as the discovery of 25 years of spying by FBI Agent Robert Phillip Hanssen through internal hacking (Verton) and Judge Royce Lamberth's (Mencimer) order to disconnect parts of the Bureau of Indian Affairs from the internet for weak security have made the public and commercial sectors doubtful about the ability of government entities to secure data. It is imperative that all IBCR staff do their utmost to protect information resources and keep the public trust.

Telecommuters and offsite contractors provided access from remote locations have more time to commit mischief at their offsite locations. They can explore the network and cover their tracks at night during times when IT staff is not available to notice problems. If remote access is via the shared IP range of FIHS' remote dial-in or VPN service it may make it difficult to determine who is attacking the network. The ISSO would have to take logs with access times and IP addresses to the ITC to have them track down what accounts were in use during that time. Another problem with remote access, besides the potential to perpetrate attacks, is the possibility of introducing viruses, trojan programs or allowing an outside hacker a path into the system on the back of a remote access method. There are three ways for remote access, the FIHS provided dial in service, the FIHS provided VPN service, currently in final testing and via the internet utilizing NetBIOS, WINS and DNS information.

Likelihood of Exploits

Unintentional compromises have a high likelihood as staff has not had security awareness training for a few years. The IBCR does not have its own security awareness program. A new web-based security awareness program will be released shortly for the FIHS community. Though IT management has repeatedly sent email explaining policy that indicates staff is not to download software or bring in software from home there are users who seem to forget. Some of this is due to lack of knowledge. Is clicking on the update button for an internet tool a download? What about a game or software that enhances the browser experience? It has proven difficult to train users on the concepts of what is software and what is downloading. It is easier to have a policy that says no downloads, period. Why does staff continue to download? There has been little to no effort to enforce the policy, consequences are almost nonexistent. If there are consequences it is usually minor; the removal of the software, but rarely is failure to comply with policy reflected in performance or personnel records. As

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

long as consequences are non-existent or minor some staff will continue to ignore the policy.

Suitability determination of IT staff is becoming an issue in the FIHS. Checks of new government hires usually include a minor background check for a police record and fingerprinting. Contractors may perform background checks on their employees but there has been no contract language that required confirmation of suitability of contract employees. Background checks can help to prevent the hiring of unsuitable employees. It's possible, without adequate background checks, that the institute may be opening its network to a possible threat.

Mitigation Strategy

Institute IT Position Sensitivity Levels and Background Checks

FIHS' parent agency has a mandate that all IT positions, federal government or contractor, be labeled with a position sensitivity level. All IT staff must have background checks and be cleared for a specific sensitivity level from one through six. The IBCR management will make a determination of what sensitivity level each position in IT requires. There are six sensitivity levels. Most IT staff positions at FIHS are expected to be rated at a level 5, public trust positions. Contractors will be working on the same data; therefore their levels will also be at five. The personnel office must initiate the paperwork for background checks for all government employees. Contract language has been suggested for IT contracts stating that it is the contractor's responsibility for initiating background checks on all personnel they propose to fulfill a contract. Since the IT support contract is already in place, the contract will be modified and background checks will begin as soon as possible. Contract staff failing a background check will not be allowed to work in an IT position on the contract.

Implement Remote Access Strategy

Internal staff and contractors are beginning to require access to institute resources from remote locations, home or off-site offices. There are security issues with remote access. One is the assurance that the remote location is adequately protected. For home users the only real way to ensure that is to provide telecommuters with the necessary equipment, set it up with the security of the network in mind and institute policy that forbids the equipment to be used for personal use. The FIHS is currently discussing a policy requiring all telecommuters to have institute provided equipment. Contractors who are off-site have to provide their own equipment as indicated in contract language. The ITC is working on contract language that would hold contractors to some level of assurance that they follow security procedures to at least match the FIHS's security precautions. Wording of the regulations are being debated at this time.

The ISSO has advised IT management that all remote access should, by policy, be via the FIHS' VPN or dial-in service. Last week the ITC shut down all

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

NetBIOS access to the FIHS network. This closed an access avenue computer savvy staff had used to access file shares and email. The only remaining access avenues will be VPN or dial-up. All dial-up and VPN access requires the user to have a separate remote access service account. Once validated, packets travel through a DMZ and are scanned by anti-virus, monitored by an IDS and all email is filtered. This helps protect the FIHS network and stops hitchhikers. Once inside the FIHS firewall staff can access network shares and email. The VPN solution adds a personal firewall that is pushed down to the client and cuts off all outside access to their 3rd party ISP during the VPN connection. At this time, these are the most secure access avenues available to the institute. While neither of these solutions will prevent malicious insider attack on the network, host intrusion detection can look for anomalies from the IP ranges for these services and break connections on suspect activity. The process packets must travel through before being allowed into the FIHS firewall help reduce the chance of unintentional attack by not allowing staff to carry a malicious hitchhiker into the network.

Implement Principle of Least Privilege

Implementing the Principle of Least Privilege allows access to only the information needed for staff to perform their duties. This prevents accidental harm to data that is outside the scope of staff's duties. There is still the chance that the data a staff member is authorized to access can be unintentionally harmed but least privilege limits the amount of harm that can occur. Principle of Least Privilege can be implemented via placing access controls on sensitive data. IBCR policy requires all staff to have a network account. All network resources have access controls to prevent those without a network account from accessing servers. Once staff has an account very little of the data has been classified and set up with internal access controls. The ISSO proposes that data be classified per roles and staff roles be matched to access lists. The ISSO also proposes that a process be implemented that requires management approval when staff request access to certain resources.

