Global Information Assurance Certification Paper

Information Security Planning

GIAC University

GIAC Information Security Officer (GISO)
Practical Assignment v1.2 (February 9, 2002)

Brooke Banks
March 3, 2003

Table of Contents

Abstract

The following practical describes GIAC University's (GU) current information security environment. After a review of the information technology infrastructure and business operations, the three top information security risks of the organization are presented. These risks are discussed in terms of their relevance to GU, potential for damage, likelihood of exploit and mitigation approach. A server security policy is evaluated, and a new server security policy is written for GU to address some of the risks identified. Finally a procedure for registering all campus servers is documented.

At a recent GU information technology planning meeting, security was rated as the number one issue in terms of importance over the next 18 months. Despite a strong feeling that security is critical, higher education institutions suffer from a culture which fosters experimentation and creativity. Institutional politics make it very difficult to implement policies that restrict use or dictate how decentralized information technology organizations should maintain their systems. A Gartner Research Note from January 18, 2002 emphasized that in the future it will be necessary for higher education to abandon the path of least resistance – laissez faire in the name of academic freedom – and encourage a climate where the need for safe and reliable networks requires users to surrender some information technology flexibility.[1]

GIAC University Overview

Description of GIAC University

GIAC University (GU) is a residential campus occupying a scenic 120 acres immediately adjacent to the downtown business district of the city of Smallville, population 50,000. The city of Smallville is located approximately 60 miles north of Metropolis. Throughout GU's 100 year history, the campus and the city of Smallville have had a symbiotic relationship. The campus brings considerable employment, economic and cultural activity to the city.

Even though GU is considered a residential campus, only about 15 percent of the students live in university housing. The remaining 85 percent become temporary residents of the city and a surprising number stay after graduation, adding well-educated settlers to the positive impact the campus has on the community.

GU has 14,500 full-time equivalent students, 16,200 total students. They come from 66 nations, 49 states and 2 U.S. territories. There are currently 590 tenured or tenure-track faculty, 400 temporary faculty and 325 staff.

The heart of GIAC University's strategic planning is the creation of a learning-centered environment. The strategic plan identifies as priorities the following: an innovative and high-quality student-centered campus; faculty and staff development; and enhancement of the academic program through state-of-the-art technology.

IT Infrastructure

GIAC University's Information Technology staff is working towards a sound Defense in Depth (DiD) strategy to protect the organization. DiD includes establishing layers of protection such that intruders must circumvent multiple defenses in order to gain access to critical institution networks and data.

A number of items from a typical DiD strategy are missing from GU's current IT infrastructure. Many of these missing items are planned for implementation in the near future; unfortunately, upcoming university budget cuts may have a significant negative impact on our ability to move forward on costly technical solutions. Fortunately, an effective security strategy requires changes in people, processes and technology. GU believes that changing staff, student, and faculty perceptions and information security processes may be more possible and more critical in the short term, even if technological change is slow.

Protecting the border of the GU infrastructure is the responsibility of the CISCO 12008 gigabit switch router (GSR), running CISCO IOS v12.0(12)s, which was selected based on its design for reliability and scalability. At this time the router is being used by GU to block incoming packets on a subset of ports.

The next layer in our defense strategy is a CISCO Catalyst 6509 switch, running CISCO IOS v12.1(13)e. This switch includes a turnkey solution for firewall services which is being used to protect certain sensitive internal networks from attacks from within the infrastructure. No firewall services are currently deployed at the border.

The GU network includes an extensive implementation of Virtual LANs (VLANs). These VLANs allow GU to logically group users and corresponding network resources. They also provide a mechanism for managing broadcasts on the network.

A CISCO VPN 3000 Series Concentrator has also been deployed for remote access encryption and authentication. At this time, the Virtual Private Network (VPN) technology is being used to provide remote access to windows networking and access to our test wireless (802.11b) network.

Deployment of a border firewall and DMZ is in the plans for GU over the next 12 months; therefore, two network infrastructure diagrams are included in this paper. The first, found in Appendix A, is a look at the current state; the second, Appendix B, represents the future plan.

Business Operations

GIAC University is administered by three organizations; Academic Affairs, Student Affairs, and Business and Finance. Although these organizations work closely together to serve the students of the university, each organization is responsible for a specific set of functions.

Academic Affairs: The largest of the three organizations, Academic Affairs includes all the colleges, schools and centers, Undergraduate Education, the Graduate Program, Regional and Continuing Education, the Library, and Information Technology.

Student Affairs: This organization includes Enrollment Management, Financial Aid, Career Planning, University Housing, Student Health Center, Athletics, and Alumni Relations.

Business and Finance: This organization includes Human Resources, Financial Services and Facilities Management.

