Global Information Assurance Certification Paper

GIAC University

(An Information Security Overview)

GIAC GISF Certification Version 1.0
May 6, 2004
James Williams
Network Security 2003
New Orleans, LA – November 2003
Track 9: Information Security Fundamentals

Abstract

The purpose of this document is to examine the issues involved with creating a secure environment in higher education. GIAC University is a fictional University based in Texas. This paper will attempt to cover all topics required for the GIAC GISF+ Practical.

Section 1: Description of GIAC University

GIAC University is a small university located in the heart of the Texas Panhandle. As a school of higher education, GIAC University has a few different resources for generating revenue. GIAC University's two main resources of revenue come in the form of the annual budgets provided by the state of Texas and from revenue generated by student enrollment. GIAC University does generate other forms of revenue as well. This revenue is received in the form of grants and donations to the university. GIAC University has an annual average income of $95 million.

The University consists of 31 buildings, on the campus grounds, that are connected to the campus local area network (LAN). Six of the buildings are residence halls and one building is an on campus apartment complex for married students, staff, and faculty. GIAC University supports two remote offices, which are in a different city, with commodity Internet connections, and VPN access to the campus network.

The Division of Information Technology at GIAC University plays a crucial role in the universities ability to generate income. The IT department supports and maintains the infrastructure for staff, faculty, and students to be able to do their work effectively. This infrastructure includes everything from mainframes to desktop computers.

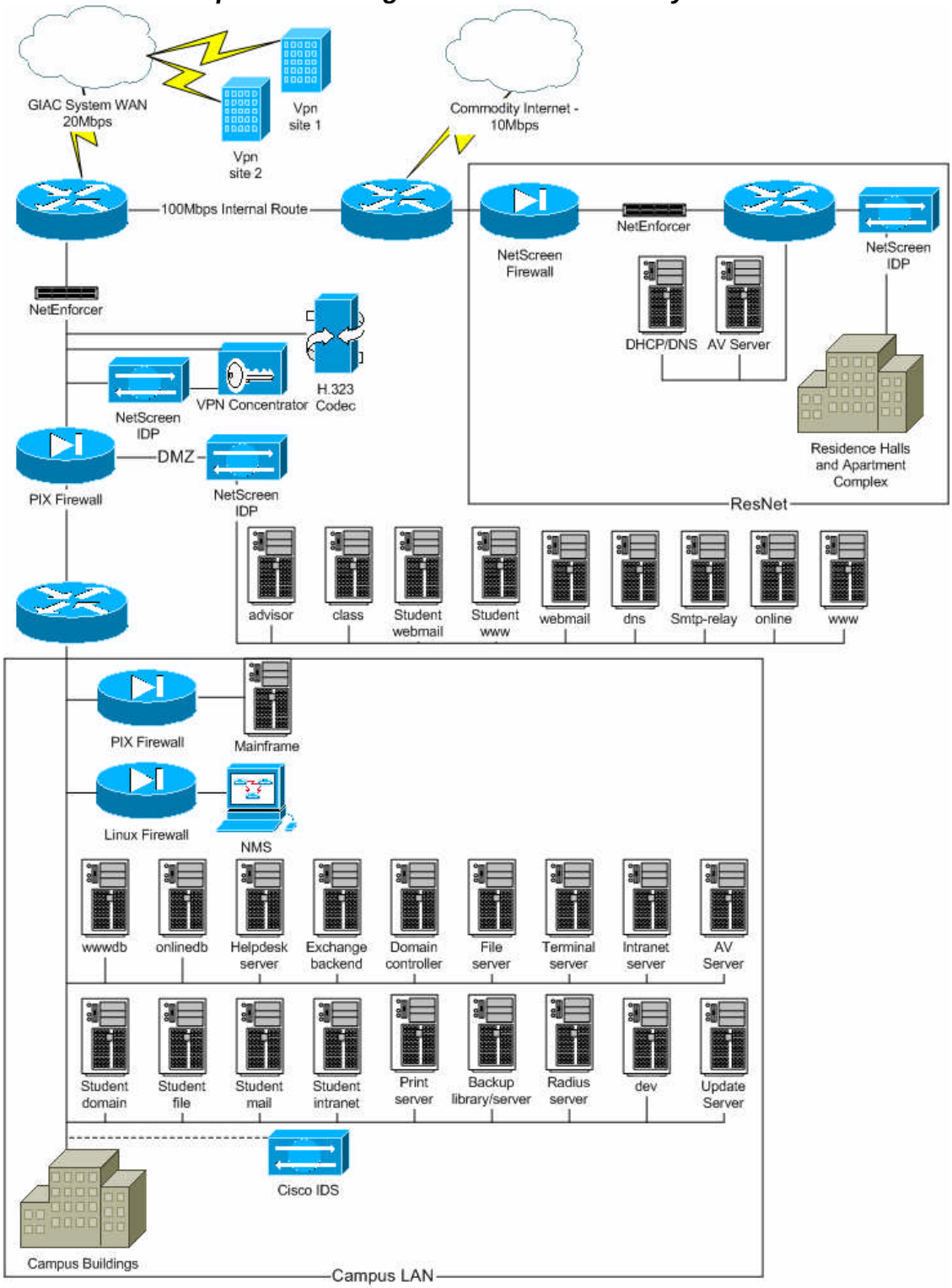
GIAC University has 34 full time employees and 28 student employees in the Division of Information Technology. In total the salaries for the IT department adds up to $1.6 million per year.