IT staff have different duties which require different levels of access. Currently the bulk of IT staff has administrative access because there has been no facility to provide granulated access for administrative needs. The IBCR will be moving to active directory shortly, this should help with some aspects of providing granular administrative capabilities to IT staff. Also, Net IQ's administrative module allows IT staff to be granted specific access based on roles. For example, help desk staff will be responsible for adding network accounts for new staff and assisting staff with forgotten passwords. In NT that would require them to have administrative access but this provides them with full access to the servers and full administrative functionality. The help desk do not have responsibility for the network and should not have access to the full administrative functions of Windows 2000. The implementation of Net IQ's security and administrative application should allow administrative access to be granted based on particular roles. It will be more of a challenge to provide the

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

appropriate access contractors working off-site require. IT management, the ISSO and contractor will need to determine the requirements for access.

Install Host-Based Intrusion Detection

A disadvantage of the current network setup is the lack of tools to ensure a server or desktop has not been compromised. This means that if an attack is perpetrated from an internal source the ISSO has no tools to determine if harm has been done, just as with an outside attack. The implementation of Tripwire will alert the ISSO when files have been altered. Tripwire will allow the ISSO to track the internal breach and repair policy, procedure or settings that allowed it to happen.

Net IQ Security Management and Administration tool's host-based intrusion detection capability and the monitoring of security event logs will assist in detection and the protection of the network from inside attack. IT staff will set thresholds that allow Net IQ to determine when a breach has occurred and to provide an automatic response. Net IQ detects unauthorized processes running on a server and shuts them down protecting against trojans.

Install Network Intrusion Detection System

While the network intrusion detection's main responsibility will be notification of possible attacks from outside the IBCR network, it can also notify the ISSO of attacks originating from within the network. Stopping attacks coming from inside reduces the institute's liability for damage to another network. This is necessary to ensure that the IBCR is practicing due diligence. The IDS may be able to identify possible attacks occurring within the network.

Install Vulnerability Scanner

The installation of STAT Analyzer will allow for the identification of vulnerabilities that insiders may be able to exploit intentionally or unintentionally. Usually these types of vulnerabilities will be configuration errors. STAT Analyzer allows the ISSO to scan and check for policy conformance. These types of scans will help to close open shares and replace blank passwords. After a new server is installed or upgraded it can be scanned to identify potential configuration problems. Patch management programs allow IT staff to patch Microsoft applications as holes are reported. Many of these holes in the Office Suite, the browser or email could be the vector through which staff may inadvertently place the network in danger. Institute staff are not computer experts and the IT department must find ways to protect network resources without having to attempt to teach staff of all the dangers present on the web.

Implement IT Security Training for All Staff

All IBCR staff needs to understand why security is important and the role they play in protecting the institute's network. All staff members must be aware that security begins and ends with them and that policy is put in place to protect them. The ITC plans to release a web-based security awareness course targeted

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

at FIHS staff. IT management plan on requiring all staff to take this course. The ISSO will suggest to management that new employees be required to prove completion by printing out a certificate and presenting it to their supervisor. Knowledge of security responsibilities and knowledge that IT staff monitors network activity might prevent someone from casual exploration. It probably will not prevent a malicious co-worker from pursuing a specific goal, but it might very well prevent the summer student or temporary employee from exploring and possibly being the source of an exploit.

The ITC is currently developing a specific security awareness module for IT staff. Providing IT staff with training is also important. Hopefully the importance of checking twice and asking when not sure will sink in. That attention to detail during the installation of a server or software is the front line in preventing vulnerabilities. Teaching them that security is imperative, what to look for to recognize possible breaches and when to ask for assistance is important. Great security can only be achieved through a team effort. The ISSO plans to give security briefings in staff meetings as a way to discourage any IT staff that might have maliciousness in mind from attempting to hack the network. Enough information would be presented to indicate that any malicious acts would be detected. If everyone feels security is their job then bad apples will be easy to detect with all staff on the lookout for anomalies.

Write Policy and Procedures for Server Installation

Creating policy and putting in place procedures for sever installation and configuration was discussed in detail in the Server Vulnerability risk section. Creating better procedures that will ensure severs are secure will help close possible vulnerabilities that internal staff may exploit. Closing holes will reduce inadvertent or unintentional problems. While it will be difficult to prevent computer savvy, malicious staff from abusing their access, configuration standards and occasional auditing will go a long way toward making their activity unsuccessful.

Institute Auditing Tools and Procedures

Routine auditing of servers for policy compliance and configuration changes can provide clues that internal staff may be attempting to attack servers. GFiLANguard's Network Scanner and Active Network Monitor allow snapshots of server configurations to be saved for later comparison. Unexpected changes will be reviewed for possible compromise. Security logs will be reviewed to check for unauthorized access. Net IQ allows the collection of all security logs from servers to a central console, therefore preventing deletion or clearing of log activity. These tools allow the ISSO to check for changes on a monthly, weekly or daily basis. If there is reason to believe there are problems from ongoing attacks the ISSO can check tools daily looking for evidence.