The Student Administration System (SAS) is the primary administrative system used by GU. It is used to develop the course schedule each semester and track student information (e.g., transcripts, grades, addresses, etc.). All teaching departments utilize SAS to assign faculty to courses, generate rosters and input grades. The Student Administration System feeds student data to many other applications. Its three primary direct connections are to the GU Portal, a student online database used for reporting, and the voice response system used for registration.

SAS sends and receives student information by batch to/from the following systems:

- Health Center System – Maintains student health information. Operated by the Student Health Center.
- One Card – Allows students, faculty and staff to utilize their ID card to purchase items at a number of campus locations (e.g., bookstore, food services, print center, etc.). Operated by Financial Services.
- CashApp – Used for fee payment. Operated by Financial Services.
- SA – Processes student admissions information, mails acceptance letters and tracks students until they register. Operated by Enrollment Management.
- PS – Provides information to and gathers information from prospective students. Operated by Enrollment Management.
- FARMS – Financial aid system, integrated with other federal and state applications. Operated by Financial Aid.
- Alumni – Tracks alumni and donations. Operated by the Alumni Office.
- Library – Includes library catalog, online books and periodicals system. Operated by the Library Systems Office.

SAS can be accessed both on campus and remotely and is running IBM OS/390. Currently none of this communication is encrypted.

Information Technology and Enrollment Management are partnering to implement PeopleSoft Student Administration as a replacement for SAS, although this implementation will take an additional 3 years.

Human Resources personnel utilize PeopleSoft HR v8.0, where the Financial Services office utilizes PeopleSoft Financials v7.6. Both run Solaris/Oracle. The system is housed at an off-campus data center. An on site data warehouse is available for both systems, again running Solaris/Oracle. This communication is encrypted.

All GIAC University faculty and staff have workstations on the staff user network; a separate network exists for the students. Users are provided access to the Internet, the GU portal/online courses and electronic mail. They are also provided remote access via the modem pool.

Student network access is managed by our GIAC directory (an LDAP directory). Students are provided a university electronic mail address on the SunOne Messaging Server platform, as well as access to the GU Portal. The portal is used to review campus announcements, class lists, grades and other student information. The portal is also the window into our course management system where students can view online class information, e-mail, chat with classmates and take quizzes and exams online. They are able to access this portal from the university home page, either from their home computer or in a student computer lab. A streaming media product is used to provide university courses to students in remote locations.

Staff and faculty authentication information is also stored in the GIAC directory, which provides them access to the GU Portal. They are also stored in the Microsoft Active Directory (an LDAP-enabled directory), which provides them access to Microsoft services (e.g., e mail, file/print services, etc.). Their primary tools are Microsoft Office and Microsoft Outlook. The Microsoft environment is currently W2K.

Information Technology is responsible for the enterprise wired and wireless network, Web site, print/file servers, telephone, e-mail and voice mail systems. They run a number of student open-access and academic computer labs and provide help desk support to students, faculty and staff. The IT staff also administers the Student Administration System (SAS), GU Portal, and course management system from the main data center. Many of the other smaller applications utilized by the university are administered by decentralized Information Technology staff.

Risk Analysis

Compromise of Confidential Data

Overview of Threat or Risk

GIAC University's greatest risk is the compromise of confidential data, its 'crown jewels.' We define data compromise as loss, modification or destruction of data.

Due to the need to safeguard the privacy of individuals, efforts must be made to prevent the inadvertent release of information that would constitute an unwarranted invasion of personal privacy.

Relevance to GIAC University

GU is responsible for maintenance, security and integrity of student academic records and manages student record information in accordance with the Family Rights and Privacy Act of 1974 (also known as FERPA). FERPA is unambiguous in asserting that the academic and personal information in a student's record may not be released to anyone without the written consent of the student or without legitimate educational interest.[2]

GU is also responsible for protecting employee data. Although a subset of employee information is a matter of public record and may be disclosed, a much larger set of employee data is identified as personal or confidential and is not subject to mandatory public disclosure.

In late 2002, the state governor passed a bill which requires a state agency (such as GU) that maintains computerized data including personal information to disclose any breach of the security of that data to any resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. This bill gives people notice that unauthorized individuals have acquired their personal and/or financial information, thereby giving them the opportunity to take proactive steps to ensure that they do not become victims of identity theft.

This bill has now become a part of the state Civil Code.[3] The requirement to disclose security breaches goes into effect on July 1, 2003. At this time, GU does not have a procedure in place to handle these disclosures.

Potential for Damage

The Civil Code is clear in stating that organizations who fail to disclose that a breach has occurred can be liable for civil damages and/or face class actions. These

actions could result in both monetary penalties for GU and damage to our reputation as a quality academic institution.

