Global Information Assurance Certification Paper

GIAC University of the State (G.U.S)

An overview of the school systems Information Security

GIAC: Information Security Fundamentals+ GISF - Practical Assignment
Version 1.0 (July 25, 2003)
Joseph L. Cosgriff
Challenge

ABSTRACT

The purpose of this document is to provide information relevant to securing a large University environment. This information is presented in the form of a fictional scenario for a fictional University located somewhere in the Carolinas. The goal of this document is to cover all the topics necessary to successfully complete the requirements of the GIAC Information Security Fundamentals (GISF) certification.

Part I – Description of GIAC University of the State (GUS)

GUS is a state run University of higher education that is considered one of the nations leading universities in engineering, science and technology. Primarily a research-extensive land-grant institution that started as an agriculture institution, GUS became a progressive campus ignited by the flames of young achievers.

GUS has an annual revenue of about $600 million. This revenue is generated by two equally important sources. First and very important to the core of the University's business, is the revenue generated by its student's enrollment. At any given enrollment period the university has approximately 35,000 students from all states within the union and well over 100 countries worldwide. Secondly, GUS is support by an annual state funded budget.

The University Managed Information Systems (UMIS) division is the IT support element that is vital to how the University generates revenue and ensures it's secure transfer, storage, protection, and backup of data. The UMIS division has sole IT support and responsibly for the entire university.

All aspects of IT support for GUS are not centrally located. However, the UMIS division centrally manages it. Geographically, the IT support is spread over the entire state with over 20 remote locations and over 60 buildings. The IT infrastructure is divided between three organizations. The Computing for Administrative Services (CAS) unit is responsible for the "business" related applications that run the University. The University Information Technology (UIT) unit is responsible for the academic, faculty, and student applications of the University as well as each college IT support requirement. Finally, the responsibility for the university network backbone and network security is the Network Technology & Communications (NTC) unit. All three groups report to the Associate Vice-Chancellor for UMIS.

While GUS has almost 5,000 employees, the UMIS division only has a staff of approximately 160 permanent and student employees.

The payroll load for fundamental UMIS IT positions:

Position	Personnel	Average annual salary	Total
Associate Vice-Chancellor for UMIS	1	200K	200K
Directors (CAS, UIT and NTC)	3	120K	360K
Admin Secretary staff	11	35K	385K
IT Managers	17	75K	~ 1.3M
Business & Technology Applications Developer	15	58K	870K
Technology Support Technician	25	40K	~ 1M
Operations and Systems	15	57K	855K
Networking	32	56K	~ 1.8M

Information Security	4	70K	280K
Business/Contract Services	8	29K	232K
Student employees	30	10K	300K
Approximate number of employees	161		
Total annual UMIS IT payroll load is:			~$7.6M

Part II – Diagram and Description of GIAC University of the State (GUS)

GUS has implemented a border router/internal router approach for their connection to the world. This is an architecture that places a router(s) external to the firewall with Access Control Lists (ACLs) on it that protects (with a broad stroke) the network. Both the internal and external routers are Cisco 7300 series routers [(1)].

The border routers have had all outside access disabled to the interfaces. This restriction is even from internal or "restricted" hosts. The only means to access the routers is via a VPN connection. The idea here is to limit access to a select group of hosts. The fewer the better!

Then a firewall is implemented. In this instance GUS uses two Check Point Firewalls (Check Point FW-1/VPN-1[(2)] solution riding on a Nokia appliance) working in redundant and failover mode. The firewall is multi-interfaced, with one set of interfaces for the border routers, one set for the DMZ environment, and one set for the internal routers. There is another set of interfaces that remain open for future growth. The DMZ environment contains the GUS public web servers and the GUS public mail servers.

There is a series of internal routers that mimic the border routers but the ACLs are slightly different. There primary purpose is to protect traffic bound for external sources.

The internal network is segmented. GUS has "protected" systems that reside behind an additional Check Point Firewall. These systems include the Human Resources (HR) and Financial (FIN) systems as well as the mainframe. These "protected" systems are separated from the GUS campus "LAN." This land contains many of the other GUS related systems. For example, the GUS student servers, Mail backend servers, the file and print serves, and the Security servers. Additionally, all of the faculty and staff desktops are on the GUS LAN.

Students have Internet access from their dorm rooms on the StuNet but this access is segmented from the rest of the internal University network. We think of it as a free Internet Service Provider (ISP) for them.