Ensure Data Backup Process Protects Resources

A reliable backup procedure is an important mitigation step. It is important to prevent extended downtime in the event a server is compromised or data is

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

deleted or altered. The Compaq storage area network protects critical servers. A more traditional system protects the remainder of the servers. Good backup has proved invaluable. IT staff are called a few times a month to replace files that have been deleted or overwritten by mistake.

Evaluate and Develop Security Policy

Server vulnerabilities can be a major exploit path for intentional and unintentional attacks. Since neither the IBCR nor the FIHS have a specific policy on securing servers and the IBCR ISSO feels this is a particularly important policy for the IBCR Security Plan the author will evaluate and develop a Server Security Policy from a SANS template. This template was obtained from the SANS Security Policy Project. The template is available at http://www.sans.org/newlook/resources/policies/Server_Security_Policy.pdf.

Server Security Policy

1.0 Purpose

The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by <Company Name>. Effective implementation of this policy will minimize unauthorized access to <Company Name> proprietary information and technology.

2.0 Scope

This policy applies to server equipment owned and/or operated by <Company Name>, and to servers registered under any <Company Name>-owned internal network domain.

This policy is specifically for equipment on the internal <Company Name> network. For secure configuration of equipment external to <Company Name> on the DMZ, refer to the *Internet DMZ Equipment Policy*.

3.0 Policy

3.1 Ownership and Responsibilities

All internal servers deployed at <Company Name> must be owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by InfoSec. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by InfoSec.

- Servers must be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:
  - Server contact(s) and location, and a backup contact
  - Hardware and Operating System/Version
  - Main functions and applications, if applicable
- Information in the corporate enterprise management system must be kept up-to-date.
- Configuration changes for production servers must follow the appropriate change management procedures.

3.2 General Configuration Guidelines

- Operating System configuration should be in accordance with approved InfoSec guidelines.

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

- Services and applications that will not be used must be disabled where practical.
- Access to services should be logged and/or protected through access-control methods such as TCP Wrappers, if possible.
- The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
- Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication will do.
- Always use standard security principles of least required access to perform a function.
- Do not use root when a non-privileged account will do.
- If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).
- Servers should be physically located in an access-controlled environment.
- Servers are specifically prohibited from operating from uncontrolled cubicle areas.

3.3 Monitoring

- All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:
    - All security related logs will be kept online for a minimum of 1 week.
    - Daily incremental tape backups will be retained for at least 1 month.
    - Weekly full tape backups of logs will be retained for at least 1 month.
    - Monthly full backups will be retained for a minimum of 2 years.
- Security-related events will be reported to InfoSec, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
    - Port-scan attacks
    - Evidence of unauthorized access to privileged accounts
    - Anomalous occurrences that are not related to specific applications on the host.

3.4 Compliance

- Audits will be performed on a regular basis by authorized organizations within <Company Name>.
- Audits will be managed by the internal audit group or InfoSec, in accordance with the *Audit Policy*. InfoSec will filter findings not related to a specific operational group and then present the findings to the appropriate support staff for remediation or justification.
- Every effort will be made to prevent audits from causing operational failures or disruptions.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Term	Definition
DMZ	De-militarized Zone. A network segment external to the corporate production network.
Server	For purposes of this policy, a Server is defined as an internal <Company Name> Server. Desktop machines and Lab equipment are not relevant to the scope of this policy.

6.0 Revision History

Evaluate Security Policy

The SANS security template is not specific to an organization so it will need customization to fit the IBCR needs. In evaluating the template it lays a

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

clear and basic outline of who is responsible and what should be done. The template is ready to have organizational specifics filled in to make the policy IBCR's own. The purpose is clear and concise as policy should be. There is no background as each organization is unique and must provide their own. The basic reasons why an organization requires a server security policy will be similar for many but the specific circumstances, prior history and the steps taken to reach this point of creating and implementing policy will be unique for each. Policy should reflect this uniqueness in its background. The scope for this policy is good in that it separates internal servers from those placed in the DMZ. This reflects the differences in hardening requirements and separate policy ensures there are no misinterpretations which might lead to compromise. A good policy statement specifies what is to be done; it defines the actions that will most benefit the organization. It clearly states who is responsible for carrying out the policy, how it shall be enforced and the consequences for failure to comply.

The policy states that the internal server's configuration and maintenance should be owned by a specific group. This is advantageous as a single group having responsibility helps to promote standards and aggregate server expertise. The policy also states that configuration guides must be established. These will be the guidelines and documentation necessary to set standards. Standards ensure that each server is installed in the same way, every time and all steps necessary to harden them are taken. The policy dictates that configuration guides should be based on the business needs of the organization. This ties policy into IT strategy. The policy requires that those responsible for server maintenance put a process in place to monitor compliance; this ensures that all the hard work put into the initial installation of the servers will continue to be maintained. Without this maintenance the simple aging of software would invariably open vulnerabilities. Good policy also realizes that there are always exceptions and this template includes directions to create an exception policy.

The sample policy also covers the maintenance of the guides used for installation. This is necessary as things change, often quickly in the IT field. Without the policy requiring its upkeep, documentation often is the last consideration in a busy IT shop. Another positive aspect of this template is the requirement for guides to be approved by the Information Security organization. This is a check of the processes to ensure the operations group is aware of current security issues and that they implement processes that take into account security issues as conditions change. This oversight means that those who are tasked with the maintenance of the servers are not the only personnel creating the guidelines as operations staff may overlook important steps they don't deem necessary.