Eighteen hundred computer security experts and managers who met at the SANS99 and Federal Computer Security Conferences developed a list of the 7 Top Management Errors that lead to computer security vulnerabilities. Number five in the list is "*Fail to realize how much money information and organizational reputations are worth."* [4]

Likelihood of Exploit

In mid 2002, two former students at a nearby university were arrested and charged with computer equipment theft. Further investigation showed that the students were also in possession of all student, faculty and staff photos, names, birth dates and social security numbers. Although it was not clear that the information was used for malicious purposes, it was clear from this incident that the correct technologies, policies and procedures were not in place to protect campus confidential information. It was also clear that this type of incident could easily happen to GU, if steps are not taken to mitigate the risk.

Mitigation Approach

Border Firewall

To begin, we need to deploy the CISCO PIX FWS module firewall currently provided with our CISCO Catalyst 6509 switch.

This firewall's primary purpose is to provide a first line of defense against threats originating from the Internet. The firewall is logically positioned at the edge of the campus network, between the GU campus and the Internet. Traffic coming into the campus is blocked, except for traffic destined to known Internet-accessible servers (i.e. campus Web server, mail relays) and traffic resulting from a campus request – such as a response to a user's request for a Web page. All outbound traffic is permitted.

There are a number of risks associated with the deployment of this firewall. Some of the risks to consider are as follows:

- *Service interruptions* - New and unknown campus services will not function for Internet clients until provisions are made in the firewall
- *Service limitations* - New and emerging network protocols may not be supported by the firewall (e.g. h.323 videoconferencing, etc.)
- *Local Attacks* - The border firewall protects the campus against attacks from the Internet, not from attacks originating on campus
- *Session Hijack* - A compromised campus server could be used as an avenue to attack other machines behind the firewall

- *Complacency* - Users and technical staff, believing themselves protected, forego system patches, hardening, and other best-practices. These machines are then more vulnerable to local attacks

GU recognizes that some faculty and staff may need to perform functions which require specific firewall rules so they can serve to machines outside the GU network. The firewall will therefore be deployed using a three-tiered structure:

Fully Firewalled
- Machines cannot serve to Internet
- Most user and remote access networks would fall in this model
- Depending on policy, users could potentially access machines on these networks via VPN connections, enabling remote desktop access

Fully Open
- Machines are completely open to Internet
- Most machines needing to serve may fall in this category at first
- These machines are considered 'untrusted' by the campus – as if they were out on the Internet

Managed Firewall Networks
- Firewall rules are tuned to only allow known services, minimizing exposure (i.e. only mail gets through to a mail server, not Web)
- Firewall rules for these networks may also protect against attacks from on-campus
- Substantial support costs (both initial implementation, as well as on-going)
- Ideal choice for critical or enterprise servers and services
- 'Fully Open' machines should eventually migrate to this model, as staff and time are available for analysis and implementation

GU acknowledges that this implementation strategy is not the most secure; however it is a good first step.

Virtual Private Network

Because this border firewall does not protect connections via our dial-up modem pool, we will require faculty and staff who access the GU network remotely to utilize the VPN functionality provided with the switch. When these remote users attempt to log-in to the network remotely without the VPN they will be prompted to download the VPN client. Once they've downloaded the VPN client they will be free to access network services remotely upon providing their GIAC directory log-in credentials.

Encryption

GU will continue to operate with its legacy Student Administration System (SAS) for some time. At this time the SAS mainframe sends confidential faculty, staff and student data over unencrypted communication channels each day. Although there are some concerns regarding the system's ability to utilize newer, more secure technologies, an analysis should be conducted to determine whether we can improve the security of this confidential information. At this point one of the potential changes would be to replace FTP and TELNET client software with Secure FTP and SSH client software.

Network/System Disruptions

Overview of Threat or Risk

Another significant risk for GU is network and system disruptions. Denial of service (DOS) attacks and unstable or insecure systems caused by non work-related software, non-current system patches and/or viruses have a significant impact on the productivity of university staff, faculty and students.

A number of the mitigation approaches discussed above, related to the protection of confidential information, will have a positive impact on our ability to manage network and system disruptions. Others are discussed below.

Relevance to GIAC University

Even though we are a public university, and are therefore not selling our services, network and system downtime is still a significant issue. It is disruptive to our user community and therefore the quality of our learning environment. At this time, 80% of all GU students use our online course management system in their classes. Because a significant percentage of faculty and students rely on this system for learning, its downtime has severe consequences. Faculty and students are unable to view course materials, complete online assignments and take quizzes and tests.

Potential for Damage

Network and system disruption causes Information Technology to lose good will with the university and community. Many faculty, staff, and students do not understand the technical environment and therefore have a difficult time not associating the downtime with Information Technology inadequacy. This perception on the part of the user community can even have a negative impact on the budget provided to Information Technology by GU administration. Not only can our reputation be damaged, but the work to bring networks and systems back online following a disruption is very costly and difficult with our short-handed staff.