Remote access for GUS is divided into four primary avenues:

- Remote Campuses: The remote campuses connect to the University core network via the Check Point VPN-1 remote access solution.
- Wireless connectivity: The wireless connectivity is considered for convenience only. It is not secure and has not been implemented campus wide.
- Distant Learning: Distant learning students use secure web (SSL) to connect to student information and applications (e.g., calendars, email, registration, syllabus)
- Web Citrix [3]: Allows employees to access the network from remote locations (e.g., home, travel)

For the network diagram, see figure 1

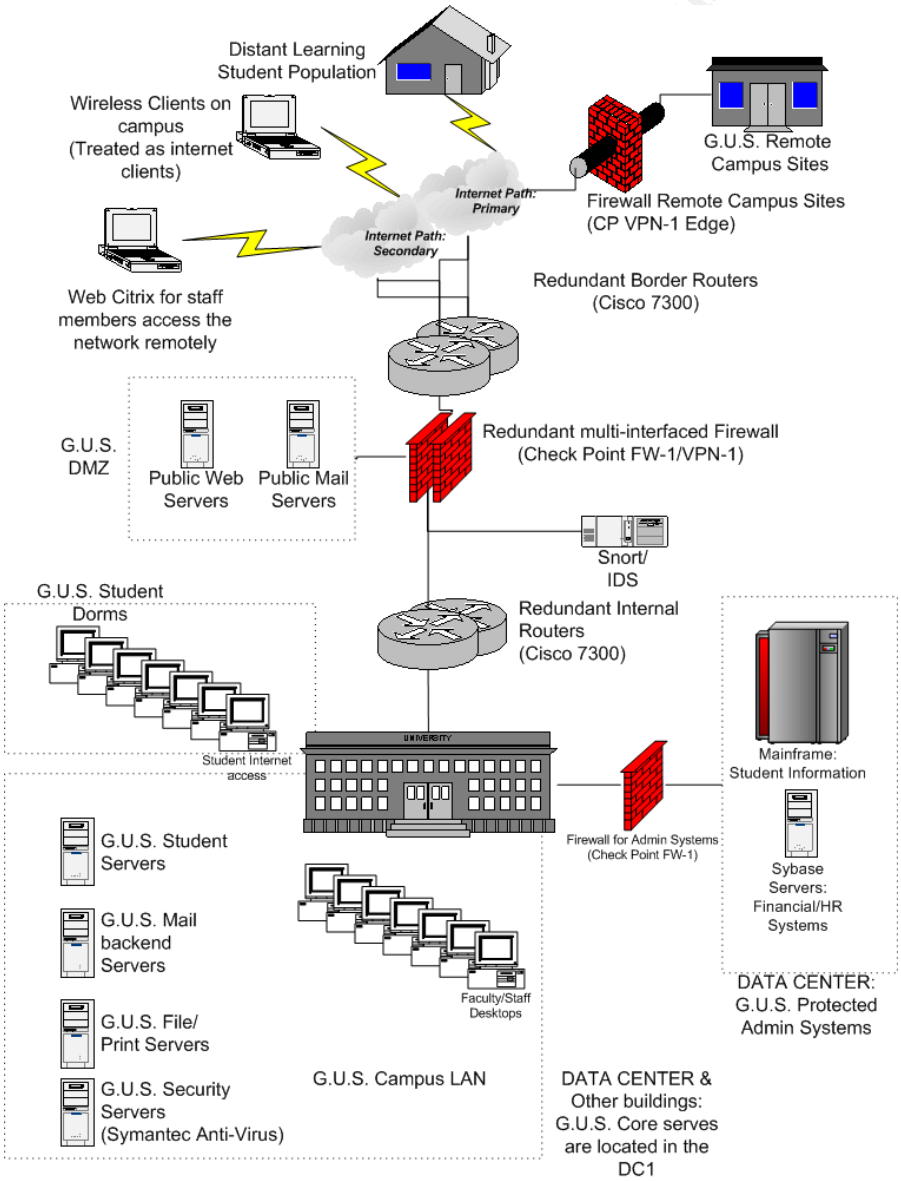

Figure 1

Part III – Description of my office at GUS

I support the Network Security Services (NSS) office that reports directly to the Director of Network Technology & Communications (NTC) unit. Even though our chain-of-command is our manager, the NTC Director, and then the Associate Vice-Chancellor (A-VC) of UMIS, we are actually a GUS UMIS IT division asset. We support the campus as a whole and provide network security services as needed or directed by our manager, director, or the A-VC.

The NSS mission statement is: "The Network Security Services team provides "top-notch" efficient and unified network security services for the GIAC University of the State."

Our team carries the banner of network security for the University. It is with this role that we support and enhance the operational effectiveness of GUS. Because information security is a dynamic and growing function within the private, government, and the individual population, it is our job to provide the technical expertise to support the needs of the University. With out our work, the information that is vital to the success of GUS is significantly diminished.

There are four employees and one manager that comprise the NSS team. We have five primary areas of responsibility. Each team member may have one or more primary focus areas but may also work a secondary and/or tertiary support role for the other areas. The following are the areas we have responsibility for,

a. the distributed firewall architecture through out the University network,
b. the intrusion detection systems (IDS) for the University,
c. the anti-virus support/management for desktops and servers,
d. the remote access control and management,
e. the development of the information security policies, rules and regulations, and conducting basic user information security training.

The UMIS A-VC has significant input on the NSS budget. We have an annual operating budget of approximately, $600K. This is divided between $355K in salary, $30K to support individual and other training requirements, and the remaining on software/hardware licenses and purchases. The total budget for security is only about 8% of the total UMIS IT budget and approximately 1% of the total University budget.

To support it's mission for GUS, the NSS team has approximately 7 laptops and 3 servers to support individual requirements and other security requirements. Additionally the team has responsibility for 25 firewall/VPN appliances distributed through the university. We also manage and control the single network IDS system that resides between the core firewalls and the internal Cisco routers.