The Server Security policy requires servers be registered with a contact name, location, and information on hardware and OS versions along with a list of its functions. It requires that this information be kept up to date and that all changes go through a change management procedure. Often network

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

administrators know they should keep this information, but in a dynamic atmosphere it can be difficult. Policy should provide staff the time required to maintain this information. This points out that policy must be endorsed by management; there must be a commitment to take the time and effort necessary as required by the policy. Otherwise, why create the policy in the first place?

The policy dictates that the operating system must be configured in a secure manner which is approved by the security team. This insists that the network administrator and the security officer work together to protect resources. It provides a mandate and consequences if network administrators decide security is too much trouble and they attempt to skimp on security. It dictates that services not needed will be disabled, patches will be applied as soon as possible, access-control methods must be put into place practicing the principle of least privilege, and servers will be placed in a locked LAN room. These are all common sense procedures but due to lack of time IT staff often doesn't get to complete these steps. Policy provides the reason and authority to maintain these procedures.

The sample policy puts into writing the basic steps required for logging and gathering audit trails. Once again these are things IT staff should be doing but don't always have time to implement. Placing them in policy implies that management believes they are important steps and that the time needed to perform these duties will be provided for staff. The policies provide the outlines needed to produce procedures for staff to follow. It also indicates what is considered an incident and who to report incidents to. The sample policy is comprehensive and would only require customization of the time frames for specific organizations. For example, if there is enough storage space the IBCR might want to maintain logs for longer than a week and weekly and monthly backups are controlled by governmental guidelines.

The weakest part of this specific policy, in the author's opinion, is the monitoring and reporting of security related events. This section implies that the organization is using tools such as an IDS and perhaps host-based intrusion detection. Depending on the organization the use of such tools should be required and perhaps this should be included in the policy. The author also feels that the policy should indicate the use of a vulnerability scanning tool. Patch management is already mentioned but all servers should be scanned for vulnerabilities before being put into production and on a periodic basis after that. Another weakness is there are no time limits placed on reporting of incidents. The author would suggest adding language that would indicate incidents must be reported to security as soon as discovered using an incident reporting procedure. Security must investigate within a specific amount of time and report to management within a specific time frame. Corrective action must be taken within a certain amount of time and reported as completed to the security officer.

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

Last but not least the policy covers how compliance will be tested, who has responsibility for conducting compliance testing, to whom results will be reported and points to an audit policy that guides the auditing process. The author might consider applying a schedule for audits, such as they will occur at least yearly or perhaps when a major configuration change is made. The policy must clearly indicate that management is behind it. Internal IT functions such as a server security policy should be signed by the CIO.

Revise Security Policy

Server Security Policy

1.0 Purpose

The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and operated by the GIAC Institute of Basic Cellular Research (IBCR). Effective implementation of this policy will minimize unauthorized access to the GIAC Institute of Basic Cellular Research (IBCR) proprietary information and technology.

2.0 Related Documents

Place links to Server Configuration Guide, Exception Policy, and Internet DMZ Equipment Policy here.

3.0 Background

The IBCR IT branch has seen the network grown from 5 servers to over 40 servers in use today. The network administration staff had responsibility for the help desk up until approximately three years ago. Over the last three years network administration staff have been training contractors in help desk procedure and installing new applications and servers. Network staff has not had time to document installation procedures. With the federal government's attention turning to increased security, it has become necessary to implement baselining procedures and to standardize server installation to ensure that the appropriate security is in place to protect the institute's information resources.

4.0 Scope

This policy applies to server equipment owned and operated by the GIAC Institute of Basic Cellular Research (IBCR), and to servers registered under any GIAC Institute of Basic Cellular Research (IBCR) -owned internal network domain.

This policy is specifically for server equipment on the internal Institute of Basic Cellular Research (IBCR) network. For secure configuration of server equipment external to the Institute of Basic Cellular Research (IBCR) on the DMZ, refer to the *Institute of Basic Cellular Research (IBCR) Internet DMZ Equipment Policy*.

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

5.0 Policy

5.1 Ownership and Responsibilities

All internal servers deployed at the Institute of Basic Cellular Research (IBCR) are owned by the IT Operations Section (ITOS) of the IBCR's Information Resource Management Branch. The network administration group is responsible for all server installation, administration and compliance. The ISSO is responsible for development of security guidelines, auditing of servers and compliance testing.

5.2 Action

A Chief of ITOS approved server configuration guide must be established and maintained by the network administration group, based on IBCR business needs and approved by the Information Systems Security Officer (ISSO). The network administration group and ISSO will monitor configuration compliance. An exception policy will be written by the ISSO and approved by the Chief of ITOS. The exception policy will be posted in the LAN room and made available from a central network location. The network administration group will establish a process for changing and updating the configuration guides. The process will include reviews by the ISSO and approval by the Chief of ITOS.

- Servers must be registered in the IBCR asset management system along with informing the ISSO of deployment of new servers. The following information is required to positively identify the server:
    - Server name, URL and IP address, LAN Tap no.
    - Name of Installer, person with knowledge of apps, Name of backup staff
    - Location of Backup service (Sans or Traditional)
    - Hardware, Operating System/Version
    - Who requested, who approved
    - Main functions and applications, if applicable
    - Special considerations
    - Who needs administrative access
- Information in the IBCR asset management system must be kept up-to-date along with changes forwarded to ISSO.
- Configuration changes for production servers must follow the appropriate change management procedures.