The Division of Information Technology positions and base salaries are listed below:

1. CIO - $140,000
2. SECRETARY x 2 - $40,000
3. DIRECTOR OF SYSTEMS SUPPORT & SECURITY OFFICER - $60,000
    a. HELPDESK MANAGER - $40,000
    b. PC SUPPORT MANAGER - $45,000
        i. PC SUPPORT TECH - $30,000
    c. NETWORK & TELECOMMUNICATIONS MANAGER - $50,000
        i. NETWORK & SECURITY TECH - $35,000

    ii. SYSTEMS ANALYST - $35,000
    iii. TELECOMMUNICATIONS TECH x 2 - $70,000
    iv. TELECOMMUNICATIONS BILLING TECH - $30,000
4. DIRECTOR OF ACADEMIC SERVICES - $60,000
    a. COMPUTER SERVICES MANAGER - $50,000
        i. MAINFRAME PROGRAMMER x 5 - $175,000
    b. WEB SERVICES MANAGER - $45,000
        i. WEB PROGRAMMER x 2 - $60,000
    c. ONLINE SERVICES MANAGER - $45,000
        i. WEB PROGRAMMER x 2 - $60,000
    d. IITL MANAGER - $45,000
        i. IITL TECHNICIAN x 4 - $120,000
    e. OPEN ACCESS LAB MANAGER - $45,000
        i. OAL DAY SUPERVISOR - $30,000
        ii. OAL NIGHT SUPERVISOR & SYSTEMS ANALYST - $32,000
5. STUDENT EMPLOYEE x 28 - $322,560

Section 2: Description and Diagram of GIAC University



GIAC University has two Internet connections. The primary Internet connection is a fractional DS3, at 20Mbps, to the GIAC System Wide Area Network (WAN). This connection not only provides an Internet connection for the campus, but also provides resources to other GIAC system schools such as H.323 (video conferencing) for distance education classes and for meetings. The second Internet connection is a 10Mbps-leased line from a commercial service provider. This connection provides commodity Internet access to the six residence halls and one apartment complex. Both circuits connect to separate Cisco 7401 routers and have internal routing setup so that students, in the residence halls network, do not get routed through the Internet when requesting resources from the university network.

In the residence halls network, the university has taken a hands off approach to managing the network. The university does not install or support hardware or software on student machines. The IT department's stance on the subject is that the departments is responsible for getting service to individual rooms and from their students are responsible for getting their computers onto the network. Given this approach the IT department has taken some extra precautions in trying to secure a historically open network.

- A Netscreen-ISG 2000 [(5)] firewall is used at the perimeter of the residence halls network. This firewall is configured to scan packets, with an external Trend Micro anti-virus appliance, coming into and leaving the network for malware threats.
- An Allot Communications NetEnforcer [(2)] is used to help control bandwidth by applying Quality of Service (QoS) features to data coming into and leaving the network. Not only does this allow the university to control the peer-to-peer traffic, but also acts as a monitoring tool for historical references to what kind of traffic traverses the residence halls network.
- A Netscreen IDP 500 [(6)] server is in-line with the NetEnforcer and the firewall to help mitigate most attacks that may come into and/or leave the network.
- Layer 3 switches are used in the edge of the network and help the IT department mitigate attacks by placing access lists as close to the edge as possible.
- A Windows 2003 server is configured for DHCP and DNS for the residence halls network.

A single Cisco Catalyst 6513 switch [(1)] supports the core of the network with dual supervisor engines and MSFCs. This redundancy within the chassis allows for a more robust and available network. This switch connects all the buildings and the core servers together.

The perimeter firewall, for the campus, is provided by two Cisco PIX 525 firewalls [(3)]. The primary firewall has an unrestricted license and the secondary firewall has a failover firewall. The secondary firewall is used in the event of a failure in the

primary firewall. The two firewalls have an internal, external, and 4 DMZ interfaces.

The DMZ is used for services that will continually be available to the public. The DMZ allows access to the www, online, smtp-relay, dns, webmail, student www, student webmail, and advisor servers. These services have a NetScreen IDP 100 server inline with the DMZ to help protect against network attacks.

- The www server is the campus primary web presence on the Internet.
- The online server is a web-based class delivery system for distance education.
- The smtp-relay is an email gateway that forwards email to internal email servers.
- The dns server provides external dns services and the primary authoritative dns server for the campus. The secondary authoritative server is provided by the GIAC system and is located offsite, which dns zone data is transferred to.
- The webmail servers provide the ability for staff, faculty, and students to check email from off-campus.
- The student web server lets students create and publish personnel websites.
- The advisor server is a web-based application so that students can add and drop classes online.

The Internal network houses the campus mainframe, network management, wwwdb, onlinedb, helpdesk, exchange backend, domain, file, terminal, intranet web, anti-virus, student domain, student file, student mail, student intranet, print, backup, radius, dev, and system update servers.

- The mainframe is protected by a Cisco PIX 515E firewall and is configured to only allow certain services, such as ssh, database, etc, from certain addresses within the network. This server contains student and employee information.
- The network management server monitors the campus network and alerts the network group, via email if any failure occurs. Since this server has access to the entire network via snmp, this server is protected by a Linux firewall.
- The wwwdb and onlinedb are database servers and provide the backend for the campus web presences.
- The helpdesk server is the way the information technology department distributes work to different areas through out the information technology department.
- Exchange 2003 is used for staff and faculty email and calendar sharing on campus.
- The staff and faculty domain controllers provide user authentication, internal dns, dhcp services, and is a focal point for pushing new software and software updates to end users.

- The file servers provide the ability for staff and faculty to be able to store data on the network drives so that it their data can be backed up.
- Citrix is used for terminal services to access network applications on thin clients and apple computers.
- Intranet web servers are used so that staff, faculty, and students are able to see what's going on around campus.
- Symantec Corporate Edition Anti-virus is used on staff, faculty, and lab machines for central management of anti-virus updates and scanning.
- The students have a separate domain controller used for authentication, and folder redirection in lab environment. The student file server is used to store the student data from folder redirection.
- The students have their own mail server and separate name space for student mail.
- A print server is used on campus to provide a central management point for network printers.
- The radius server is used for authentication for VPN access.
- The dev server for developing web applications.
- The systems update server for central patch management for windows computers.
- The backup server is used to backup all servers on the network to a tape library.
- A Cisco IDS module for the 6500 provides intrusion detection services for services on the inside of the network.

Services outside of the firewall are limited to special applications.