Likelihood of Exploit

On Saturday, January 25, 2003, GIAC University was affected by a denial-of-service (DOS) attack that resulted in a complete loss of Internet connectivity. The attack was noticed on the GU campus shortly after 10PM, when a number of hosts on campus began flooding the outbound network connection with traffic -- to the tune of >450Mbps trying to head down a 150Mbps pipe. Shortly before midnight, technical staff had identified and disabled all local machines involved in this attack, restoring GU's connectivity to the Internet.

It didn't take long for GU to learn that the Microsoft SQL Slammer Worm had been responsible for the attack. In all, 18 campus servers were infected with the Worm which brought our network down for a number of hours. The worm used an exploit that had a patch released 129 days prior.

Mitigation Approach

Improved Desktop System Practices

At this time many faculty, staff and student desktop computers do not have consistent logging, auditing and backup procedures, they are not fully patched, are missing service packs, have no personal firewalls and have many unused services left enabled.

To mitigate some of these risks GU will:

- Implement a domain policy enforcing logging and auditing
- Implement a domain policy that will disable extra services
- Deploy a centralized storage location for critical user data with enough space and backup capacity to accommodate user needs
- Research and develop a patch deployment method
- Deploy personal firewalls

Improved Server System Practices

Like desktops, many GU servers are left unprotected. The development of a Server Security Policy will help Information Technology work with decentralized technical staff to ensure better server security practices.

Virus, Trojan and Worm Protection

GU's faculty and staff e-mail system is protected by virus software; however, the student e-mail system is left unprotected. GU also has no central mechanism for updating virus software or auditing that current versions of anti-virus software are installed. GU will implement Norton Antivirus Corporate Edition to ensure central management of virus, Trojan and worm protection software across the entire network.

Damaging or Illegal Actions by Staff, Faculty, and Students

Overview of Threat or Risk

The risk of damaging or illegal actions by staff, faculty and students is significant for GU. The users of our network vary greatly in their technical abilities and security awareness. They have easy access to our vast resources and because of the academic freedom inherent in our environment, would not think twice about taking an action which creates a significant hole in our security strategy. Often these actions are innocent and unintended, while other times they are not.

Relevance to GIAC University

An article by Todd Lawson in SC Online Magazine from January 2002 describes the 80/20 dilemma. If only 20 percent of damage done is perpetrated from outside the organization, the remaining 80 percent is elusive and perpetrated from within. [5] GU is not exempt from this dilemma.

Potential for Damage

Damaging and illegal actions perpetrated from within can cost GU significant amounts of money. The implementation of technical solutions and the IT staff time to fix problems are one set of costs. However, if these actions result in the public obtaining personal information regarding our constituents, GU faces legal action and therefore additional monetary loss. University good will and reputation is also at stake.

Likelihood of Exploit

Both of the GU security incidents discussed earlier in this paper were a direct result of internal user actions. A former student and staff member knowingly stole computer equipment and personal information. Overworked or under-trained server administrators contributed to the pain of the Slammer Worm. A recent random scan of machines on the network found an average of 11 missing patches and 1.5 missing service packs.

It's clear that to overcome this 80 percent will require more than a border firewall and virus protection. Good proactive security policies and practices are needed at GU. Without these policies and practices, intentional and non-intentional damage is likely to occur.

Mitigation Approach

Policy

GIAC University published an Acceptable Use Policy in 1997 and has made small changes to the policy each year since the initial approval to keep it up to date. At this time, however, no additional security policies are in place. This leaves the university without a sense of what information security means and how we all play a part in ensuring security.

The GU security policies need to define responsibilities and accountabilities associated with security and consequences for not protecting the elements of the network for which you are responsible.

A Gartner Research Note from December 31, 2001, highlights the tension in higher education between user freedom and systems integrity. In order to comply with stricter security policies, users will be required to give up some of their individual freedoms (to set up their machines in any way they want) if they want to be connected as "good citizens" within the institutional network and wider Internet community. [6] This represents a significant cultural shift for GU, making development and approval of security policy a non-trivial undertaking.

Security Awareness and Education

There are three different audiences for GU's Security Awareness and Education program: end users, the technical staff within the central IT organization, and technical staff outside the central IT organization.

End Users - There are two opportunities to improve end-user security awareness. The first is to develop and execute an Information Security Communication Plan to include items in IT publications as well as posters, Web pages and targeted presentations. This communication plan will be executed over a longer period of time, perhaps 12 months, in hopes that we can slowly change campus culture. With all the perceived freedoms associated with a university campus, it's not easy to mandate practices around computer use.