5.2.1 General Configuration Guidelines

- Operating System configuration should be in accordance with approved ISSO and FIHS security guidelines.
- Services and applications that will not be used must be disabled where practical.
- Access to services will be protected through NT/Windows Domain access-control methods. Administrative access will be limited to IT staff with direct responsibility for the server. Access should be logged.

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

- Remote access will only be allowed via FIHS provided VPN or dial-in service. Contractors who need access must be cleared for administrative accounts or must be monitored by administrative staff while accessing the server.
- Terminal Client access must be approved by ISSO or Chief of ITOS.
- The ISSO must respond to notices of necessary security patches within 48 hours or must inform the Chief of ITOS if application would interfere with business requirements.
- The ISSO will scan all servers with a vulnerability tool weekly and inform the Chief of ITOS of reported vulnerabilities and apply patches and fixes to all high priority vulnerabilities unless application would interfere with business requirements.
- Always use standard security principles of least required access to perform a function.
- Network administrative staff will perform all admin functions on servers with their private administrative account rather than the general administrative account.
- Before being put into production or after a major configuration change servers will be scanned by the ISSO with the institute's vulnerability scanner and with FIHS' self Sara Scan.
- Servers will be physically located in the LAN room and the LAN room will be closed and locked so that access is only via cipher lock.
- Servers are specifically prohibited from operating from uncontrolled cubicle areas.
- This policy applies to all installations of Windows/NT/XP servers, even those used for development and testing.

5.2.2 Monitoring

- All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:
    - All security related logs will be kept online for a minimum of 2 weeks and collected and maintained by a central logging program.
    - Daily incremental tape backups will be retained for at least 6 months.
    - Weekly full tape backups of logs will be retained for at least 6 months.
    - Monthly full backups will be retained for a minimum of 6 months.
- The ISSO and Network administrators will be trained in the use of tools installed to assist in monitoring the network for possible attack. It will be the responsibility of the ISSO and a backup to monitor logs of host-based intrusion systems or to respond to alerts.
- Security-related events will be reported immediately to the ISSO or Chief of ITOS. The ISSO will review logs and report incidents to the Chief of ITOS. Corrective measures will be prescribed as needed; breaches will be reported to the FIHS IRT following the FIHS incident reporting guidelines. Security-related events include, but are not limited to:

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

    - Port-scan attacks
    - Evidence of unauthorized access to privileged accounts
    - Anomalous occurrences that are not related to specific applications on the host.
- The ISSO will keep a detailed log of any security incidents in the incident log book.
- Corrective measures to be performed by network administrators must be performed within 48 hours. Problems will be brought to the attention of the ISSO immediately. Report of completion will be provided electronically to the ISSO.
- The ISSO will respond to FIHS IRT notices and Sara Scan reports indicating attacks or vulnerabilities with a report on corrective measures or false positives within 48 hours of notification. All responses will be carbon copied to the Chief of ITOS and the CIO.

5.2.3 Compliance

- Audits will be performed on a regular basis by the ISSO.
- Audits will be performed on newly installed servers and upon major configuration changes.
- Audits will be managed by the ISSO in accordance with the *Audit Policy*. The ISSO will present the findings to Chief of ITOS for remediation or justification.
- Every effort will be made to prevent audits from causing operational failures or disruptions.

6.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

7.0 Definitions

Term	Definition
DMZ	De-militarized Zone. A network segment external to the corporate production network.
Server	For purposes of this policy, a Server is defined as an internal IBCR Server. Desktop machines and Lab equipment are not relevant to the scope of this policy.

8.0 Revision History

This policy was revised on Oct 13, 2002 to fit the GIAC Institute of Basic Cellular Research.

9.0 Signature

This policy is approved for use by: CIO's signature Date:

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

Develop Security Procedures

The purpose of implementing the Server Security policy is to establish a base configuration for servers to protect them from unauthorized access. A good procedure often includes a step by step checklist that can be followed by responsible staff. There are numerous resources that provide configuration guidelines. For this policy to fit the needs of the IBCR various guidelines have been combined to create an installation procedure. Resources used to create procedures are ITC developed Windows 2k and Windows Server checklists, processes learned from SANS W2k Gold Standard Tour, and Microsoft TechNet's Windows 2000 Server Baseline Security Checklist (Microsoft).

Server Security Installation Procedure

Server Installation will be performed by IBCR network administration personal in the IBCR LAN room in response to an official request from the Chief of ITOS. Servers are not to be located in accessible office areas. The following information must be submitted in writing to the ITOS Chief with a copy provided to the ISSO before installation begins.

- Need for the server and the original request
- Hardware requirements
- Software requirements including OS/Version
- List of applications, main functions and any special needs/concerns
- Who will need access, at what level and reasons
- Any special considerations
- Is service considered to be critical
- Location of Backup service (Sans or Traditional)
- Name of Installer and backup contact
- Name of staff responsible for applications if not the same as above
- Server name, URL/domain name, IP address & LAN tap no.