- A Cisco VPN Concentrator is used to provide VPN tunnels to remote offices and telecommuters The inside interface of the VPN concentrator, resides on the outside of the perimeter firewall and has a Netscreen IDP 100 server inline to help mitigate attacks from telecommuters and remote offices.
- H.323 codec's reside outside of the perimeter firewall to provide a more stable video service for videoconferences.

Section 3: Describe your office, or department at GIAC University

The Division of Information Technology at GIAC University consists of 34 full time employees and 28 student employees. The IT department's mission statement is "The Division of Information Technology, a service organization, will promote, support, and facilitate the University mission of teaching, research, and service through the efficient and effective use of technology to maximize students, faculty, and staff success." The budget for the information technology department is $3.1 million, with $1.6 million of the budget dedicated to salaries and benefits. The remaining funds are dedicated to operating costs, training, travel, and licensing.

The Systems Support office is a division within the Information Technology department. Our focus is on supporting the systems that the university uses for everyday business. The divisions within Systems Support are Networking Services, Telecommunications Services, PC Support Services, and Help Desk Services. The Systems Support division supports the networking, server, pc, and telephone infrastructure. Networking Services also acts as the security group on campus and is primarily responsible for maintaining an acceptable risk on campus. Networking Services is responsible for keeping backups up-to-date, keeping systems patched and secure as possible, distributing anti-virus updates, scheduling anti-virus scans, maintaining all firewall and router access-lists, monitoring the network, reviewing system logs, working with managers to help create policies, and generating reports for the campus and for the state.

GIAC University relies on the Division of Information Technology greatly to conduct business. Our role of creating a reliable, available, and secure infrastructure allows registrars to add students to the mainframe, students to add and drop classes from a web presence, students from half way around the world to take classes online, and allows for students to watch a professor on campus that is thousands of miles away in a different school. Without this functionality the school would be severely limited in its ability to generate income.

The Director of Systems Support is responsible for managerial functions over networking, telecommunications, pc support, and the help desk. The Director of Systems Support reports to the CIO of the campus. The CIO is responsible for overseeing all of the IT department and reports to the president of GIAC University.

Section 4: Describe your Job Description at GIAC University

I have been assigned the position of "Network Specialist II." [8] I have two direct reports depending on what function I'm performing and earn $35,100/year [9] in accordance with the state of Texas Human Resource pay grade scale. My position currently holds two primary responsibilities.

1. Networking: The primary responsibility of the Network Specialist II is to design, price, propose, implement, maintain, and monitor the LAN networking infrastructure. Monitor and generate monthly bandwidth usage reports on the WAN networking infrastructure. The networking infrastructure includes everything from LAN Ethernet switches, routers, packet shaping equipment, and wireless LAN equipment. This work directly reports to the Networking and Telecommunications Supervisor.
2. Security: The secondary responsibility of the Networking Specialist II is to design, price, propose, implement, maintain, and monitor the security infrastructure. This includes working with router access-lists, firewalls, intrusion detection systems, intrusion prevention systems, monitoring anti-virus updates and scans, monitoring the patch management system,

minimizing the risk of clear text network services by providing secure alternatives or encapsulating clear text protocols in some form of a strong encryption. This position also generates monthly security reports for the state of Texas as well as work with the campus Security Officer in creating and maintaining security policies. This work directly reports to the university security officer.

The university has a good track record with security when compared with other GIAC System schools [(22)]. For Example: The beginning of the Fall 2003 semester brought many schools to their knees with the propagation of blaster on their dormitory networks. GIAC University quickly noticed the propagation and decided to shut down the residence halls network. The network was offline for two days while the Systems Support group planned and implemented new network configurations and handed out CD's with a stinger utility to scan systems for malware, remove malware, and apply patches to patch student systems. The network configurations consisted of implementing new access-lists on the perimeter firewall and on the edge devices. This helped mitigate the propagation of blaster to the administrative network as well to computers on the Internet. Other schools within the GIAC system remained offline for weeks and in some cases months trying to implement an effective plan for mitigating such worms. The administrative only had five occurrences of blaster during the whole epidemic; this can be accounted for by Networking Services proactively monitoring system updates, anti-virus services, and implementing quickly firewall changes, updating IDS, and IDP systems.

Section 5: How does GIAC University conduct its business?

The Information Technology Support Center, ITSC, is the first point of contact for students and employees requesting services from the Division of Information Technology at GIAC University. When a customer contacts the ITSC for service a helpdesk technician follows a process of trying to determine what the customer wants.

If a department hired a new employee, the department head will call the ITSC. A helpdesk technician will send a new employee form to the department and open a work order to the telecommunications, network, pc support, and academic departments. In addition to the work order, the telecommunications, network, pc support, academic departments will receive copies of the signed new employee forms.

- Telecommunications Services will setup a phone and voice mailbox for the new employee.
- Network Services will create a network, email account, and configure the switch port in the new employee's office for their computer.
- PC support Services will setup the employee's new computer and install it in their office.

- Academic services will setup an account on the mainframe, if an account is needed, and get Network Services to allow their ip address through the firewall for the service they need.

When the departments have completed their work, they will fill out the proper documentation on the work order and complete it. The departments will then fill out a form with their account information and send it to the new employee. Voice mailboxes and long distance access codes are generated randomly. Network accounts and mainframe accounts are created a generic password and the new employee is forced to change their password at first logon.

If an employee leaves the university a process occurs for the leaving employee. The department head will call the ITSC and have them put in a work order for the leaving employees. The telecommunications, network, pc support, and academic departments will not act on the work order until they receive a signed leaving employee form from the department head of the employee. The department head then signs a leaving employee form and sends it to the needed departments. The departments within IT then follow a process of deleting accounts, removing phones and computers.

If a customer wants a service that the Division of Information Technology offers, then the customer will call the ITSC and tell the helpdesk technician what the customer wants. The help desk technician then opens a work order and sends the work order to the group that would handle the request. For example: If a staff member wants to have a videoconference with a person at a remote site, then the staff member will call the ITSC and explain the situation to the helpdesk technician. The helpdesk technician then opens a work order and sends the work order to the ITV group. The ITV group schedules the videoconference and lets the staff member know when the videoconference has been scheduled.