Some of the initial and critical communications will be to university leaders in Academic Affairs, Student Affairs, and Business and Finance, as well as the University Cabinet which includes the President and his top advisors. It will be critical that we gain support from upper management prior to proceeding with our information security plans.

The second is to modify our existing 'introduction to computer use for new staff and faculty' course to include the following topics.

- Password handling (not to share, use simple, or publicly display).
- Computers are university property, not personal property. And as such, users must refrain from installing non-work related software on university-owned systems.
- Installation of OS patches (manual or automatic installation).
- Use and upkeep of virus protection software, including uploading current virus definitions, scanning system files, and identifying hoaxes.
- Handling of sensitive data (locking computers instead of leaving data on screens and securing printouts).
- Risks of laptops being stolen (use laptop locks, BIOS passwords, and encrypted data).
- Offsite communications (use of VPN clients and encrypting data).

IT Technical Staff - At this time, a group of technical staff within the central IT organization, the Electronic Security Team (EST), is primarily responsible for overall campus information security. They tend to be very aware of the information security issues faced by GU and stay abreast of how to resolve these issues. The remainder of the IT technical staff has varying levels of information security expertise. Both groups will continue to require training going forward, especially on the new technologies we plan to deploy which assist them in protecting the network (e.g., border firewall, centrally managed virus protection system, etc.).

Decentralized IT Technical Staff - The technical staff outside the IT organization have vastly different levels of technical expertise. In some cases they are very knowledgeable in ways to protect their systems and servers; in other cases they are student assistants with very little technical ability. Part of the Information Security Communication Plan discussed above will include communication and training opportunities for decentralized IT technical staff.

Security Policy Evaluation

Although GU published an Acceptable Use Policy in 1997, there is no additional computing or security policy in place. The Information Technology organization has a good deal of work ahead to develop a set of policies and believes that at this time the university's most urgent needs are for a network security policy, data confidentiality policy and server security policy.

Although the cumulative affect of having these policies will be improved overall security, some of the policies also have a positive effect on reducing the risks outlined in this paper. For example, the network security and data confidentiality policies will assist the organization in moving forward to mitigate the first risk discussed; compromise of confidential information. The server security policy should assist in mitigating the second two risks, network/system disruptions and damaging or illegal actions by staff, faculty and students.

At this time, the university is still feeling the pain of the SQL Slammer Worm. Many of our campus servers are run by decentralized IT staff and unfortunately, for a variety of reasons, they are not all as secure as the IT organization would mandate. Since 18 of these servers were affected by the SQL Slammer Worm, it's clear that many are not even up to date with current patches. When the worm hit campus, the central IT staff spent many hours restoring the campus network and assisting system administrators to address the problem on individual servers. The IT organization would like to see a server security policy adopted so university faculty, staff and students, especially system administrators of these decentralized servers, are aware of the minimum security measures required by IT. They are also interested in a method to charge back organizations for the time associated with fixing server issues which could have been mitigated by following policy.

Based on the pressing need described above for a server security policy, in this paper I will analyze an existing server policy and develop a policy to suit the needs of GU.

Evaluate Server Security Policy

The Server Security Policy provided by the SANS Security Policy Project at the following link http://www.sans.org/resources/policies/, appears to address most of the concerns of GIAC University.[7] In addition, GU has some policy guidelines that will be followed in developing the new policy. The following evaluation addresses areas of the sample Server Security Policy which need to be changed and items which need to be added to meet the needs of GU.

Purpose: The purpose section of the sample policy clearly states that the policy's effective implementation will minimize unauthorized access to proprietary information and technology.

Background: No background section is included in the SANS sample policy, nor will one be added to the GU policy.

Scope: The scope section of the sample policy will be expanded to state that the policy includes servers operated by any faculty, staff or student. It also includes language regarding faculty, staff and student owned equipment. The second paragraph in the sample policy scope will be removed since GU does not currently have a DMZ.

Policy Statement: The policy section of the sample includes information regarding ownership, configuration, monitoring, compliance, and enforcement which will be changed only slightly to meet the needs of GU.

In the ownership section the policy will state that servers must be registered with Information Technology. Further procedures will be documented which include naming the groups involved in the registration process. Additional information regarding the servers will be required by the policy (i.e., physical location, MAC address, IP address, port and domain.)

The general configuration section has been renamed to include (server) administration. In addition, many of the 'should' statements have been changed to 'must' statements to make the policy stronger. Since many of GU's current servers are not located behind a firewall, a bullet has been added to address firewalls. The bullet regarding uncontrolled cubical areas has been removed because, for the most part, GU does not have cubicles and because the previous bullet covers the same principle.

The monitoring section has been reorganized for clarity so that security related events are defined first. The schedule for backups has been provided as a suggestion and 'tape' has been removed since this is just one media for backup.

The compliance section has been changed only slightly. The policy now states that audits can happen both regularly and on an ad hoc basis.