Installation Check List (DRAFT)

(This process will be refined and reworked as security software arrives and is implemented. Instructions for processes such as setting up Tripwire, and installation of Net IQ's Security Manager would be linked to this procedure. The ISSO, for the time being, will perform security scans – so staff will have to coordinate installation efforts. At certain points in this procedure the author will insert notes to explain why some of these actions are important. These notes would not normally be included in this procedure.)

Installation should occur off network if possible. If not, then immediately after OS installation install all patches from the Microsoft Update site. Do not leave the machine unattended until after all patches have been installed. If there is a time lag between the time the operating system is installed and the time patches can be installed, remove the machine from the network for that period. Immediately after patches are updated perform a Self Sara Scan. Work with the ISSO to fix any vulnerabilities before continuing the install process. Until this is done, do not leave the machine on the network unattended.

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

Operating System Install

1. Run Compaq Smart Start (for Compaq Servers)
2. Install Windows 2000 Server from CD
3. Server name should reflect its main function and be approved by the ITOS Chief and follow the IBCR naming conventions
4. Set static IP address
5. Configure NIC 100 Full.
6. Use only NTFS file system
7. Do not install IIS unless approved
8. Rename the administrator account. Follow IBCR password conventions, use numbers and characters.
9. Create a dummy “Administrator” account, disable it and make it a member of the Guest group.
10. Enable network lockout of the Administrator account. Use PASSPROP.EXE from the Resource Kit.
11. Set Log files to 80mb and enable over write.
12. Set domain admin permissions on the security event logs.
13. Disable Guest Account.
14. Set Performance Options
    My Computer/Properties/Advanced Tab/Performance Options
    Set Foreground application performance boost to NONE
15. Set Recovery Options
    My Computer/Properties/Advanced Tab/Startup and Recovery
    Only write event to system log
    Automatically reboot
    Use Small Memory Dump
        Edit Boot.ini file so it displays process during boot-up.
        Add /sos to end of boot string in BOOT.INI file
        Do not change the line marked “default=”

```
[boot loader]
timeout=5
default=multi(0)disk(0)rdisk(0)partition(1)\WINNT
[operating systems]
multi(0)disk(0)rdisk(0)partition(2)\WINNT="Microsoft Windows 2000 Server" /fastdetect /sos
```

16. Enable Auditing

Event	Level of Auditing
Account logon events	Success, failure
Account management	Success, failure
Logon events	Success, failure
Object access	Failure
Policy change	Failure

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

Privilege use	Failure
System events	Success, failure

17. Replace the EVERYONE group on file ACL's with Authenticated Users.
18. Display log on banner

    ***** NOTICE *****

    This is a U.S. Government computer system, which may be accessed and used only for authorized Government business by authorized personnel. unauthorized access or use of this computer system may subject violators to criminal, civil, and/or administrative action.

    All information on this computer system may be intercepted, recorded, read, copied, and disclosed by and to authorized personnel for official purposes, including criminal investigations. Such information includes sensitive data encrypted to comply with confidentiality and privacy requirements. Access or use of this computer system by any person, whether authorized or unauthorized, constitutes consent to these terms. There is no right of privacy in this system.

19. Set Logon Screen Saver with a 5-minute time out for all accounts
20. Apply Windows Server Gold template (when available)
21. Remove the OS/2 and POSIX Subsystems
    Delete the **\winnt\system32\os2** directory and all of its subdirectories.
    Use the Registry Editor to remove the following registry entries:

Key: HKEY_LOCAL_MACHINE\SOFTWARE
Subkey: Microsoft\OS/2 Subsystem for NT
Entry: delete all subkeys

Key: HKEY_LOCAL_MACHINE\SYSTEM
Subkey: CurrentControlSet\Control\Session Manager\Environment
Entry: Os2LibPath
Value: delete entry

Key: HKEY_LOCAL_MACHINE\SYSTEM
Subkey: CurrentControlSet\Control\Session Manager\SubSystems
Entry: Optional
Values: delete entry

Key: HKEY_LOCAL_MACHINE\SYSTEM
Subkey: CurrentControlSet\Control\Session Manager\SubSystems
Entry: delete entries for OS2 and POSIX

22. Table of settings (see Table 2) – apply the following settings

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

Configuration Setting:	Recommended:
Configure the Account Policy In Local Security Policy under Administrative Tools.	8+ characters for passwords. Minimum password age: 1day Password history 24 Require complex password Enable account lockout to 4 hours after 5 failures and reset after 4 hours
Secure the Administrator and Guest Accounts	Rename accounts and assign 14 character complex passwords. Disable Guest.
Customize Security Options	
Additional Restrictions for Anonymous Connections	"No access without explicit anonymous permissions."
Allow System to be Shut Down Without Having to Log On	Disable
Audit Use of Backup and Restore Privilege.	Enable
Automatically Log Off Users When Logon Time Expires (Local)	Enable
Digitally Sign Client Communication (Always/When Possible)	Enable "When Possible."
Digitally Sign Server Communication (Always/When Possible)	Enable "When Possible."
Do Not Display Last User Name in Logon Screen	Enable
LAN Manager Authentication Level	At least 2
Message Text/Title for users attempting to Logon	Use FIHS standard warning banner – see step 17 above
Number of Previous Logons to Cache (if Domain Controller is Not Available)	10
Prevent System Maintenance of Computer Account Password	Disable
Prevent Users From Installing Print Drivers	Enable
Prompt User to Change Password Before Expiration	14 Days
Recovery Console: Allow Automatic Administrative Logon	Disable
Recovery Console: Allow Floppy Copy and Access to All Drives and Folders	Disable
Restrict the CD-ROM and Floppy Drive access to locally logged on user only	Enable
Secure the Netlogon Channel	"Digitally Sign…" and "Digitally Encrypt" when possible.
Send Unencrypted Credentials for Third Party SMB Servers	Disable
Configure Smart Card Removal Behavior	Lock Workstation
Strengthen Default Permissions of Global System Objects	Enable
Configure Unsigned Driver Installation Behavior	"Warn but allow installation"
Configure Unsigned Non-Driver Installation Behavior	"Warn but allow installation"