If a customer has a problem with a product that the Division of Information Technology manages then the customer will call the ITSC. The helpdesk technician will try to determine what the customers' problem is. The helpdesk technician will proceed to do some basic troubleshooting of the problem. If the helpdesk technician is not easily able to fix the problem then the helpdesk technician will create a work order and forward it to the group that is best able to fix the problem.

Section 6: What applications and/or what type of access are required to carry out business operations?

Email: The smtp-relay server in the DMZ acts as an email gateway for the email servers in the internal network. Filtering emails against an open-relay database [(10)] is the only type of spam filtering that the smtp-relay checks against. If a sending server has been blacklisted with an open relay, then the email is bounced back to the sender address.

The internal mail server for staff and faculty is much more then a mail server. It is a groupware application provided by Exchange 2003. Exchange 2003 provides staff and faculty with email services, as well as calendar sharing and a centralized contact database. Staff and faculty are able to utilize the Exchange 2003 services by using Outlook on campus, using the Outlook Web Access from off campus, or by using Outlook from off campus via VPN access. If an end user only wants to utilize email services then the end user can use any email client that the user wants.

The internal mail server for students utilizes Linux and Postfix for email. Students are able to utilize email services via a web-mail server in the DMZ. The Division of Information Technology does not support any other local email clients for the students.

User Authentication: User authentication for staff, faculty, and students is provided by Windows 2003/Active Directory. Staff and faculty are on one domain and students are on a separate domain. The password policy for the campus calls for a mixture of at least one capital letter, one number, one special character, eight characters long, and to be changed every 42 days. The Active Directory server is setup with a five-password rotation, which means you cannot use the same password until it has been changed five times.

File Storage: Staff, faculty, and students are able to utilize the file servers to store critical data. Every user with a network account is able to access their shared folder on the file server by accessing their "U" drive. Every user has a 1Gbps user quota.

WWW: The campus web presences are provided on multiple servers. The campus has a separate web presence from the students. Departments are able to publish information to the web presence with Macromedia Contribute. The Web Services department chose this package because it easily allows departments to publish data onto the www server and keep a similar theme for the campus web site. Dynamic web applications pull information from a database setting in the internal network. The wwwdb and www server are only able to communicate with each other through the specified database port. Students are able to publish to the student web presence via a secure session content manager. This eliminates the need for clear text protocols like ftp and the need to give students an account with shell access.

Online: Online courses are provided through this server. This server is very dynamic and requires data to be stored in a database server, which lies on the internal network. The onlinedb server is only allowed to serve database information to the online web server. Only students who have signed up for online classes are able to login to this server and only faculty that teach classes online are able to login to this server. The online server uses a custom programmed web interface that has been developed over the past five years.

Class: The class server is a place where faculty members are required to post their syllabi for their classes. This lets the students download the syllabi before classes begin and get the materials they need before each semester begins.

Mainframe: The campus mainframe holds all student and employee information. This server has a separate firewall from the rest of the campus and only allows specific services for specific ip addresses on campus. Users on this server are required to change their passwords monthly. Registrars use this server to add/remove students from classes and many departments on campus use this server to add/change/remove employee information from its databases. This server also interfaces with the advisor server in the DMZ. The advisor server allows students to add/remove classes online from a secure web session.

Terminal Services: Citrix is the campus terminal server. The registrar's office uses thin clients and logs onto the network via Citrix. Apple computers around campus also use Citrix to use applications that only run in a Windows environment.

Intranet Web: Staff and Faculty have a separate Intranet web server from the students. This server allows staff, faculty, and students to see what is happening around campus, allows staff, faculty, and students to participate in campus polls, and allows staff, faculty, and students a central place to download campus forms.

H.323: H.323 is used for videoconferencing applications. Students use these services to take class with professors at a remote university on the GIAC system WAN. Staff and Faculty use these services for meetings with personnel at remote campuses.

VPN: Two remote sites connect to the campus via VPN. This allows the remote sites to have the same services that the rest of the campus has. These sites connect to the VPN concentrator via a VPN router. Telecommuters can also connect to the VPN concentrator. They use VPN clients or can use a web browser and use the SSL VPN services provided.

Internet: Internet services are provided to the entire campus. The administrative network takes advantage of the GIAC system WAN and the residence halls use the commercial Internet circuit. Allot Communications help regulate some of the services the come into and leave the network. For Example peer-to-peer services are not allowed at all on the GIAC system wan, but are allowed to a degree on the residence halls network. The residence halls are allowed to use 3Mbps for peer-to-peer communications. The Division of Information Technology has been keeping up with the latest peer-to-peer legal battles and is ready to eliminate the communications if needed.

Section 7: Identify three "crown jewels" your office has access to and is responsible for

Network Infrastructure: The network infrastructure is a key piece to how the university conducts business on a daily basis. The Division of Information Technology recognizes this and has created processes to make sure that all device configurations get backed up nightly, all access to network devices is done in a secure manner, and any changes made to the infrastructure are properly documented.

The network management server backs-up all router, switch, and firewall configurations nightly. After that process is finished the network management server is backed-up to the backup server. This ensures that a near current configuration is always easily available.

Any person needing to make changes to switches has to first SSH to the Linux firewall, which separates the administrative network segment from the network management segment, and telnet to the switch that they want to make changes to. The SSH tunnel ensures that all data is encrypted from the firewall to the end users computer. Access to the switches is controlled by Authentication, Authorization, and Accounting (AAA); this allows the networking group to permit/deny access to the switches by username/password and from there allow only certain commands to be executed based upon username. Locked cabinets regulate physical access to the switches, except in the university data center, which is regulated by keypad code and swipe card. Routers and firewalls utilize SSH features to access the devices and use the same AAA parameters for user control. All remote access is limited by ip address.

All changes to configurations are documented in the helpdesk software. This documentation explains what and why configurations were changed. This historical data allows the network technicians to go back and look at the documented changes anytime something goes wrong.