PART IV – Describe your Job Description at GIAC University of the State (GUS)

I am one of the Network Security Engineers for NSS with a salary of $84,500 for NSS (Networking Specialist Band: salary band range - $45,000 - $95,000)[4]. The NSS team reports to the Manager of NSS who reports to the Director of NTC.

For my role, I have two primary responsibilities. First, I provide network security engineering services and support to the University. This includes the management and control of the firewalls and the intrusion detection systems. This requires approximately 70% of my time. Secondly, I work as the primary network security liaison to other UMIS IT organizations, campus entities/offices, and other business partners for the University. This is similar to a consultant. This requires about 30% of my time.

My daily activities include: assisting the University management team in planning, organizing, implementing, and executing a network security infrastructure; the design and development of system/network security plans, security architectures, diagrams, and recovery test plans; reviewing system audit records and intrusion detection data to assist in the incident response effort; assessing adequacy of security controls and procedures; assisting in the development of policies, procedures, standards, and instructions on network security activities; coordinating and facilitating the resolution of network security related issues; interpreting and providing guidance/assistance on local and federal regulations and policies; teaming with other college and University personnel to identify and address network related security improvement areas; and helping University leadership and their staffs in accomplishing their security responsibilities.

State Auditors and University Internal Auditors ensure compliance with established policies, rules, regulations, and best practices by auditing our group annually. My success or failure is determined by my ability to anticipate and pro-actively address network security related issues and findings. My group's motto is: "Find it before they do, or find a new job!"

My secondary area is as the primary network security liaison to other UMIS IT organizations. This role involves consultation and recommendation of network security solutions to the University IT Committee (UITC). Many times this includes conducting training sessions to the University population on basic information security guidelines and procedures. My ability to interact with these groups is crucial. I am evaluated twice a year through team evaluations, customer/peer surveys, and management observation.

Part V – How does GIAC University of the State conduct its business?

The NSS team divides their work into two major categories of requests. Category one is comprised of services that are initiated by customer requests. These are typically for new firewall implementations (to include management or control of firewalls and remote access services), anti-virus support and installation requirements, and network security consulting services. The second category is comprised of security related implementations that are initiated by strategic security infrastructure changes, security services that are discovered due to some security compromise or deficiency, and others.

Requests are typically generated through the GUS Remedy [(5)] (Help Desk Supporting) ticketing system and initiated from the University help desk. Any request for work regardless of how it is made to the NSS team is eventually placed into the remedy ticket system to track information such as requestor, requirements, workflow progression, sponsor, and dependencies.

The process is as follows:

1. Calls are taken by the University Help Desk, which falls under CAS.
2. From there, if the request is network related the ticket is forwarded to the NTC Help Desk. The NSS staff, to ensure proper tracking of requirements, may generate a ticket for themselves, or by contacting the NTC Help Desk.
3. At this point, depending on the type of request (customer work or security trouble call), a ticket will be generated. Customer requests for security services (category one) are placed in a security cue and the "on-call" NSS specialist will review the ticket and forward it or work it as required. Security tickets that are generated due to a trouble issue (category two) are received by the "on-call" NSS specialist and worked to resolution. Should the call require additional resources the NSS manager determines the significance of the trouble call and the work required to resolve.
4. Request calls (category one) are reviewed and matched against the following requirements:
    a. What is the business requirement? And, who is the business sponsor?
    b. Does the request contradict a current established security policy, rule or regulation?
    c. What is the business impact if the request is not approved?
    d. Are there current implementations that could support this request?

Any services that require the IDS are only implemented based on network observations by the NSS team and the manager. This is not a service that is provided to the University for normal functions.

Part VI – What applications and/or what type of access are required to carry out these business operations?

The staff and students connect to one or more systems and applications on the University network to send or received data via their PCs and/or multi-users systems (such as computer lab computers). There are a number of applications that the students, faculty and administrative staff require access to. They are divided between the two primary functions. Student based applications and faculty/staff based applications.

Faculty members and administrative staff employees (here after both groups will be referred to as "Staff") use University provided equipment to connect to the network and applications. In some instances, staff members may have access to internal applications from an external non-University PC by means of a VPN connection.

However, most internal communications are handled through the GUS LAN. Depending on the college or department (many times just the colleges), a user may also have a separate LAN not connected to the University network for specific work related to research and grant related projects. Because these networks are not connected to the University network the UMIS IT division is not responsible to support and manage those systems.

That doesn't remove the threat from those systems though. We have annual training programs for security that address concerns with "sneaker" transfer of data from one system to another.

Student services and systems are primarily accessed by systems that are segmented from the University network. Students have access through the University network to the Internet via the StuNet connection. This service is provide free of charge to the students. The primary purpose for this allowance to the students is to provide them an available means to have access to University web resources designed for the students. For example, access to on–line classroom assignments, calendars, and other student class data. GUS also provides students with a free email service but does not ensure it's confidentially, availability, or integrity of the messages.

Staff members also have access to "business" provided email. This is how the primary work communications flow at GUS. Email is considered a critical application/service. Depending on the type of work required (administrative staff versus faculty) the average employee would also require access to HR and Financial data. This requirement is for processing of requests and/or performing data input (e.g., pay, benefits)

There are a number of remote solutions that staff members and students of the University use. Staff members use remote access services from home such as Web Citrix or web based email. Remote access is available to all GUS faculty and staff. Before access is granted though, each user must comply with a remote access agreement.

Typically Universities are open networks, especially state run organizations. As the threat from external sources increased, it was decided that aspects of the University required protection. As such the remote services required access by flexible and innovated means. GUS provides campus network services via two remote access methods, WebCitrix and Cisco VPN clients. This is separate from the remote network solutions provide by the Check Point firewall appliances for remote offices.

A VPN software client is required to access the secure campus resources. GUS provides this client for home PCs and University provided equipment (such as desktops and notebooks). The VPN client requires a username and password to verify the staff member's identity. Once the user's identity has been verified, the VPN Client connects the remote system to the network. The University provides the VPN client for free.

Student remote access services are provided via the Internet through the University network for access to the student academic services. These remote services are primarily for access to student-based applications, such as class work and materials.

As stated earlier, the staff members and students of GUS have access to email as well. The staff is provided work email through the use of Microsoft Exchange. They also have the ability to access email from home via the VPN solution or via the Outlook Web Access (OWA) for Microsoft. This provides a 24/7 access to email. Additionally, all staff members are authorized to access the Internet and each system (unless there is a specific security or internal department requirements that prohibits it) has a network connection that support Internet access.

Students are provided Internet access by means of the StuNet. It is a student residential computer network provided to students living at the University. StuNet lets students connect their computers to University's computer network to the Internet.

The University provides anti-virus software free of charge to the students and highly suggests its installation for access to the StuNet. However, at this time it is not mandatory that the systems on StuNet install and update their anti-virus software.

Part VII – Identify three "crown jewels" your office has access to and is responsible for.

As with any organization there are many aspects of the business that can be considered “crown jewels.” GUS has identified the following as their crown jewels: Student data (resides on the University Mainframe), staff and faculty personal data (such as Human Resource (HR) and Financial (FIN) data) (resides on Sybase [6] servers), and the Email systems for GUS (exchange servers).

Members of the administrative offices as well as members of the Student Administrative Development team access student information on the mainframe. Students do not have direct access to any of this data.

Access to this data is tightly controlled and monitored. Before any member of the University can have access to University data (regardless of type) they must first sign a compliance statement that reminds them of their obligation to protect data. This is a mandatory process and the Access Control Security Team (ACST) group for the University must have this signed document before granting access.

Data stewards have been established for each “type” of data. Their associated Dean Vice-Chancellors must approve the data stewards in writing. The data stewards have the sole responsibility to approve access to data. This access request/granting process is accomplished via an internally developed application called, The Security Access Request Application (SARA).

SARA is mainly automated and uses a web interface for the request and a workflow processor to funnel the request through the channels. The immediate manager/supervisor must submit a request via SARA. This request is forwarded to the Data Steward who approves (with comments if needed) or disapproves the request.

The ACST then processes the request. The ACST is also the group that generates an annual report to the data stewards for review and certification of the University staff members who have access to their data. This report is signed by the data stewards and maintained for audit purposes by the AST.

Staff data that is considered personal/private or performance related and financial data (salary) is maintained on Sybase servers in the GUS Data Center. The data center is a protected building with 24/7 monitoring. During normal duty days a security guard force also mans the Data Center (DC1). After hours, weekends, and holidays, the DC1 operates with a staff of about of about 3 systems operators. They monitor the production jobs and batch jobs. The building is monitored with Close Circuit Television (CCTV) that is controlled by the campus police. The campus police also make two checks per day during after hours and 3 times during weekends and holidays.

The Sybase servers have a very restrictive access control list and access directly to the server is logged and monitored. Access to data on the server is the same as explained above.

Personal information for the students (e.g., student applications, grades, financial information) is considered part of the student related data side of the University and is maintained on the mainframe. There are separate laws or acts that regulate and protect each type of data. For example, the Family Educational Rights and Privacy Act (FERPA) [(7)], provides guidance and direction on what student data may or may not be released without proper consent.

The email system is also maintained in the GUS DC1. Access to these systems is restricted to the exchange administrators. Although the email servers are also located in the DC1 they are segmented by a firewall from the rest of the systems listed above. The exchange servers are architected to provide for redundant and failover operations.

The NSS has data that is also considered important and in some stances a "crown jewel." That is that data that comprises the firewall rule-base for the distributed firewalls. The architecture for our firewall design is comprised of three systems. They are the firewall appliances it's self, the management server, and the desktop systems with the firewall client that accesses the firewalls.

Access to the rule-base on the management servers is protected with full auditing and logging. Additionally, the management server is configured to only allow access by specific systems (Access Control Lists). This access is configured to accept only access based on correct user credentials and by specific IP addresses. The rule-base is also backed up every time a change is made to the firewall. This is also to ensure that in the event after a change is made something goes wrong, the firewall administrator can easily revert back to the last good installation.

Part VIII – Insider threat vector for each of your office's crown jewels.

The threat from inside is always considered a very likely and a somewhat less than complicated issue (depending on the significance of the compromise). The reason that insider threat is consider more probable, is that the protective measures that are put in place to prevent the outsider threat are sometimes not implemented or reduced with respect to insiders. As outlined in the second edition of the Information Systems Security Officer's Guide [Establishing and Managing and Information Protection Program] [(8)],

> "People are the driving force behind it all, and it is people as threat agents that the Information Systems Security Officer (ISSO) must always take

into account when building a Corporate Information Assets Protection Program (CIAPP)."

Access to the student data on the mainframe is slightly more secured than most. The fact is that it usually takes a more skilled level of user to manipulate the tools to gain access to the data. This old belief is somewhat antiquated now due to the introduction of web based applications that open the data up to more and more users. The simple rule is anything that can compromise the web can now compromise a mainframe for access to the data. These can include but are not limited to sniffing of sessions, key loggers, and Trojan horses.

The methods to gain access to the mainframe are very similar to gaining access to any other system. (e.g., social engineering, compromised credentials) However, with more and more web-based applications gaining access to data on the mainframe there is more and more a potential of compromise with the data.

The threat of access of the Sybase servers is reduced due to control measures put in place to limit the users that have availability to them. This access is through three areas. First, users must be granted access by the data stewards and those users must be given accounts to those servers. Secondly, the servers are protected from the rest of the network by at firewall. Finally, auditing and logging has been turned on for the servers.

These measures provide a significant deterrent for would be attackers. However, the threat from internal attackers could easily circumvent these security measures. The motivation to gain access to this data speaks for its self. The data contained on the Sybase servers is the HR and FIN data. With this data you have account numbers for banks for direct deposits. There is personal information such as social security numbers, addresses, and birth dates.

For the HR systems someone could access the semi-annual evaluations. This could cause for some embarrassing situations depending on the content of the evaluations. Also, any pending actions that may be taken against a person could be accessed here as well. The motivator behind this is that this data could be used to embarrass or extort someone for personal for financial gain.

Gaining access with out have the account information is not as easy as some might think. With the above-mentioned security measures there are enough levels of protection to limit the possibility. However, should someone truly want or desire access, they could get this through a number of means.

One possible way is by social engineering. If a user were to contact the help desk and request a password change and the proper procedures were not followed to authenticate the user. Then an attacker, specifically an internal user, could gain access to the servers and the respective data.

Another way is through “shoulder surfing” over a user that is authorized to have access to the servers. Many times users forget that when logging into a protected systems they should not allow others to see there id and password being typed in. The issue here is that many users feel uncomfortable with telling fellow employees not look the other way or to try and protect they log in by turning away. The “You are to paranoid” mentality comes to mind when users attempt to do this.

With respect to the rule base, the one potential weak area is the access that is configured for the PCs that manage the firewall management server. There are two levels of protection for access to the rule-base. First the administrator must use the client with proper log on credentials to access the management server. The second level is that only certain systems (via IP) are authorized to access the management servers.

If the PC is not configured to implement a password protected screen saver, there is a window of opportunity that may allow someone that is not a firewall administrator to access the rule base. For this to happen the authorized administrator would have to have the client opened and accessing the Management server. Then they would need to leave the system unattended.

If these steps are taken then a user may have gain access to the server and manipulate the rule-base. The primary motivator for the action could be for any number of reasons. If the rule-base was copied then someone could have intimate knowledge of the infrastructure.

If the rule-base was manipulated there could be catastrophic repercussions to the production environment. With this approach significant public relations issues could result.

Part IX – Outsider threat vector for one of your office's crown jewels.

The reduction in the threat from out side the University of the theft of student data is considered a high priority for GUS. This data is considered important not only because of FERPA, but because of the increasing concern over personal information (Identity theft) being released, copied, or used. GUS considers student identity theft important not only because of FERPA but from a public relations standpoint as well.

As outlined in FERPA and due to the fact that students attending GUS are considered “eligible students,” GUS implemented a written policy to all employees, who have access to student data, that they must sign a memorandum stating they understand their role and responsibility in protecting student data. Annually, each employee must attend training on the rights of students attending the University.

(Note: eligible students are those students which by virtue of their age and attendance at GUS assume the same level of responsibility and right to dictate the release of their data that their parents had when they attended high school.)

After an assessment of the current procedures employees use that handle student data, it was discovered that there were no checks-and-balances put in place to monitor the release of student data. One potential means by which someone external to the University could gain access to student data is by means of social engineering or an out right conspiracy (personal financial gain) by a current employee to release student data.

The motivation to gain access to this data may be driven by two primary areas, identity theft of student data or extortion of the student based on the information released. A perpetrator may gain access to this data by means of social engineering. An unsuspecting employee, that has access to student data, may be thinking they are assisting a parent and provide data to the person.

There could also be an issue with an employee that is attempting to gain personal financial growth by providing this information to criminals. The term criminal could be as simply or sophisticated as one's imagination. Their criminal activity could be the extortion of a student by means of releasing the data to parents. Although this concept may seem unusual to most, there are many students that consider the release of this data to parents of the utmost importance.

In light of this concern, GUS also implemented a policy where by weekly audits of release student data are completed by management. Any discrepancies are immediately noted and addressed.

Part X – Malicious code threat vector for one of your office's crown jewels.

With the many measures GUS has taken to secure it's environment, one if it's greatest weaknesses is the fact that their anti-virus program is not a required implementation. Additionally the fact that GUS has allowed some of the older operating systems (e.g., Microsoft 95/98) to remain in operation on the campus network allows the threat of malicious codes to be varied. The GUS email system is highly susceptible to the threat of malicious code.

There is a mindset with in the University that "mandating" is a bad thing and GUS has a policy that allows for the incidental personal use of University provided resources. These two issues are the primary reason GUS has not fully implemented a University wide mandatory anti-virus usage program. The feeling here is that the University is here to provide and share information. Because of this openness in communications the threat is compounded with issues related to

attachments within the Email system. So, whenever there is a major outbreak of some type, the IT staff ends up being mainly reactive instead of proactive.

The mass-mailing worm "W32.Netsky.D@mm" (here after referred to as Netsky) [(9)] is one such malicious code that could cause significant heartache to the GUS mailing environment. As described by Symantec, "W32.Netsky.D@mm is a mass-mailing worm that is a variant of W32.Netsky.C@mm. The worm scans drives C through Z for email addresses and sends itself to those that are found."

The potential threat to GUS that Netsky can cause is from the fact it works on the vulnerability of social engineering to encourage users to open the attachments that are sent via email. Social engineering is one to the toughest avenues-of-approach to protect against. When appropriate technical security measures are not implemented or adhered to, social engineering will inevitably win in its battle to compromise a system.

Because Netsky can and will change the makeup of the subject line in emails as well as the information contained within the body of the email and the attachments, it difficult to ensure that users don't open attachments. It is this approach (social engineering) coupled with the fact that the anti-virus program is not mandatory that makes GUS susceptible to these types of attacks.

Part XI – Identify the most severe threat.

There are a number of threats looming over GUS. One threat that appears to stick out over others is the potential compromise and/or adverse reaction to newer applications (the production environment) from the older legacy systems (older operating systems) that the University allows on the network. This is especially a significant problem in the administrative financial offices.

As the world of newer and faster web based applications continues to grow, GUS has a reoccurring and time consuming role in developing, testing, and putting into production applications that support the business of the University. This vary diverse environment creates a decrease in supportability while increasing the potential over looking of a vulnerability.

The Financial offices continue to use older operating systems that have meet end-of-life support. The potential for loss of production time/effort and data increases as the months go on. Additionally, the ability for the older systems to interface properly with newer applications without some personal TLC (Technical Loving from Coding) increases the potential for adverse reactions to expected results.

The potential damage from the unintentional loss of data or production time can be severe. Many of the legacy systems have been allowed to interface with or have been provided feeds from systems where the data is considered to be

confidential, proprietary, or personal. This data, manipulated with systems that are no longer supported can potentially be lost or compromised with very little effort.

Part XII – Recommend a remediation strategy for one of the threat vectors you have described.

For the Financial systems the recommended remediation strategy to address one of the threats considered most severe to the University is to take the legacy systems and replace them with newer "supported" operating systems. This recommendation should eventually be implemented across campus but the scope of that would entail buy in by not only the business side of the University but the separate colleges.

The aspect of getting this approval would be significant and well out of the area of responsibility for the IT department at this time. Although UMIS supports that IT environment for all of GUS, it is an excepted and understood issue that the University is separated into two organizations. Those organizations are the business related or administrative systems and the "school" side of the university.

It is estimated that this remediation strategy will take approximately 2 months to complete. The implementation steps required will be to as follows -

Step one will be to define the job in detail. This will include the resources required and the estimated time to complete the project. In defining the project and detailing the resources needed we will require management approval and support for the project. [Estimated time for step = 30 days.]

> Step two will be to gain commitment for the appropriate IT staff section to purchase, test, and install the systems and supported applications. [Estimated time for step = 2 – 3 weeks.]
>
> Step three will be to develop a completed project plan listing the tasks and resources for each task. Part of this will be to also set up change procedure to formally request changes to the project schedule. [Estimated time for step = 2 – 3 weeks.]
>
> Step four will be the final implementation or the "roll out" phase of the project. This implementation phase will take approximately 3 – 4 four weeks to complete. The time estimated is for the slow implementation of 3 – 4 systems per week. This latency is because of the concern over lost production time over the change out of systems.

The resources required to complete the project will be the purchasing group to purchase the equipment needed to replace the legacy systems. Additionally, the desktop support group will be required to change over the upgraded systems

with the legacy systems. It is estimated that 3 desktop support members will be required to complete the roll over.

There will need to be 13 desktop systems purchased to replace the 11 systems currently in use. The additional 2 systems will be used for support of systems problems after the roll out. Current site licenses for newer operating systems are covered so no additional licenses will be required.

The 13 financial systems that must be replaced (including the desktop systems and associated peripherals) will cost about $1,300.00 per system for a total of $15,600.00. The estimated man-hours required to complete this project is, $55.00 per hour per FTE. It is estimated that it will take approximately 50 man-hours to complete the project for at total of $8,250.00.

The grand total for the recommended strategy is $15,600.00 + $8,250.00 = $23,850.00.

Part XIII – Review the backup strategy.

As the University has progressed from an educational and a technological standpoint, there are many aspects of the University that seemed to be antiquated. This was made evident during a recent assessment of the current backup strategy. While data on the networked systems is backed up, data this is saved on the local drives for many of the systems is not backed up.

The current University policy is that users only store data on networked servers and not locally. Unfortunately there are a number of experienced University employees that have chosen to over look this requirement.

As such, the recommended strategy is to automate the backup approach so that all data is at least secured monthly. To ensure that we have a plan that will allow not only a sufficient backup approach but also a recovery option that allows for quick return to normal operations; the recommendation is to use a third party vendor that supports off site and automated backup option. The plan is to implement a client-server based and near real-time backup strategy for all the PCs in our office.

Due to production requirements, the automated approach will separate the total of all the systems into two groups. Each group will undergo a full backup every two weeks and an incremental backup every two weeks (e.g., group A will be fully backed up on the first week and incrementally backed up on the third week. Group B will be fully backed up on the second and incrementally backed up on the forth week.)

This approach should ensure that all systems are backed up fully every month.

I am recommending the Storactive "LiveBackup: Reliable Backup for PCs & Laptops", solution [10]. This vendor supports the backup approach required to effectively do what we need. As per their web site the following software and hardware specifications are needed:
(The following is a snippet for the specifications from their web site [10].)

LiveBackup Minimum System Requirements

LiveBackup 2.73 Client

- Windows 95 OSR2, Windows 98, Windows ME, Windows NT 4.0 SP5 (or higher), Windows 2000 Professional, or Windows XP
- Intel Pentium ® Processor or higher or AMD Athlon ® Processor or higher
- 64 MB RAM (128MB recommended for Windows 2000/XP)
- 100 MB Free Disk Space (500 MB+ recommended)*
- Internet Explorer 5.01 or later + TCP/IP

LiveBackup 2.73 Server

- Windows 2000 Server or Advanced Server with Service Pack 2 or Windows Server 2003 Standard or Enterprise Edition
- Intel Pentium Pro Processor or higher, or AMD Athlon Processor or higher
- 512 MB RAM
- Microsoft SQL Server 2000 Standard Edition with Service Pack 3a
- At least 5 GB free disk space* + TCP/IP
- Internet Explorer 5.01 or higher

LiveArchive 2.73

- Windows 2000/2003 Server
- 128 MB RAM
- Intel Pentium Pro Processor or higher, or AMD Athlon Processor or higher
- 250 MB Free Disk Space*
- Microsoft RSM-Compatible Tape Device or Library (recommended)
- ActiveDirectory or NT Domain Networking

The approach recommended above will dump data to tapes and the tapes will be moved once per week to a secure vault. The vault is located on the southern campus. This is about 5 miles from the data center on campus where the data is being loaded to the backup servers.

The primary purpose for having the tapes couriered to a secure vault is for two reasons. As explained in the Information Security Management Handbook, 4th

Edition, those reasons are, “Off-site storage of backups is a strong defense against two serious threats, physical theft and natural disaster.” (11)

The estimated costs for the recommendation is:

Item	Estimated Cost
Equipment (Servers)	$11,000
Software	$25,000
Man-hours (2 FTEs X 80 hours)	$12,000
Total:	$48,000

Part XIV – Review offsite backups

Although the tapes are located in a secure vault, the vault is only located 5 miles from the DC1. This is not recognized as a safe distance from the data center to ensure ample protection in the event of a regional or University wide disaster. As such, the recommendation is to that the tapes couriered to an off-site location that is at least 20 miles away.

There are a number of tasks that must be completed to ensure this happens. To get the recommendation to move forward GUS will need to evaluate the current backup procedure to see what will be the total courier requirement that will be needed to meet the remote or off-site backup necessity.

The tasks that considered “repeating” in nature are those tasks that ensure the confidentially, integrity, and availability of the tapes. The continued process of evaluation and review of the procedures for the backup and the goal or objective of the requirements must be reviewed at least annually.

The confidentiality safeguards that are needed will primarily be from a service level agreement (SLA) type procedure. In this instance, confidentiality refers to our ability to ensure that the data that resides on the tapes is protected from unauthorized individuals. There are technical/man-made measures that can be taken as well as procedural or management steps that can be implemented.

The University and the vendor will need to agree to certain access controls and data compromise steps prior to the shipment of tapes for backup storage. For example, contractual agreements must be signed and enforced that obligate the vendor to protect and ensure its employees protect our data.

The technical or procedural measures that must be taken are things such as an access control roster that lists the only members allowed to add, remove, or release tapes.

To ensure the integrity of the tapes, they must be locked in secure containers that are checked before release to the courier and after return to the data center operations teams. The vendor should have no reason to access the data on the tapes. This being said, the tapes should be maintained in secure containers that only the operations staff has access to. As part of the semi-annual audit at the vendor location, the containers must be examined. Any observable compromise of the containers must be handled immediately.