Table 2. Adapted from internal FIHS ITC Server Configuration Guidelines

23. Install all Service Packs and Updates from Microsoft.com

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

24. Scan with St. Bernard Update Expert
25. Run Microsoft Baseline Security Analyzer,[11] save the report.

Notes:

- Compaq Smart Start is used for server installation on Compaq servers. It allows for installation of Compaq Insight Manager, an SNMP server monitoring application.
- The Administrator account is by default not locked out after a set number of tries (set by security template). This allows a hacker freedom to use brute force until he gives up or guesses the password as he is never locked out. Set the admin account to lockout to prevent this.
- Renaming the Administrator account will prevent hackers from breaking in. Setting up a fake Administrator account, disabling it and placing it in the Guest group will prevent hackers from getting into the server and will also log the attempt.
- Log files are set to larger sizes to collect more information, overwrite ensures information is continually collected. Net IQ may change how this happens.
- The Guest Account is never used in IBCR, therefore its disabled.
- Performance options are set so that servers evenly distribute resources to all services as high availability of critical services is a high priority.
- Recovery options are set to minimize server down time as availability is important.
- The /sos tag in the BOOT.INI forces the boot-up process to display on the screen. This allows the administrator to view problems that occur doing boot-up. This may indicate impending problems or make troubleshooting easier.
- Replacing EVERYONE with Authenticated Users in file and dir ACLs requires anyone trying to connect to the server to be an authenticated user.
- A logon banner provides warning that the user is entering a US Government system. Servers need to have logon banners in case of log on via Terminal Services or local access from staff.
- Logon Screen Saver with a 5 minute time out ensures that the server will be locked after 5 minutes without input.
- When the institute moves to Active Directory and the Windows Server Gold template is released it will be customized and applied to all servers.
- The table is a list of suggested policy settings. Many of these will be covered by the CIS security templates when released.
- Update Expert will ensure all patches are installed. It will scan faster than STAT Analyzer and should ensure the server is protected well enough until the installation is completed.
- Microsoft's Baseline Security Analyzer is used as a quick vulnerability scanner to ensure that holes are patched before a server is allowed to run on the network for the remainder of the installation process.

[11] For information on Microsoft's Baseline Security Advisor see http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/Tools/MBSAhome.asp

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

Installation of Support Software

1. If not already place server on network.
2. Configure Additional Drive Partitions.
3. Install Compaq Smart Start
4. Install SNMP for Compaq Insight Manager.
5. Set Community string name as xxxxxxxx and remove public community name.
6. Install Terminal Services. Set for domain admin access only, unless written requirements direct otherwise.
7. Install Net IQ Security Manager client and set logs to be monitored from the Security Manager Console.
8. For critical servers install Tripwire, generate report (currently on order).
9. Install Ups client (Network Version).
10. Configure IT located Network Printer.
11. Install Virus Software, set to be monitored by E-Policy.

Notes:

- For servers the OS is installed on partition C, applications are installed on partition D.
- Terminal Services are used to allow administrators to access servers from their desktop rather than having to have access to the LAN room. Offsite contractors will need these services to perform their duties.
- Net IQ Security Manager will provide the ISSO with a central security console to assist in auditing and monitoring all servers.
- Tripwire is a host-based intrusion detection that monitors files for alterations.
- UPS client - interface for uninterruptible power supply. Provides backup and clean power for servers.
- Anti virus, MacAfee is monitored by its console product, E-Policy.

Security Scan and Audit

1. The ISSO will scan server with St. Bernard's Update Expert and patch as needed.
2. The ISSO will run the CIS scoring tool – mitigating any problems and save reports
3. The ISSO will run Microsoft Baseline Security Analyzer and save the report.
4. The ISSO will scan with port scanner; investigate non-standard ports and save as baseline.
5. The ISSO will scan with GFiLANguard and save report.
6. The ISSO will scan with Active Network Monitor and save report.
7. The ISSO will scan with Stat Analyzer to determine any remaining vulnerabilities.
8. The ISSO will mitigate any vulnerabilities with Hercules – report results and save electronic version of report.

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

9. The ISSO will run a Self Sara Scan and save the report.
10. ISSO will release server for production when cleared.
11. All reports will be filed in an electronic directory under the servers name to be used as the basis for future auditing. Access to this directory will be limited to security staff.

Note:

- The security and reporting tools will be used to mitigate any remaining vulnerabilities and to provide various audit and base lining reports.
- Over time the author expects that favorite tools will be selected and tools that duplicate functions will be dropped.
- The CIS scoring tool will be used once a gold template for Windows server has been released.