Mainframe: A mainframe is a crown jewel of any business or university. It is no different for GIAC University. The campus mainframe holds sensitive information about students and employees. This information includes contact information like email addresses, mailing addresses, and phone numbers. The mainframe also holds information like social security numbers, mother's maiden name, date of birth, employment date, background checks, current salary, and other personnel information that employees and students would not want public. The university takes this very seriously and takes precautions in making sure that data is safe.

One form of protection is a Cisco PIX 515E firewall. This firewall is configured to only allow specific ip addresses to access specific services on the mainframe. All employees' who access the mainframe do so via SSH. This ensures that all data sent across the wire is done so via an encrypted tunnel. The vendor who wrote

the software package for the mainframe also has access to the mainframe via SSH. The firewall is configured so that only certain ip addresses from the vendor's network are allowed to access the mainframe. All vendor accounts are disabled by default unless the vendor asks for access for support purposes. The advisor web server is allowed to access the database of the mainframe. This functionality allows students to access their account information, make changes to that information, and add/drop classes from a web interface. The web interface is secured via SSL communications.

Another form of protection on the mainframe is user based access control. Every department that has access to the mainframe is places in groups on the server. The group determines what data a specific user is allowed to access. For example: A registrar's job is to enroll students for class. Registrars do not need to access employee information. So the registrars group is only allowed to enroll students for classes. Only managers of individual departments are able to access employee information about employees in their department.

Every user on the mainframe is required to follow a separate password policy from the campus password policy. Passwords are required to be changed every thirty days, must contain at least one upper-case character, one number, one special character, and must contain at least eight characters.

Exchange: The Exchange 2003 server is a central point for department contact lists, distribution lists, and departmental calendar sharing. It is very important for the university to protect those assets.

There are public contacts and private contacts. The public contacts include inter-campus contacts. This information is open to employee utilizing Exchange. Private contacts include state agency contacts, salesperson contacts, etc. These contacts are managed by individual departments and are only available to those employees within the departments.

Departmental calendar shares are managed by individual departments and are only available to the departments.

The Division of Information Technology maintains distribution lists. These lists contain "all", "faculty", "staff", and "students". The all list is a list of email addresses of every staff and faculty; the faculty list is a list of email addresses of every faculty member, the staff list contains the email addresses of every staff member, and the student list contains the email addresses of every enrolled student at GIAC University. The systems analyst and the network manager are the only employees who have access to these lists and are the individuals responsible for sending emails to the lists.

Section 8: Insider threat vector for each of your office's crown jewels

The threat from the inside is possibly the largest threat faced by any information security professional. The Division of Information Technology recognizes this threat and works towards minimizing this threat.

As mentioned, the network infrastructure is one of the universities crown jewels. If somebody were able to break into the network management infrastructure it could cause havoc for the network. This person would be able to create backdoors, Denial of Service attack, and use the management infrastructure to sniff data on the network.

If a person were able to gain physical access to any network switch on campus it would be trivial for a person to gain access to the management infrastructure of the network. All a person would have to do is plug a laptop into a switch with a console cable and follow the password recovery procedures for the switch. Cisco Systems has the password recovery procedures listed for every single product they produce and is the first link found when searching for "password recovery" on the www.cisco.com website [(11)]. Once an attacker has enable mode on a switch the attacker can perform a number of attacks.

An attacker would be able to set an open port to the default management port (vlan1) and setup their laptop with a sniffer, such as Ethereal [(12)] or Ettercap [(13)]. Eventually the attacker will gather usernames and passwords to switch management accounts from personnel using telnet to manage the switches. The attacker would be able to use common switch commands such as "show mac-address", "show cam", "show cdp-neighbors", "show arp" to map the network and locate specific computers on the network.

The attacker could create a "span" (switched port analyzer) port. This would allow the attacker to tell the switch to send all data from a specific port or a specific vlan to their computer. The attacker could then use a sniffer to capture the data from the specific port or vlan. Using this technique an attacker could gain usernames and passwords from clear text protocols and other information about services running on the network.

If an attacker, with physical access, were able to gain usernames/passwords to the switch management infrastructure then the attacker could login to as many or as few switches as he/she wanted to and remove the start-up configurations and set the switches to reboot at a certain time. This could be disastrous and could take a very long time to have the switches up and operational again.

The different attacks have endless possibilities if an attacker were able to gain physical access to the network. GIAC University does take precautions to protect against such an attack. All switches are in locked cabinets in locked telecommunications closets. Only authorized personnel are given keys to the closet and the cabinets. If a switch were to physically be compromised then there could only be a few possibilities. Switch configurations are backed up nightly to the network management server, which is then backed up to tape. This helps insure that a near current configuration is always at hand.

Another insider threat would be to the campus mainframe. The campus mainframe holds a wide variety of information from student enrollment information to employee salary information. The IT department feels that this information held on this server is probably one more high value targets on campus. There could be many types of attacks ranging from man in the middle, replay attacks, or placing backdoors and Trojans on an unexpecting end users computer.

One attack could be creating a man in the middle attack. This attack would consist of an attacker arp spoofing the router into thinking that the attackers computer was the mainframe computer and then setting up a fake SSH server to log incoming usernames/passwords.

The replay attack could have the similar characteristics of the man in the middle attack, but instead of logging usernames/passwords the attacker could log information heading to the server and then manipulate the data and forward the manipulated data to the server. This type of attack could possibly corrupt the database on the server or change personnel information about a student or employee in the system database.

Backdoors or Trojans could possibly be the easiest attacks to perform. This attack could consist of the insider posing as a pc support technician or the attacker could be the department "computer guru." The attacker could do a number of different attacks. The person could disable the system anti-virus by deleting a few key dll files. This would give the appearance that the anti-virus software was still running, but render the anti-virus software useless. The attacker could install a software or a hardware based key logger [(14)] onto the computer. If the attacker wanted to have remote control of a particular computer then the attacker could install a backdoor onto the system like sub7. This would allow the attacker to logon to the computer from anywhere with a network connection.

Windows 2003 and Exchange 2003 are fairly new products added to the Microsoft line of Server products. Exchange 2003 is a groupware server that offers email services, shared contacts, and shared calendars just to name a few features.