To ensure that tapes are available for recovery when needed the vendor must agree to 24/7 availability. This availability must be allowed to support immediate or "as required" recovery operations that are required for the BCP. The availability of the tapes is a must or regardless of the integrity of the tapes we will be unavailable to recover.

GUS must have availability through a courier, direct site visit or automated measures if supported.

The audit will take place with internal procedures on a weekly basis. This will be to ensure that the tapes removed and sent for backup are the expected tapes. One issue with tape backup is thinking you have the proper tapes for recovery online to find out that the tapes are not the proper tapes or corrupted.

A 100% audit of the vendor site should take place at least every 180 days. One of the audits can be held during the annual Disaster Recovery test. This audit should ensure that the tapes being held in the off-site location are the tapes that are expected and that they are available for recovery operations.

Part XV – Devise a guerilla business continuity plan

The opportunity to develop a business continuity plan (BCP) where one doesn't exist is a difficult task to say the least. After a little research and homework, I discovered that the "Disaster Recovery Journal," web site offered a wealth of information in developing a BCP [(12)].

In developing this plan I needed to fully understand the concept of a BCP and what the scope would be. Ideally, any BCP will identify resources required to fulfill obligations of recovery. Additionally, it should include the actions and procedures in a well-documented format so that any competent technology person should be able to recovery systems.

This documentation should include the procedures and information that has been designed and tested. It should ensure that the above-mentioned procedures are

held in a state of readiness for use in the event of a major disruption of normal business operations. This disruption could be from the introduction of an unknown event of even a planned event that is expected to disrupt the normal flow.

As with any project it is considered effective if it can be divided into phases. This approach tends to lesson the over all impact to resources required to completely design and implement the BCP. As phased approach also allows for adjustments to the project (financially, scope, resource) in the event obstacles or opportunities impact the final deliverable.

Some of the necessary one-time tasks required are developed once an understanding of the plans ultimate objective is outlined. Developed out of the understanding of the objective will come a litany of assumptions due to the diverse environment any IT infrastructure can pose.

Ideally we need to list the project scope and estimated cost. The initial design phase will help to clearly document this. This initial design and cost will need to be processed through the project sponsors for their review and ultimately full support. With out this support from the Vice Provost level management staff, no plan worth it's weight will be successful.

In the University environment, many projects are reviewed and developed through the administration of a committee. For GUS, a Business Continuity Planning and Disaster Recovery Oversight Committee will need to be established to track and review the progress of the project. Also, they will have authority to authorize spending and project phase implementation.

This committee's responsibility will be to assist with the gathering of information, review of additional options, and ultimately the decisions to implement the BCP.

To establish a base line of the current status of the University, a complete IT risk assessment must be accomplished. This risk assessment will provide valuable information as to what is the current IT infrastructure can accomplish in the event of a business interruption. A Business Impact Analysis (BIA) will provide information on critical business activities, the business process owner, and the impact of a business interruption on such things as public relations, financial loss, and significant of certain business activities versus the significance of the threat/event.

Once the phases that move the project to the implementation phase are completed there will be a number of repeating tasks that will need to be accomplished. Procedures that outline the responses to emergency events will need to be reviewed and updated on at least an annual basis.

There must be a bridge between the response that is expected during an event and the required recovery operations. This bridge is must be reviewed regularly or when major procedures, process, systems, or applications change. In line with this should be an annual review of any vendor contacts and Service Level Agreements (SLA).

As explained on the Disaster Recovery Journal web site, once many of the previous phases are complete, the "TESTING and EXERCISING PHASE," will be implemented. This approach will ensure that the previous phases have been designed properly and executed appropriately [(12)].

The testing and exercising phase will include such tasks as; "a. Exercise Program and Objectives, b. Exercise Plans, Scenarios and Actual Exercises, c. Plan (Exercise) Evaluation, and d. Training, Corporate Awareness Program(s) and Vehicles for Dissemination." [(12)] These tasks will provide GUS the ability to audit the overall project to ensure it is successful.

The above outlined approach should allow for a full-scale implementation for the entire GUS UMIS IT operations. By allowing for a phased project and a continually review of the successful and unsuccessful tasks outlined in the project plan, GUS IT teams will be able to ensure that the BCP will be rolled out to completion.

Resources

1. http://www.cisco.com/en/US/products/hw/routers/ps352/index.html

2. http://www.checkpoint.com/products/firewall-1/index.html

3. http://www.citrix.com/

4. http://www.osp.state.nc.us/salschd/2004/careerbandedpayplan.pdf

5. http://www.remedy.com/solutions/servicemgmt/help_desk.htm

6. http://www.sybase.com/products

7. http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html

8. Kovacich, Dr. Gerald L. Information Systems Security Officer's Guide, Establishing and Managing an Information Protection Program, 2nd Edition, Burlington, MA: 2003. pg. 48.

9. http://securityresponse.symantec.com/avcenter/venc/data/w32.netsky.d@mm.html

10. http://www.storactive.com/solutions/liveBackup/systemRequirements.asp

11. Tipton, Harold F. & Krause, Micki, Information Security Management Handbook, 4th Edition, Boca Raton: Auerbach, 2000. 512.

12. http://www.drj.com/new2dr/model/bcmodel.htm