The author will refine this procedure over time. It has been a while since the author has been involved in a server installation. The author needs to test this procedure on a "live" process. The author plans to install the Windows 2000 server that will host STAT Analyzer's vulnerability scanner and Citadel's Hercules vulnerability mitigation tool. As mentioned in the procedure notes, once the Win 2k Gold Server Standard is released, it will be integrated into the installation process.

The last section of server installation is concerned with the ISSO performing vulnerability scans, patch management and baselining the server. This process captures a snapshot of the server's setup after its installation. These reports will be used to compare against future reports. For example, after the ISSO releases the server for production, application software will be installed to fulfill the main function of the server. After all the applications have been installed and the server is in its final configuration the ISSO will run the security and auditing scans again to look for changes and holes the software may have created. These vulnerabilities will be repaired and the reports will be studied to look for situations that may need to be documented for the installation of future software. Some of these tools will be used more often than others. The goal is to run the vulnerability scanner weekly and to repair any high to medium vulnerabilities within 48 hours. Tools like Update Expert will be used to install critical patches indicated by CERT or IRT notices and the port scanner will be used when new vulnerabilities have been identified, for example trojans that may be detected by a port scan. Microsoft's baseline analyzer will probably only be used for server installation or after a major configuration change. The CIS scoring tool will serve a similar function as the MS baseline analyzer; it will be used to baseline and audit new servers and after major configuration changes. LANguard and Active Network Monitor will be used to do much of the periodic auditing. Both of these tools generate reports about services, ports open, shares open, applications installed, hotfixes installed, password settings and more. Both allow reports to be saved and compared to indicate changes. With 40 servers it may be too ambitious to attempt auditing more than once a month.

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

Compliance with policy will be tested with the various automation tools that have been purchased. STAT Analyzer and Hercules check for vulnerabilities against policy. Reports can be used to provide a compliance report to management. Hercules can be used to attempt to fix these problems or appropriate staff can be tasked to bring them back into compliance. Tripwire monitors file changes, logs and alerts will be used to check for compliance. Net IQ's Security Manager's main job is to monitor for compliance and alert the ISSO of problems. This tool hopefully will be a real time compliance monitoring tool.

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

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

References

FIHS' Parent Agency (Name withheld.) Automated Information Systems Security Program Handbook. Internal document. (11 Oct 2002)

Hulme, George V. "Cyberattacks Reach All-time High." Sept 25, 2002. <http://www.informationweek.com/story/IWK20020925S0005>. (11 Oct 2002).

Mencimer, Stephanie. "Lone-Star Justice." Apr. 1, 2002. <http://www.indiantrust.com/clips.cfm?news_id=222>. (11 Oct 2002).

Microsoft. "Windows 2000 Server Baseline Security Checklist." < http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/w2ksvrcl.asp> (14 Oct 2002).

Naidu, Krishni. Firewall Checklist. <http://www.sans.org/SCORE/checklists/FirewallChecklist.doc> (11 Oct 2002).

Perez, Juan Carlos. "Biggest Security Threat? Insiders." Oct. 2, 2002. <http://www.pcworld.com/news/article/0,aid,105528,00.asp>. (11 Oct 2002).

Stoneburner, Gary, Goguen, Alice, and Feringa, Alexis. Special Publication 800-30: Risk Management Guide for Information Technology Systems. National Institute of Standards and Technology. Jan. 2002. 12. < http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>. (11 Oct 2002).

Tippett, Peter. "The Risk Equation." <http://www.trusecure.com/methodology/riskequation/> (11 Oct 2002).

Tillett, L. Scott. "Feds Get Failing Grades On Information Security." Nov. 9, 2001. <http://www.internetwk.com/story/INW20011109S0006>. (11 Oct 2002).

Verton, Dan. "Spy case demos insider threat." Feb. 26, 2001. http://www.computerworld.com/securitytopics/security/story/0,10801,58062,00.html >. (11 Oct 2002).

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

Footnote References

[1] Tripwire Server Product Website
URL: http://www.tripwire.com/products/servers/ (11 Oct 2002).

[2] Net IQ Security Management and Administration Solution
URL: http://www.netiq.com/solutions/security/default.asp (11 Oct 2002).

[3] St. Bernard's Update Expert Website
URL:
http://www.stbernard.com/products/updateexpert/products_updateexpert.asp. (11 Oct 2002).

[4] Harris Corporation's STAT Analyzer Website
URL: http://www.statonline.com/solutions/sec_policy/index.asp. (11 Oct 2002).

[5] Citadel Software's Hercules Website
URL: http://www.citadel.com/Hercules.asp. (11 Oct 2002).

[6] GFiLANguard Network Security Scanner Website
URL: http://www.gfi.com/lannetscan/index.htm. (11 Oct 2002).

[7] Active Network Monitor Website
URL: http://www.protect-me.com/anm/. (11 Oct 2002).

[8] Windows 2000 security benchmarks and CIS scoring tool Website
URL: http://www.cisecurity.org/. (11 Oct 2002).

[9] Net IQ's Security Manager Website
URL: http://www.netiq.com/products/sm/default.asp. (11 Oct 2002).

[10] GoToMyPC Website
URL: https://www.gotomypc.com/. (11 Oct 2002).

[11]Microsoft Baseline Security Advisor
URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/Tools/MBSAhome.asp. (14 Oct 2002).

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