Probably one of the easiest way's to gain information from the exchange server that an insider attacker would want is to set down at somebody's computer, which is turned on. Most people that are not savvy on information security choose laziness over security and either saves their passwords or write down their passwords on sticky notes. The attacker could easily be able to send emails posing as the absent person, add, remove, and change shared and person calendar and contact objects.

The university holds many vendor contracts. Most of these contracts are in both electronic format and paper format. The paper format contracts are stored in file cabinets in the manager's office. These cabinets are not locked; however the manager does close and lock his office door when he is not in the office. This is a normal precaution to take, but the office building has a set of master keys that is able to open most doors in the building. Every employee who works in the office has a set of master keys. This makes contract information available to any person who has a set of master keys.

The electronic format of the data is held on the campus file servers. They are stored in a shared folder in which only the managers of the IT department are able to access.

Insiders may have many motivations to threaten the campus crown jewels. They may attack resources for purposes of sabotage, create fraudulent documents, steal individual identities, or modify or destroy identity profiles.

Section 9: Outsider threat vector for one of your office's crown jewels

Theft, modification, and destruction of user data occur daily on the Internet. Stories circulate on the Internet about malicious hackers stealing everything from credit card numbers to social security numbers. This is a very serious threat to GIAC University as the mainframe database holds all the information necessary for an attacker to steal one's identity. GIAC University feels that this type of data is a high value target in any environment and works towards all possible way an attacker can take advantage of vulnerabilities to gain access to this data.

One way that an attacker could possibly gain access to this information is to compromise the advisor server, which sits in the DMZ and has access to the mainframe database in the internal network. The advisor server consists of a server with Linux as its operating system. The system runs OpenSSH for remote administration, Apache and OpenSSL for secure web sessions, and a Computer Associates ArcServe client for system backups.

Cross-site Scripting: Cross-site scripting vulnerabilities, or XSS [(15)], are prevalent in many software products. This vulnerability is exploited when an attacker manipulates a website URL to execute commands that the server software was not meant to execute. This vulnerability could have the potential for the attacker

to grab a copy of the mainframe database by manipulating the URL so that the server queries the database to print all of its data from a specific database.

Directory Traversal: The attacker could also potentially execute a directory traversal exploit to drop the attacker into a shell in the server. This shell would be printed out in the web browser and would be pretty useless by itself. The attacker could manipulate the URL to upload and execute a tool like Netcat [(23)]. Netcat has been described as "The TCP/IP Swiss Army Knife" and has been a key tool in exploitation of vulnerabilities like the Microsoft IIS Unicode vulnerability. Once the attacker has a shell on the advisor server the attacker could download the database to their computer, make changes, and/or delete information from the database.

The attacker can have several motivations for committing such malicious acts. One such explanation is the attacker gets a "high", if you will, from gaining information that he/she would not normally be able to get. The attacker maybe a very sophisticated person and knows a great deal about the package that many universities use for their mainframe. This person may use this information for identity theft or possibly sell the information gained from the mainframe.

Section 10: Malicious code threat vector for one of your office's crown jewels

The Scenario: An employee at GIAC University has her child at work one day, because school is out for a holiday. The employee grabs a random ip address and sets her laptop on the network so that her child can entertain himself by surfing the Internet. The employee realizes that it is against the university policy to place non-university computer equipment on the network, but thinks to herself "What's the harm?" What the employee doesn't realize is that her laptop is infected with the slammer worm [(17)] from unpatched Microsoft Office Applications.

The slammer worm targets systems running Microsoft SQL 2000, as well as Microsoft Desktop Engine 2000 (MDE 2000). "The vulnerability allows for the execution of arbitrary code on the SQL server computer due to a stack buffer overflow." – CERT Advisory CA-2003-04 MS-SQL Server Worm [(16)]

In no time at all the employee's laptop starts scanning the internal network for unpatched versions of MS SQL and MDE. If the worm finds a vulnerable host then it will infect that host and the process repeats itself. If numerous MS SQL servers and MDE products are on the network and unpatched can create a Denial of Service attack consuming available bandwidth on the network and rendering services unavailable.

SQL servers infected with the slammer worm will need to be formatted and have their operating system and other software reinstalled. The system will be patched and its database restored from backups. This can be a very time consuming

process and can cost the university thousands of dollars just in salaries for the technicians to reinstall computer software. Thousands more in salaries would be wasted because many employee's on campus would not be able to access the resources needed to do their job.

Section 11: Identify the most severe threat

Computers that are not owned by the university and are not managed by the Division of Information Technology are the most serious threat to the IT resources at GIAC University. People are able to bring their personnel laptops onto campus, spread worms through the campus, and steal information from other systems on the network.

Employees, students, and other personnel often connect computers to the internal network without the knowledge of the IT staff at GIAC University. This is a growing problem. Personnel can connect his or her machine to the network to let somebody surf the Internet or even at times to save some information to work on at home. These personnel either do not read through university policy or choose to ignore university policy concerning network usage.

People do not seem to understand the issues with connecting non-university equipment to the network. As mentioned earlier, the five hosts that were infected with blaster, in the administrative network, during the blaster epidemic were because of infected non-university machines connecting to the network. Thankfully what incidents have occurred because of non-university computers hasn't affected the university in a large way, but the incidents that do happen cost the university money. The money comes in the form of the network group sniffing the network for problems; pc support fixing infected machines, and the person with an infected machine not being able to work. Add the salaries up of time-spent tracking and fixing the problem and the money can add up quickly.

Section 12: Recommend a remediation strategy for one of the threat vectors you have described

As mentioned in the previous section the most serious threat to the security of the university is non-GIAC owned computers connecting to the internal network. This section describes what steps can be taken to help mitigate that threat and give an estimate of how much it will cost.

There are several options that can be exercised to keep non-authorized computers from accessing the internal network. Implementing URT [(18)] is the option that will not only help mitigate non-authorized computers from accessing the network, but will also help make the network friendlier to transient users.