The enforcement section of the sample has been changed to meet GU policy guidelines and is now called sanctions and disciplinary actions. This section has been changed to make it clear that violators will face disciplinary action based on existing university procedures. It also states that servers not compliant with this policy can be removed from the GU network.

Responsibility: The sample policy does a nice job of stating that the operations group has some responsibilities and the InfoSec group has others. In the case of GU, we've changed InfoSec to Information Technology since at this time an Information Security office does not exist. Procedures which support this policy will provide more detail regarding who in Information Technology will be responsible for compliance.

Action: The bullets under configuration, monitoring and compliance are very clear regarding what is to be done to support this policy.

General:

To conform to GU policy guidelines, the following changes have also been made:

- The definitions section has been moved to the beginning.
- The scope section has been moved to follow the definitions.
- GIAC University policy comes out as an executive memorandum from the university president. The policy is dated at that time and although revisions occur, a revision history is not kept in the document.

Revised Server Security Policy

SERVER SECURITY POLICY

GIAC UNIVERSITY

DEFINITIONS

Server – For purposes of this policy, a server is defined as any electronic device administered by any faculty, staff or student on the internal GIAC University network that is configured with the intent to provide information or services to any other device either internal or external to the GIAC University network. Examples of information and services include, but are not limited to, Web services, file transfers, e-mail services, and database services.

SCOPE

This policy applies to all servers connected to the GIAC University network for personal, departmental, and central university wide use and to servers registered under any GIAC University owned internal network domain. This policy does not apply to servers that are the property of faculty, staff, and students except that the use of servers linked to university facilities (e.g., a personally-owned server linked to the campus network) will be subject to applicable provisions.

PURPOSE

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

POLICY

Ownership and Responsibilities

All internal servers deployed at GIAC University 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 Information Technology. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish processes for changing the configuration guides, maintaining the server and ensuring data protection which includes review and approval by Information Technology.

- Servers must be registered with Information Technology. At a minimum, the following information is required to positively identify the point of contact:
  - Contact(s) name and location, and a backup contact
  - Server physical location, MAC address, IP address, port and domain.
  - Hardware and Operating System/Version

    - Main functions and applications, if applicable
- The operational group must notify Information Technology of any changes to the above.
- Configuration changes for production servers must follow the appropriate change management procedures.

General Configuration & Administration Guidelines

- Operating System configuration must be in accordance with approved Information Technology guidelines.
- Services and applications that will not be used must be disabled where practical.
- Access to services must be logged and/or protected through acceptable access-control methods.
- The most recent security patches must be installed on the system as soon as practical.
- 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 or an administrative privileged account 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 must be configured on switched network ports if available.
- Servers should not be used as workstations except by the administrator for purposes of server administration or in exceptional situations.
- Servers should not be located outside a firewall.
- Servers should be physically located in an access-controlled environment.

Monitoring

- Security-related events include, but are not limited to:
    - Port-scan attacks.
    - Evidence of unauthorized access.
    - Anomalous occurrences that are not related to specific applications on the host.
- Security-related events will be reported to Information Technology, who will review logs and report incidents to IT management and the campus Information Security Officer. Corrective measures will be prescribed as needed.
- All security-related events on servers must be logged and audit trails saved. Suggested schedule would include:
    - All security-related logs will be kept online for a minimum of 1 week and must be reviewed by system administrators.
    - Daily incremental backups will be retained for at least 1 month.
    - Weekly full backups of logs will be retained for at least 1 month.
    - Monthly full backups will be retained for a minimum of 2 years.

Compliance

- Information Technology reserves the right to perform audits on a regular and ad hoc basis.
- Results of the audit will be presented to the appropriate support staff for remediation or justification.
- Every effort will be made to prevent audits from causing operational failures or disruptions.

Sanctions and Disciplinary Actions

University faculty, staff, and students who violate any of the above policy may be subject to disciplinary action following established university channels for disciplinary matters.

Machines found not to be compliant with this policy may be removed from the GIAC University network.

Server Registration Procedure

The following procedure is intended to support the GIAC University Server Security Policy. The procedure should be followed by any faculty, staff, or student who wishes to connect a server to the GU network.

SERVER REGISTRATION PROCEDURE

GIAC UNIVERSITY

DEFINITIONS

Server – For purposes of this procedure, a server is defined as any electronic device administered by any faculty, staff or student on the internal GIAC University network that is configured with the intent to provide information or services to any other device either internal or external to the GIAC University network. Examples of information and services include, but are not limited to, Web services, file transfers, e-mail services, and database services.

PURPOSE

The purpose of this procedure is to document and communicate the steps necessary for a GIAC University operating group to obtain authorization from Information Technology to connect a server to the GU network. It is intended to ensure base configuration standards of all internal server equipment are met.

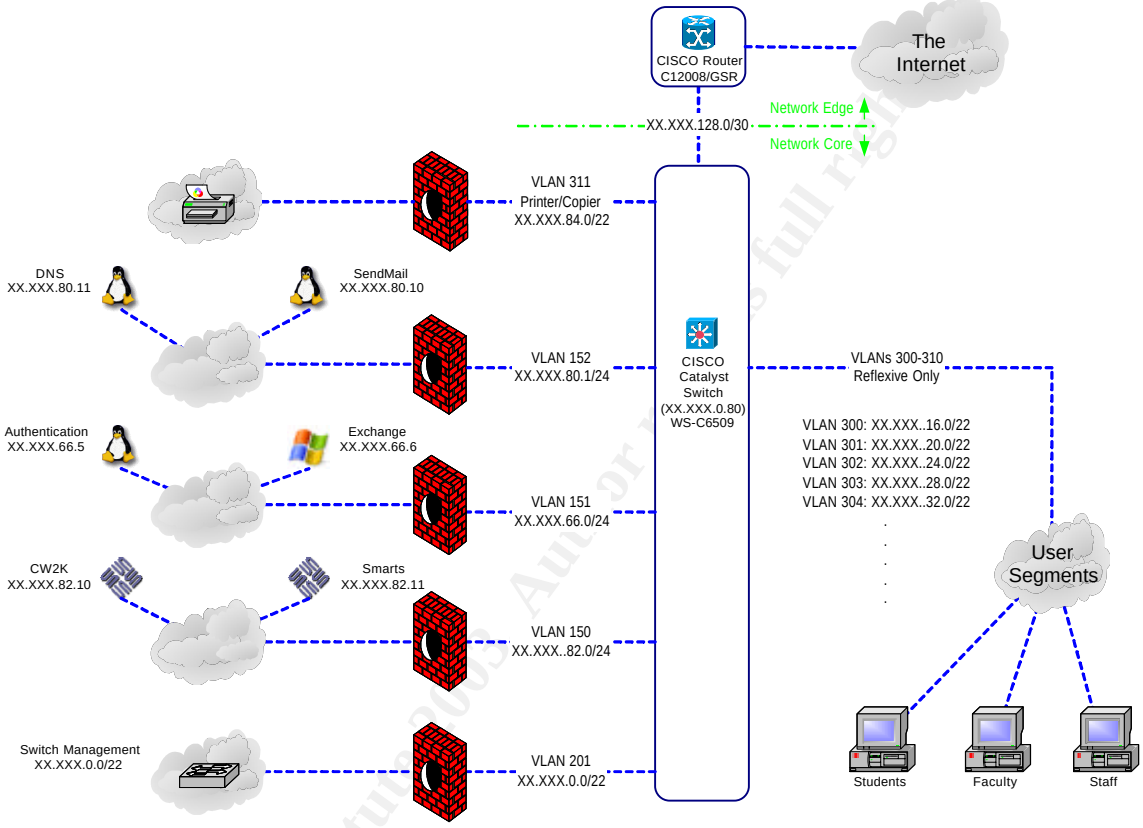
PROCEDURE

1. The operating group compiles the following information required by policy:
    - Dean or department head name and location
    - Server administrator contact name, location and desk, wireless and home/emergency phone numbers
    - Backup contact name, location and desk, wireless and home/emergency phone numbers
    - Server physical location
    - Server MAC address, IP address, port and domain
    - Hardware and operating system/version
    - Main functions and applications
    - Configuration guides
    - Maintenance processes
    - Data protection strategy
2. The operating group provides the above information to GIAC Information Technology at the following URL: www.gu.it.edu.
3. IT Network Operations reviews the information provided within 10 business days. This review may also include a tour of the server facilities to verify appropriateness.

4. If the operating group's server appears to be in compliance with the GU Server Security Policy, a copy of the policy and IT Charge Back Procedure is provided to the dean/department head by IT Network Operations. This charge back information is provided to ensure the dean/department head is aware they will be charged for GU IT server administrator assistance.
5. The dean/department head acknowledges either via e-mail or signature that both policies are understood.
6. The operating group is free to select its server hardware and software. Information Technology can provide assistance in selecting, obtaining and installing compatible server hardware and software; however the IT Charge Back Procedure will apply.
7. The operating group agrees to keep the server operational 24x7. Any malfunctions or maintenance tasks that disable the server for an extended period of time must be brought to the attention of the IT Network Operations group immediately.
8. As stated in the Server Security Policy, Information Technology reserves the right to conduct periodic and ad hoc audits of network servers. See the IT Server Audit Procedures for more information.
9. The IT Network Operations team can remove the server from the GU network if the server falls out of compliance with policy. Five days notice will be provided.

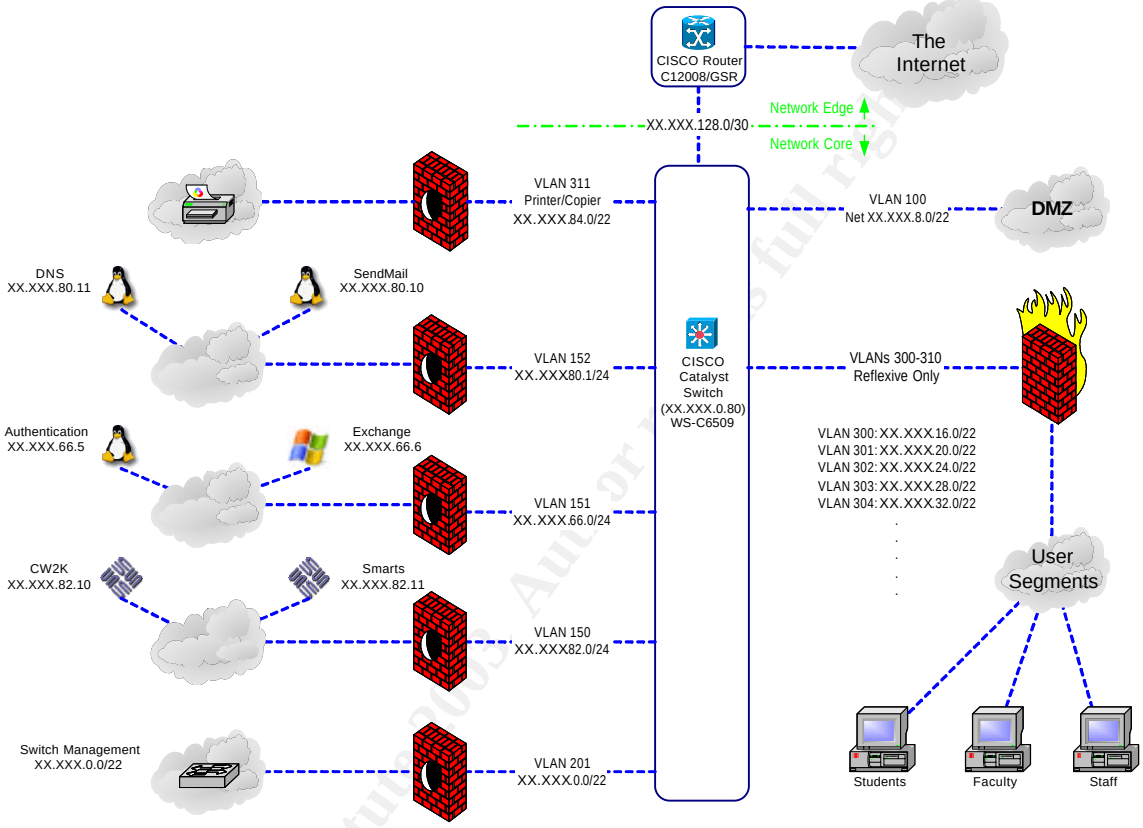
Appendix A – Current GIAC University Network Infrastructure

GIAC University- Current Network Infrastructure Diagram



Appendix B – Planned GIAC University Network Infrastructure

GIAC University- Planned Network Infrastructure Diagram



Appendix C – Sample Policy

SANS Security Policy Project

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.
- 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-militariezed 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

References

[1] M. Zastrocky, R. Yanosky, *Building a Responsible Campus Cyberculture in 2002*, Gartner Research Note, January 18, 2002.

[2] Family Educational Rights and Privacy Act (FERPA) **http://www.ed.gov/offices/OM/fpco/ferpa/index.html** (February 2003)

[3] State Civil Code
DIVISION 3. OBLIGATIONS, PART 4. OBLIGATIONS ARISING FROM PARTICULAR TRANSACTIONS, TITLE 1.8. PERSONAL DATA, CHAPTER 1. INFORMATION PRACTICES ACT OF 1977, Article 7. Accounting of Disclosures - **1798.25-1798.29** - **http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.25-1798.29** (February 2003)

[4] SANS Seven Top Management Errors that Lead to Computer Security Vulnerabilities **http://www.sans.org/resources/errors.php** (February 2003)

[5] T. Lawson, The *Most Commonly Overlooked Security Holes*, SC Online Magazine, January 2002. **http://www.scmagazine.com/scmagazine/sc-online/2002/article/03/article.html** (March 2003)

[6] M. Zastrocky, S. Bittinger, R. Yanosky, *Improving Higher Education IT Security in 2002*, Gartner Research Note, December 31, 2001.

[7] The SANS Security Policy Project **http://www.sans.org/resources/policies/**