Cisco Systems makes a user registration application for their networking equipment. The application is called “Cisco Secure User Registration Tool”, or URT. This application has two forms of authentication.

The first form of authentication is mac address based authentication. When a computer connects to the network the switch will query the VLAN Policy Server (VPS) database. If the computers mac address matches an entry in the VPS database then the switch will configure the switch port dynamically based on the VPS database values. If the computer’s mac address does not match any entries in the VPS database then the switch will configure the switch port to be in a “quarantined” vlan.

The second form of authentication is user-based authentication. Before the end user will be able to access any network resources the end user will have to open up a web browser and authenticate himself or herself with a username/password. Any site that a user tries to surf to will be redirected to the URT login page until the user has logged into the network. After successful login the user will have access to network resources as normal.

The process of adding every GIAC owned computer to the VPS database, reconfiguring every port, and training all employees will be a very personnel intensive process. The migration for this process is expected to take four months from the time the system is setup and running.

First step is to add all computers to the VPS server. After the server is setup the networking and pc support group will have access to add and remove machines from the VPS database. These two groups will work together to populate the VPS database for the initial implementation. After the implementation, the pc support group will be responsible for the day-to-day maintenance of the VPS database.

The second and third steps will involve pc support going to every individual computer and calling the networking group to change the switch port for the dynamic vlan configuration. When the change is finished the pc support technician will reboot the computer and give the employee a training session on how to connect to the network.

This project is estimated to cost the university $22,000. This includes two Dell PowerEdge 1750 servers with windows 2003 operating system and the Cisco URT software.

Section 13: Review the backup strategy

GIAC University has an existing backup strategy, but after a reviewing the strategy it is clear that not all data is being backed up. The current backup strategy is to backup all user data that resides on the file servers. Many users do

not save their data on the file servers, because they never had any formal training on how to save data to the file servers and simply do not know how. Other users do not take the time to save data to the file servers, but instead opt to save data in default locations.

This is a troubling trend for the university. If a users hard drive crashes or the accidentally deletes their data the IT staff has no way of recovering the data. The Division of Information Technology proposes implementing two solutions to help mitigate the problem of possible data loss.

The first solution is to implement "roaming user profiles" [(19)] in Active Directory. This would backup the entire users' folder to the file servers every time users logged off the network and would allow the users to logon to any computer in the university and have familiar desktop. This solution could be implemented quickly with little cost to the university. It still does not backup the entire hard drive though, which means if users have data stored in a directory that is not in their user directory then the roaming-profiles will not backup that data.

The second solution involves installing ArcServe clients on the workstations and backup workstations on a rotating basis. For Example: Group A would have their workstations backed up to tape on night one and Group B would have their data backed up to tape on night two, etc. This would be a monthly rotation. This rotation would help ensure that nightly backups are done in a timely manner and not running when a user logs on in the next business day.

This solution will integrate into the existing backup schedule and utilize an existing server, tape library, and backup software to backup the data on the workstations. The backup server is a Dell PowerEdge server and is connected to an Exabyte tape library. The only hardware costs associated with this implementation is the cost of the media. This process is estimated to use an additional twenty-four tapes per month. Each tape costs one hundred dollars, so for twelve months of tapes the cost would come to nearly twenty-nine thousand dollars. The only additional costs would salaries of the technicians involved in installing the ArcServe software onto the workstations. It's estimated to take seven hours for three student technicians to install the software on sixty machines. The cost of salaries for the student technicians will be one hundred and sixty eight dollars.

Tapes are in one of two places when not being used by the tape library.

- The first place is in an on-site vault. This vault is comprised of a cinder block room that is used for only storing backup media. Only IT managers and the backup technician (systems analyst) have access to this room.
- The second place is in an off-site, on campus vault. This vault is located on campus, but is in a different building as the datacenter. This vault houses the universities critical information.

Tapes will be rotated on a daily basis. Newly written tapes will be taken from the tape library to the university vault. The day old tapes, in the university vault, will then be taken to the datacenter vault. This process helps ensure that “not all our eggs are in one basket” in the event that something happens to the tapes at the datacenter.

Section 14: Review offsite backups

After reviewing the current backup strategy the senior management in the Division of Information Technology realized that GIAC University has no offsite backup strategy to help the protect the university against loss in the event of a disaster. The offsite backup strategy recommended is to work with a local university to implement a “tape exchange.”

The local university is two hundred and fifty miles away from GIAC University, which if a disaster were to occur at one location it should not affect the other location. This process will involve the two universities exchanging their monthly backup at the first of every month. For this process to happen the two universities will need to coordinate with each other to know when each university should know when to expect each others

- All tapes going to the offsite location will need to be stored in a fire resistant transportable media vault. This media vault will have the capability to store thirty 8mm tapes within the vault. The Division of Information Technology will have a rotation of two media vaults. One will be at the local site and the other will be at the remote site. This will ensure that the tapes will be able to be sent to each site on time without having to wait for the media vault to be mailed back each month. The two IT directors and the systems analyst who is responsible for backups will the only individuals who will carry the keys to the media vault. A spare key will be kept in the university vault.
- Offsite backups will be sent on the first business day of every month. This includes sending back the remote universities tapes. The systems analyst responsible for the backups will put the monthly tapes into the media vault and mail the tapes via USPS.
- The backup technicians will verify via phone and email at both locations when the tapes have been received.
- The remote universities tapes will be stored into the university vault for the remaining of the month.

Being able to have access to the tapes in the event of a disaster is a must. To solve this problem the two universities will work with each other. Each university will have three contacts available for each other. Those contacts are the CIO, Networking Supervisor, and the Systems Analyst responsible for backups.

In the event of a disaster the Networking Supervisor for GIAC University will call its contacts at the other local university. The local university will get GIAC's tapes from their vault and the Networking Supervisor will meet the personnel from the local university at a predetermined location to retrieve GIAC University's backup media. Once the media is back at GIAC University the groups involved will go through the needed procedures to restore data from its backups.

These procedures will be tested every three months. Instead of mailing the tapes on the third month, GIAC University and the local university will test their procedures. GIAC University's Networking Supervisor will meet personnel from the local university at a predetermined location. The two groups will exchange their media vaults and return to their universities. When the Networking Supervisor returns from retrieving the media he or she will hand the media vault to the systems analyst. The systems analyst will then restore media to test servers to verify that the media works properly and to test the restore procedures for the Division of Information Technology.

Section 15: Devise a guerilla business continuity plan

To have a effective business continuity plan the Division of Information Technology needs to have buy-in from the university administration. To gain buy-in from the university administration the Division of Information Technology must take the one time step in presenting the administration the following:

- What are the short-term and long-term costs involved with creating a business continuity plan?
- What are the possibilities if the plan is not implemented?
- The Texas Administrative Code (TAC) 202.6 requires all state entities to implement a business continuity plan. [(21)]
- Present an initial recovery time-line in the event of a disaster.

Developing a business continuity plan is a difficult process. After the buy-in from the university administration the Division of Information Technology has many steps of planning and implementing the business continuity plan. Some of the repeated tasks are:

- Annual testing of the documentation.
- Updating the documentation as needed and distributing the documentation to the employees at GIAC University.

Creating an effective and efficient business continuity plan is crucial to the livelihood of GIAC University. For this reason testing the business continuity plan is executed annually. Mock disasters recovery scenarios are simulated within the Division of Information Technology and the documentation is followed to be sure that no step is left out.

Service Level Agreements (SLA) have been signed with all critical vendors to be sure that the university is able to get equipment and services as soon as possible in the event of a disaster. The GIAC System has provided the university with floor space in their datacenter down state so the university is able to implement core-networking services quickly. These services include the mainframe, DNS, email, and all web presences will point to a website stating that the services are unavailable.

In the event of a loss of phone service because of a disaster the local telecommunications company will redirect all phone calls coming into the university to a system that will explain that the phone services are down for the time again and please check back later. The university has an SLA with their telecommunications vendors so that PBX equipment can be replaced within 24 hours in the event of a disaster.

Networking and server vendors also have similar SLA's with the university that they will replace equipment in the event of a disaster. This allows the Division of Information Technology to quickly get networking services up quickly to essential personnel.

Once the plan has been thoroughly tested and works properly the same procedures should be taken with all other departments within the University to be sure that they will be able to continue to work in the event of a disaster.

References

1. http://www.cisco.com/en/US/products/hw/switches/ps708/index.html - The Cisco Catalyst 6500 Product Page.
2. http://www.allot.com/pages/product_content.asp?intGlobalId=6 – The Allot Communications Product Page.
3. http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/ps2118/index.html - The Cisco PIX 525 Product Page.
4. http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_package.html - Cisco SAFE Blueprints.
5. http://www.netscreen.com/products/firewall/ - The Netscreen Firewall Product Page.
6. http://www.netscreen.com/products/idp - The Netscreen IDP Product Page.
7. http://www.faqs.org/rfcs/rfc1918.html - RFC 1918: Address Allocation of Private Internets.
8. http://www.hr.state.tx.us/compensation/jobdescriptions/r0288.htm - The Network Specialist II Job Descriptions from the state of Texas
9. http://www.hr.state.tx.us/Compensation/FY0405SCHEDULEB.html - The state of Texas pay scale.
10. http://www.ordb.org/ - The Open Relay Database

11. http://cisco.com/en/US/products/hw/contnetw/ps789/products_tech_note09186a00801746e6.shtml - Cisco Systems password recovery procedures.
12. http://www.ethereal.com/ - Ethereal
13. http://ettercap.sourceforge.net/ - Ettercap
14. http://www.thinkgeek.com/gadgets/electronic/5a05/ - PS/2 Key logger
15. http://www.itsecurity.com/dictionary/xss.htm - Definition of Cross site Scripting (XSS)
16. http://www.cert.org/advisories/CA-2003-04.html - CERT MS SQL vulnerability page.
17. http://securityresponse.symantec.com/avcenter/venc/data/w32.sqlexp.worm.html - Information about the Slammer worm.
18. http://www.cisco.com/en/US/products/sw/secursw/ps2136/index.html - Cisco User Registration Product Page.
19. http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/all/deployguide/en-us/dmebc_dsm_yapz.asp - Implementing Roaming User Profiles.
20. http://www.keysan.com/big/picffir2712.html - Tape Media Vault.
21. http://info.sos.state.tx.us/pls/pub/readtac$ext.TacPage?sl=T&app=9&p_dir=N&p_rloc=94899&p_tloc=&p_ploc=1&pg=5&p_tac=&ti=1&pt=10&ch=202&rl=2 - Texas Administrative Code 202.6: Business Continuity Planning.
22. http://www.securityfocus.com/news/6877/ - Universities Rush to Protect Networks
23. http://www.atstake.com/research/tools/network_utilities/ - Netcat

Last Updated: September 19th, 2017

Upcoming Training

SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Cupertino SEC301	Cupertino, CA	Oct 02, 2017 - Oct 06, 2017	Community SANS
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VA	Oct 14, 2017 - Oct 21, 2017	Live Event
Community SANS Portland SEC301	Portland, OR	Oct 30, 2017 - Nov 03, 2017	Community SANS
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS Ottawa SEC301	Ottawa, ON	Dec 04, 2017 - Dec 08, 2017	Community SANS
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS Las Vegas 2018	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	Live Event
SANS Southern California- Anaheim 2018	Anaheim, CA	Feb 12, 2018 - Feb 17, 2018	Live Event
SANS New York City Winter 2018	New York, NY	Feb 26, 2018 - Mar 03, 2018	Live Event
SANS Secure Singapore 2018	Singapore, Singapore	Mar 12, 2018 - Mar 24, 2018	Live Event
SANS Northern VA Spring - Tysons 2018	Tysons, VA	Mar 17, 2018 - Mar 24, 2018	Live Event
SANS Secure Canberra 2018	Canberra, Australia	Mar 19, 2018 - Mar 24, 2018	Live Event
SANS 2018	Orlando, FL	Apr 03, 2018 - Apr 10, 2018	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced