Creating a secure IT network for a small, non-profit organization

By Jay Johnson
Lewis University

May 5, 2007

Table of Contents

Introduction

The Valley of Chicago learning center for children with dyslexia is a non-profit educational center located in LaGrange, Illinois. The center requested the assistance of an IT consultant to setup and configure a computer tutoring network to provide computer aided instruction to their students and to assist their tutors. They received a special budget to purchase four desktop computers and a server as well as a server-based tutoring software application. This project describes the security considerations for the computer network implementation, as well as the integration with and improvement of their existing computer infrastructure and the development of an effective security program to meet these needs.

The approach used for this project was to follow best practices for IT security project management and effective IT security program implementation and first create a risk assessment and then apply appropriate security controls to mitigate the risks of operating such as computer network. First, appropriate policies and procedures were created to govern the use and operation of the computer network, and to make sure that these policies and procedures are followed and agreed to before access is granted. Management would sign off on these policies and procedures first. Physical security was then analyzed, and technical controls were applied to the network as well as the server and the desktop computers and specific applications. Then, appropriate security training was created and distributed to both tutors and students, and tools to assist in periodic auditing were developed. Also, an incident response and disaster recovery plan for the system was developed. At all stages of the project, appropriate documentation was provided, so that the system and security plan is easy to understand and manage.

Review of Literature

Few studies have been done regarding the application of appropriate Information Technology security controls to non-profit organizations such as this center. A recent survey showed that although computers were central to nonprofit organizations, only about half of these groups backed up data daily, and about a third had a plan to recover data [1]. Also, only four percent of these organizations encrypted sensitive files, although two thirds of such organizations stored sensitive files on network attached computers, and 25% of these organizations did not have a policy to lock or shutdown computers when not in use.

In Information Security, the CIA triangle is used to describe the three goals of information security. The three elements of the triangle include Data Confidentiality, so that private information remains private and prevents unauthorized access of the information, Data Integrity, which means that the information remains complete and unmodified, and so its origin can be trusted, and Data Availability, which means that the information can be accessed without delay or interruption, and that it can be retrieved when needed [2]. The primary goal of the security plan established for the center is to maintain the confidentiality, integrity, and availability of the information.

An effective security program will include education, training, and awareness to everyone, including end users, administrators, managers, and senior management [3]. Before developing a specific security strategy to meet the needs of the particular organization, a risk assessment must be done so that risks can be identified and so management can understand the risks, prioritize the risks and decide how to best allocate available resources mitigate them. Unfortunately, according to a recent survey, only 30% of higher education institutions have conducted a risk assessment. For smaller educational organizations, the number would probably be much smaller. The risk assessment should take into account the magnitude of the harm that could result from the unauthorized use of information systems, and should be used to develop appropriate policies, operational procedures, and technical controls that will cost-effectively reduce these risks to acceptable levels, creating a security plan to provide adequate security for the IT infrastructure in the organization [4]. In addition, security awareness training, which includes the risks associated with normal business operations, and the responsibilities of the employees in following the rules and procedures that will reduce these risks, will be developed. An effective security program will periodically test and evaluate the effectiveness of these security policies, procedures, practices, and controls, will address remedial actions identified to correct deficiencies discovered, will detect and respond appropriately to security incidents, and will plan for continuity of operations in these computer systems. The project plan that was used follows the best practices of both IT security project management as well as the best practices of developing a good information security program, while tailored to the specific needs of the non-profit organization.

The IT security project management process is used to accomplish a specific effort, such as implementing a new secure computer network. It involves first getting a meeting of affected stakeholders in the project to define the project objectives, goals, deadlines, and budget in order to create a project plan, with defined goals and objectives, specifying how the tasks or goals are achieved, and what resources may be needed, including budgets and completion timelines. The project plan is monitored during the course of the project to make sure that appropriate priorities are being followed and that the project doesn't fall off course. It also shows what tasks must be done ahead of other tasks, to assist in better management of limited resources, including time and effort. Each project has several phases, including planning, implementation, evaluation, and support/maintenance [5].

There are also legal considerations when setting up a computer network that is being used by children. The Children's Internet Protection Act of 2000 requires schools and libraries that receive federal technology funds to install pornography blocking software on their computers [6]. However, this center does not fall under that act, since it does not receive any federal or public funds. Such a filter should be mandatory on ANY computers used by children with access to the Internet. In the center, the students' computers did not have an Internet connection, making such a filter unnecessary at the present time.

Procedures Followed

Initial Project Planning

The start of this project began with a meeting of all the affected stakeholders of the tutoring center. This meeting included the author, the director of the center, a few members of the center's board of directors, and some of the senior and most computer literate tutors from the center. This mix of people from various roles in the organization helped to give various perspectives and identify the requirements and concerns for the project early on. Too often, projects are started without clearly identifying the requirements of the project, as well as identifying cultural attitudes of the organization that may affect the effective implementation of a security related project or program.

Security projects often fail due to being heavy on the "technology" while neglecting the policies and educational training necessary to successfully implement the project in the organization. It is important when implementing IT security projects that there is staff buy-in and that the management is totally supportive of the changes that may be required. Successful IT security project implementations often need someone high up in the organization to serve as a "champion" for the cause, and give the project the attention and support from upper management that it deserves. Fortunately for this project, the newly appointed director of the tutoring center, Paula Conroy, was such a champion, and she fought for the project even when others were concerned that such a network could be manageable, cost effective, and secure.

Early on in these discussions, it was apparent that some of the board of directors for the center had serious concerns about computer security. Attacks from the Internet cost businesses $55 billion in damages in 2003 [7]. Since this tutoring center would be used by children, there were realistic concerns about the ability of the children to access inappropriate content on the Internet, as well as concerns about potential student misuse of the computer equipment and legal liability. They were assured that all of these concerns and risks would be taken into account and that appropriate risk mitigation strategies would be developed and implemented.

The main purpose of purchasing these computers was to be able to run the latest, server based versions of the Lexia suite of Dyslexia tutoring software. The vendor's website is: http://www.lexialearning.com. The startup screen for the software can be seen in figure 1. The software was purchased to provide tutoring for students of various ages, as well as software to test the current strengths and weaknesses and track progress of the students. Lexia can tailor custom lessons to each student's specific strengths and weaknesses. Whatever security plan was implemented needed to be able to accommodate running this software.

The budget for this project was estimated at about 10K. While this budget was deemed sufficient to purchase the hardware and software needed, it would not be sufficient to

purchase a great deal of additional system administration or security back-end infrastructure, so keeping the network as simple as possible while not sacrificing security

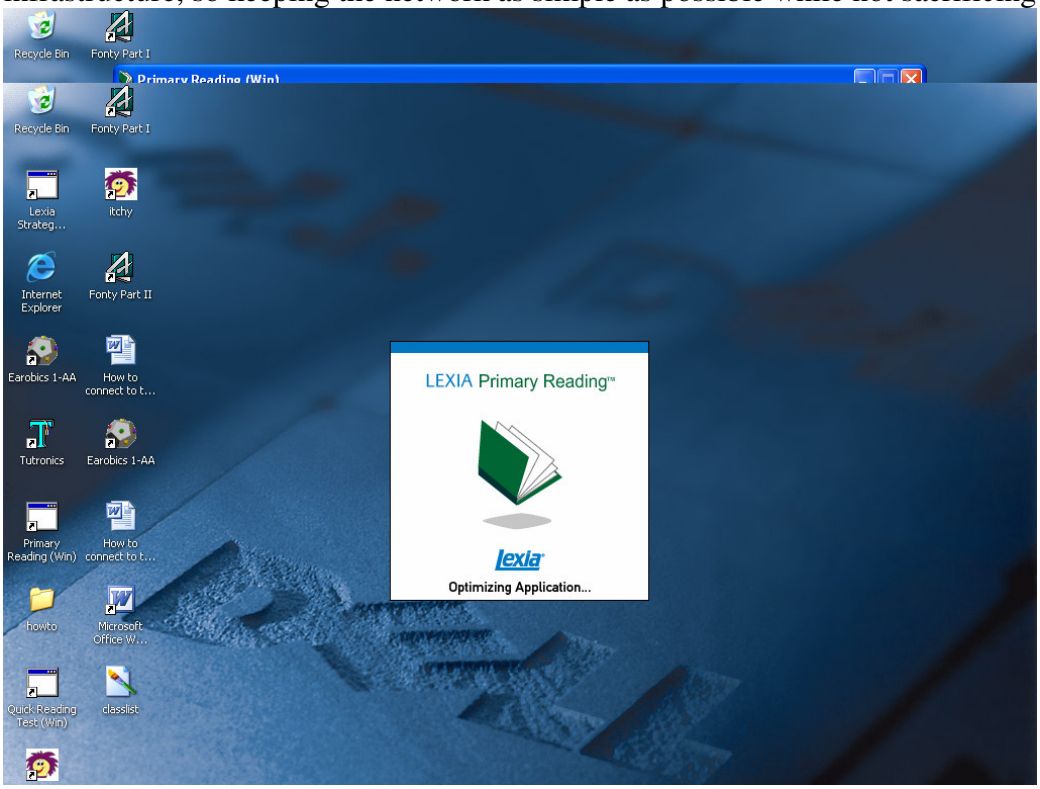


Figure 1: Startup of Lexia Primary Reading Network Application

was seen as a key consideration. The board of directors was concerned about the possible complexity of such a computer network. In the past, IT projects for the center had required hiring expensive consultants, who did not always deliver what they were promised, or who locked them into requiring their expensive services, and they were concerned with having to pay regular large amounts of money to an outside consultant or having to hire someone just to handle their computer problems and system management. They were assured that the network would be easy to manage as well as secure

Based on the initial meetings, it was possible to create a set of requirements for the tutoring center.

Requirements for Valley of Chicago Learning Center Network

Primary Use - The student computers need to be able to run the server-based Lexia Learning Software Application Suite (Quick Reading Test, Primary Reading Strategies, Strategies for older and adult students).

Security – The computer network should be protected from malicious or accidental actions of both students and employees of the center, as well as protection from outside attacks.

Safety – The computer network should prevent access to inappropriate content from student PCs.

Manageability – The computer network should run reliably without regular need for IT specialist intervention, and should be easy enough for students and tutors to use with minimal additional training.

Future flexibility – The computers should be flexible enough to be able to accommodate running other modern appropriate applications in the future.

Risk Assessment

Armed with the requirements identified for this project, a fairly generalized risk assessment was next completed which identified the security risks associated with the operation of such a computer network, along with mitigation strategies and residual risks. The risks and threats were identified and controls were put into place to mitigate these risks. Of course, even after applying management, operational, and technical controls to mitigate these risks, there is always residual risk. Residual risks were also identified, and were accepted by the center's management. The detailed Risk Assessment, along with mitigation controls and residual risks is listed in table 1.

Table 1: Security Risk Assessment for Valley of Chicago Learning Center Network

Risk	Mitigation Controls	Residual Risks	Residual Risk Approved by Management
Physical damage to computer or computer hardware failure	Gold 3 year Dell warranty, on site service	Short-term computer downtime	Yes – computers not necessary for daily tutoring
Unauthorized access or theft of private information on computers	Folder/file security controls, database stored on server only, separate database password configured, regular backups	Accounts may be compromised	Yes – two layers of authentication for critical database access
Server operating system/configuration failure	Documentation and media to rebuild/reinstall	Short-term computer downtime	yes -computers not necessary for daily tutoring
Desktop operating system failure	Documentation and media to rebuild/reinstall, other computers can be used	Short-term computer downtime	yes -computers not necessary for daily tutoring
Lexia software failure	Documentation, media, and backups to reinstall, other computers can be used	Short-term computer downtime	yes -computers not necessary for daily tutoring
Other application failure	Software to reinstall, other computers can be used	Short-term computer downtime	yes -computers not necessary for daily tutoring
Theft of computer	Locked offices, lockdown kit for laptops, server in locked closed inside office	Theft of computer despite security controls	Yes – insurance will support emergency replacement if

			needed
Loss of critical data	Regular backups performed	Backup failure/not done	Yes – small risk, data could be recreated, older backups will work
Unauthorized installation of software or unapproved computer setting changes	Group policy locks down desktop systems from configuration changes Students and staff not given administrative rights on PCs	Some software can be installed without administrative rights	Yes – can easily be detected, most not harmful, system can be rebuilt if needed
Unauthorized internet access by students	Student PCs on isolated network, no Internet access possible	Student could access Internet on staff PCs	Yes – students should not be unattended on staff PCs (policy)
Deliberate or accidental damage to computer OS or software by students	Group policy locks down desktop systems from configuration changes Students and staff not given administrative rights on PCs	Possibility to circumvent security controls	Yes – should be detected, systems can be rebuilt, use is supervised
Damage to critical network switches	Cheap and easy to replace	Short term network loss	yes -computers not necessary for daily tutoring
Damage to critical network router	Cheap and easy to replace	Short term Internet loss	Internet not required for tutoring software
Virus/Worm/Malware attack from Internet	Managed e-mail blocks malicious code Desktop anti-virus software up to date on all PCs with Internet access Users trained not to open suspicious files	Risk that system will become compromised despite security controls	Yes – documentation, software to rebuild compromised system
Unauthorized network connection from Wireless access point	Security settings implemented to make it difficult to infiltrate wireless network	Risk that hacker will get onto wireless network circumventing security controls	Yes - Sensitive data only transmitted on wired connections; Domain authentication for file access uses encryption
Problem requiring IT expertise to solve	Extensive documentation, manager training, stable, self-managing computer network	Risk that system will need IT assistance despite self-managing network	Yes – volunteer or paid help is available through multiple sources

Finally, the security controls that were put in place need to be periodically tested for effectiveness, and the security plan should be periodically reviewed and audited to make sure that it is still valid and to see if any revisions might be necessary.

Project Proposal

Based on the results of the risk assessment, as well as the identified requirements for the project, the project proposal listed below was submitted and signed off by the board of directors. This project proposal identified the deliverables, timetable, and the scope of work for the project.

I volunteer to provide computer consulting and research, installation and ongoing hardware, software, and network support for the Valley of Chicago Learning Center. I will gather all of your system requirements, research available options within your budget, and submit my purchase recommendations for your review, along with other options I've examined. I plan to have this done in the next few days. I will setup and configure these systems to meet your needs, while making them secure and easy to manage. I am willing to provide on site setup and ongoing support of these systems and the rest of your computer network until May of 2007 when I graduate. In addition to warranty support, I will provide suggested resources for additional computer support if needed after next May, and I will continue to be available after May 2007 to answer any questions that your group may have and offer technical suggestions.

I will set up everything so it is as easy to self-manage as possible. I will provide detailed documentation and training to staff on the use and support of these computer systems.

I am a certified computer networking and system administration professional with over nine years of experience working for Argonne National Laboratory. While at Argonne, I've been involved in desktop and server support, networking, and security. I've also worked at Fermilab and Lewis University. I also have a great deal of volunteer experience including setting up a computer network for Hurricane Victims for the PADS organization at the Tinley Park mental health center last fall. I have a Bachelor's degree in Computer Science from Lewis University, and am finishing up my Master's in Information Security also at Lewis.

Project Timetable:
October 2006: Meet with center staff, define objectives for project, do risk assessment
November 2006: Place orders for hardware and software
December 2006: Install and configure hardware and software for network
January 2007: Test network and work out bugs with software and operating system configuration
February-May 2007: Resolve any issues that develop and create necessary documentation for the network

Project Deliverables:
Working computer network with Lexia software operating according to needs of the students and tutors
Complete Documentation regarding configuration/setup of the network, use of the network, and recovery/repair of the network.

Hardware Purchasing

After researching a number of hardware vendors, it was decided to go with Dell hardware because they offered an excellent educational discount, yet were business class systems. Dell OptiPlex desktops and an entry level Dell PowerEdge server were purchased. See figures 2 and 3 for close up photos of these desktops. They all came with a three year hardware warranty. See table 2 for hardware specifications.

Windows XP professional was chosen as the desktop operating system, while Windows 2003 standard was chosen as the server operating system. This platform was chosen because it supports their desired software, has numerous features for security, yet is still easy to administer and use. The academic pricing made both operating systems a very affordable choice for the center, and the operating systems were able to be purchased as a bundle through Dell along with the computers as OEM software.

Table 2: New Computer Hardware Purchased

4 Dell OptiPlex GX520 Desktop Computers, Pentium D 820/2.8Ghz Dual Core Processors, 512MB RAM, 80GB hard drive, 17" flat panel monitor, USB keyboard & mouse, 16X DVD-ROM drive, 2 piece speakers, Integrated audio, Windows XP Professional, 3 year extended warranty, on-site response, Gold technical support
1 Dell PowerEdge 840 Server, Pentium D 915/2.8Ghz Dual Core Processor, 1 GB RAM, 2, 250GB hard drives, DVD-ROM drive, Add-in SAS5iR (SATA/SAS Controller) which supports 2 Hard Drives – RAID 1, Basic Enterprise Support: Business Hours (5X10), On-site, 3 year Extended warranty, Windows 2003 Standard Server
5 Copies Office 2007 Charity edition Licenses & 1 copy CD media
1 8 Port Netgear 10/100 Ethernet Switch
2 5 Port Netgear 10/100 Ethernet Switches
Lexia Learning Systems Lexia Software Suite Strategies
Cables to Go Category 5e Ethernet Cables, various 7ft, 15ft, 25ft, and 50ft cable lengths

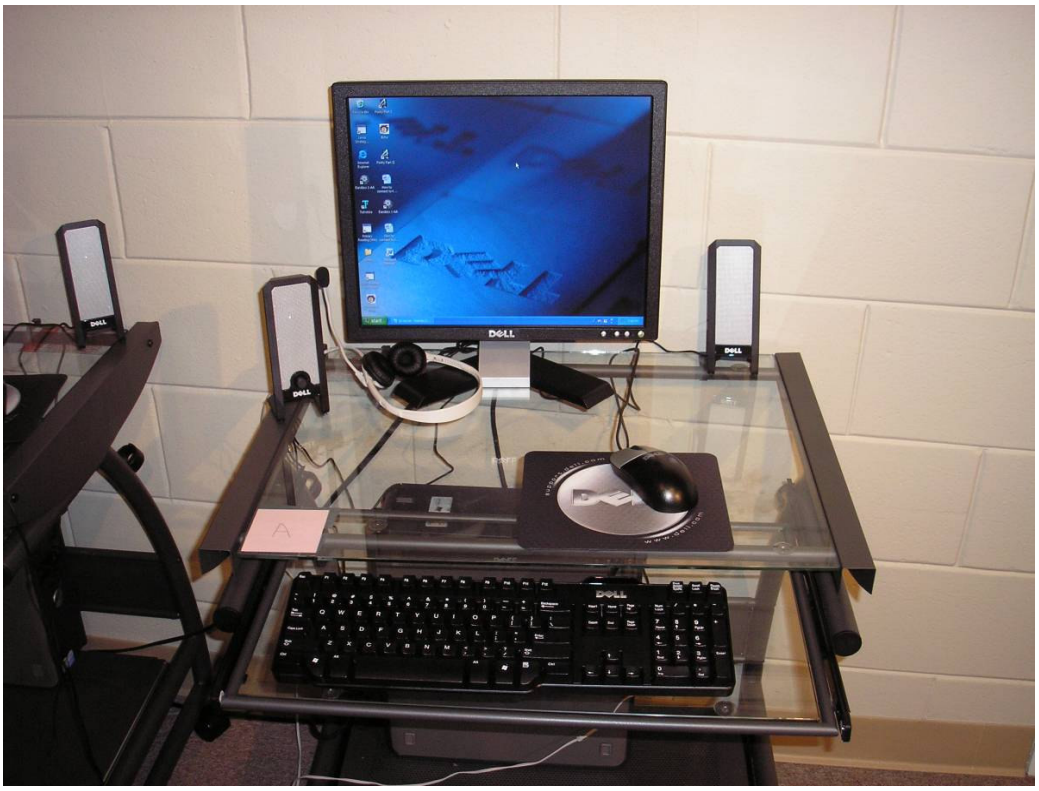


Figure 2: Student Workstation at Center

Figure 3: Close up of Student workstation CPU

Policies and Procedures

Acceptable Use Policy

An Acceptable Use Policy (AUP) is "a set of rules applied by network owners which restrict the ways the network may be used". They are written to reduce the potential for legal action that may be taken by a user [8]. They are considered key to an information security framework, and new users of a computer system should read, agree to, and sign an AUP before computer access is given. It should be clear and cover the most important points about what users can and can't do with the IT network within the organization. It should also specify what sanctions are enforced if the AUP is violated. Audits should be used to verify compliance with the AUP. As such, it protects both the owner of the network as well as the user, by defining security policies in place that both the user and the network managers agree to, thus becoming the first step in developing the security awareness program, as well as protection from legal liability. Tables 3 and 4 show the Computer Usage Policy and Parental Agreement used by the center.

Table 3: Valley of Chicago Learning Center Computer Usage Policy

Valley of Chicago Learning Center Computer Usage Policy

Computers are available to tutors and the children at the Valley of Chicago Learning Center. Our goal in providing this is to augment the children's tutoring with the latest and best computer software tools. The Center's computers are on a private network and have no access to the Internet. Access to these computers is a privilege, not a right. Usage of technology at the Valley of Chicago Learning Center is limit to the software installed by the Center. All users shall only use their assigned username and password. Usage will be monitored. Respect and care for the property of the Center is expected.

Parents/Guardians must sign the Acceptable Use Procedures Agreement form before your child is given access to the computers.

Table 4: Acceptable Computer Usage Parental Agreement

Acceptable Computer Usage Parental Agreement
I have read and understood the *Valley of Chicago Learning Center Acceptable Computer Use Policy*. I agree that my child, _____ will not have access to the Internet, and will only access the special tutoring software. He/she will only use their assigned username and password. My child, _____ will not attempt to load or download any files, and will use the computer appropriately. I will be responsible for any damage caused by my child. Date: _____ Child's Name: _____ Parent or Guardian Name (please print): _____ Parent or Guardian Signature: _____

Documented Procedures

Documented procedures were developed for everyone at the center that is using the computers, which includes various "how-to's" for various tasks on the system. Some example "how-to" documents have been included in the appendix. This documentation wherever possible includes extensive use of screen shots, in order to make them as easy to follow as possible. This use of documentation makes it easier for the administrators of the center to "self-manage" their computer network without the constant need for an IT security professional, and has the added security benefit of reducing the risk of accidental problems and misuse due to lack of information. These procedures were distributed to everyone at the center.

Physical Security

Theft was a serious concern identified in the risk assessment. The building and offices containing the computers were all kept locked when not in use, and most of the computers in the building were desktop PCs as opposed to laptops, making it somewhat harder to take since they were fairly bulky. There was one laptop used by the tutors for

one on one tutoring in the private tutoring rooms. It was determined that since this laptop was moved around so much, the tutor would keep it with them when they were using it, but for the times when it was not in use, a lockdown kit was purchased for it when it was set up in the tutor's tech room, which was its normal storage location, since this room was often open during working hours with lots of traffic.

Network Security

The center had previously installed Category 5 Ethernet cabling into all of the classrooms, and terminated them in a patch panel (see figure 4) in a wiring closet located within the center director's private office, that also contained their security system and office telephone system. Unfortunately, none of these network connections were connected. Instead, a phone line also in that closet was connected to a DSL router, which was in turn connected to a wireless access point/router, and both the director's and secretary's computers had wireless access cards connected to an unsecured wireless network. A network switch was purchased and these systems were connected to the wired network and had the wireless connection removed. Since this closet was normally locked, this provided a layer of physical security to the network. This also was chosen to be the best location to put the server, since it would remain locked, and out of the way of students. Although it was a closet and didn't give much extra room for a server, remote desktop was used so the server could normally be managed remotely from one of the office computers, so that someone need to have physical access to the server only in emergency situations.

Remote Access

Remote access to the server was granted by enabling the remote desktop service on the server, and then by remotely connecting to it from any of the other manager's computers in the center. The remote desktop client is installed by default with Windows XP.

In order to enable remote desktop on the server,

- Right click on my computer -> properties
- Click on the "remote" tab
- Under the remote desktop section, click on the checkbox "allow users to connect remotely to this computer" and click "OK".

In order to connect via remote desktop from the desktop client,

- Go to start -> programs -> accessories -> communications (usually) -> remote desktop connection.
- Type the correct machine name or IP address of the server. In this case, it was:
- "clc-server" (without the quotes)
- A logon prompt appears, and you can then log in as if you were at the actual console of the computer.

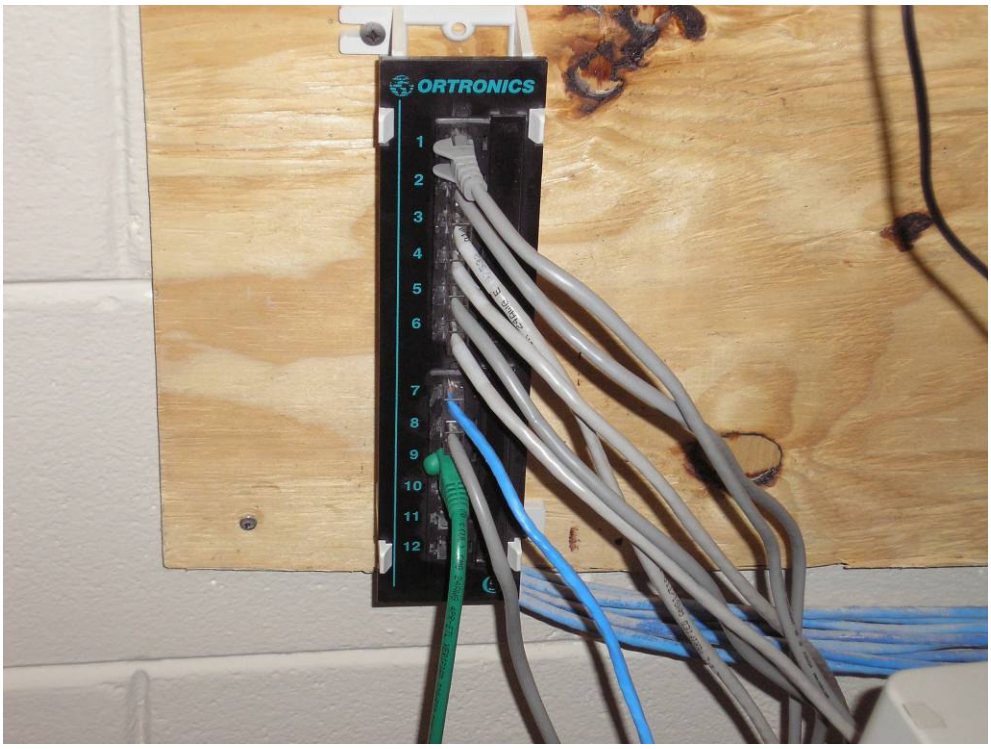


Figure 4: Patch Panel in Network Closet

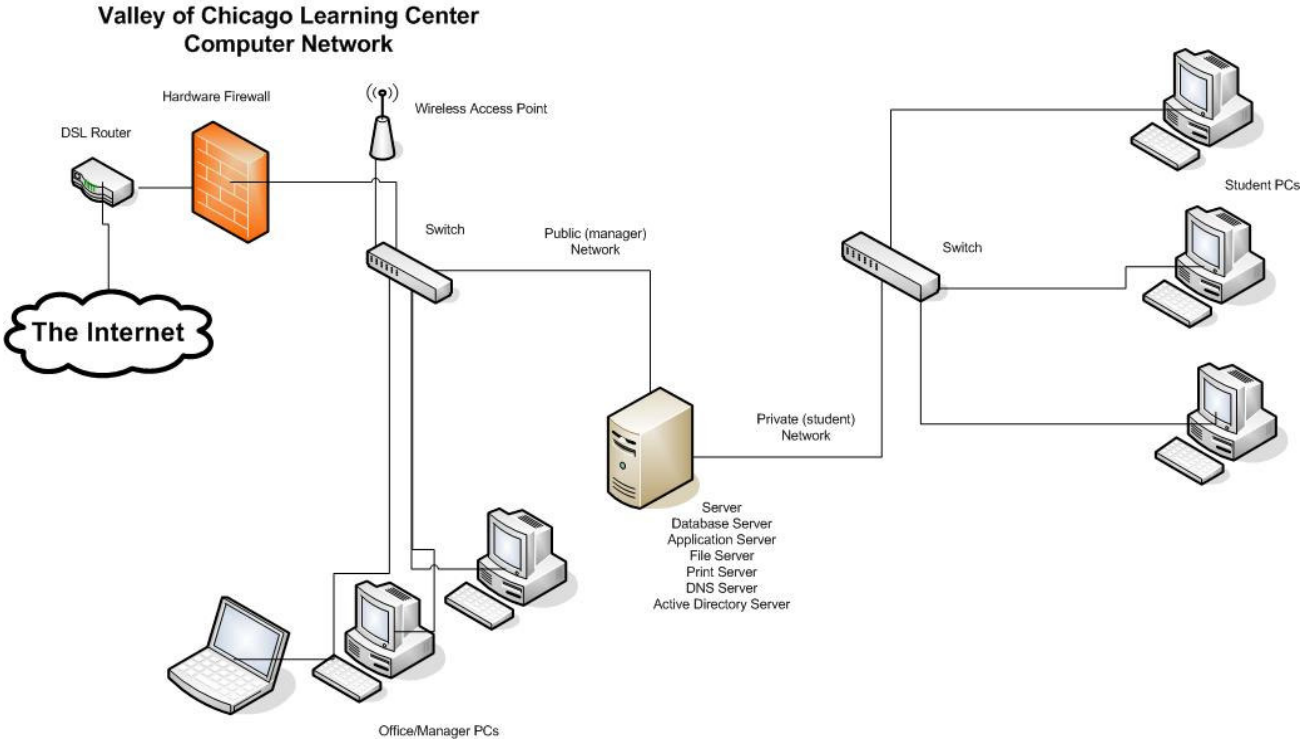


Figure 5: Network Diagram of Center

At the beginning of the project, there were two computers using wireless internet connections to connect to a wireless access point which was in turn connected to the Internet. There were also a number of stand-alone computers without Internet access which were used for various stand-alone tasks, such as printing certificates and running DOS-based legacy tutoring programs. Securing the network involved maintaining the systems that currently had and needed Internet access, providing Internet access to systems that currently did not have it, while restricting it from systems that did not need it, while doing this in the most secure method possible.

The network was designed based on the initial premise that students do not need, and should not have any Internet access from their computers in the center. Therefore, the network as shown in Figure 5 was designed with this in mind. Two Ethernet networks utilizing category 6 cabling were created. The "manager" network is for the employees of the center. It has a direct connection to the Internet through a DSL router attached to a multi-port switch and hardware firewall box. This box was Linksys branded, and is commercially available for home or small office use. The hardware firewall prevents malicious traffic from the Internet from getting to any of the computers in the center. It was determined that remote access to the computers in the center is currently not needed, so the hardware firewall also prevents any sort of remote access connections to the center's computer network that was not initiated from inside the center. The server is also accessible from the manager network, so that the managers can access and manage the server. The "student" network uses private (non-routable) Internet addresses, and is connected only to the server, and has no direct connection to the Internet. The server contains two network cards, one for the private student network and one for the Internet accessible manager network. Also, the systems on the private network cannot connect to the Internet through the server, though it would be possible to configure to do so, if desired in the future. Figure 5 shows a diagram of the network, including the separate student and manager networks.

Network Settings

Configuring the public (manager) and private (student) networks involved a combination of client and server configuration settings. Systems on the manager network were configured with DHCP (dynamic host configuration protocol), which grabbed an IP address from the hardware firewall/router that connects to the DSL modem. This hardware firewall/router has a built-in DHCP server which was configured to automatically assign IP addresses to systems that requested them. These addresses forward Internet based IP traffic from these computers onto the Internet, while only accepting incoming connections from the Internet if they were initially requested from the internal computers. This one way routing provides an effective protection from malicious Internet traffic scanning for host vulnerabilities, and is the default configuration on most commercially available firewall boxes.

For the computers on the private student network, each computer had its IP address settings configured manually using the following configuration.

Start -> settings -> network connections -> right click on “local area connection” -> properties -> Internet Protocol TCP/IP
IP address: 192.168.0.x (from 2, 3, 4, etc)
Subnet mask: 255.255.255.0
Gateway: 192.168.0.2 (this was the internet address of the server)

192.168.0 is in a range of private, class C addresses, and is defined as non-routable, and not allowed on the Internet, but reserved for use in private networks such as this one.

The server could have been configured as a DHCP server to give out these addresses automatically. However, since there was a very limited number of student PCs (4), it was determined to be easier to just configure the IP addresses manually on each student PC. For larger networks, installing a DHCP service on the server would have probably been easiest.

For the routing configuration of the server itself, the “routing and remote access” service was installed and configured, and the internal network card was given a private address of 192.168.0.2 using the procedure listed above. See figure 6 for the configuration screen.

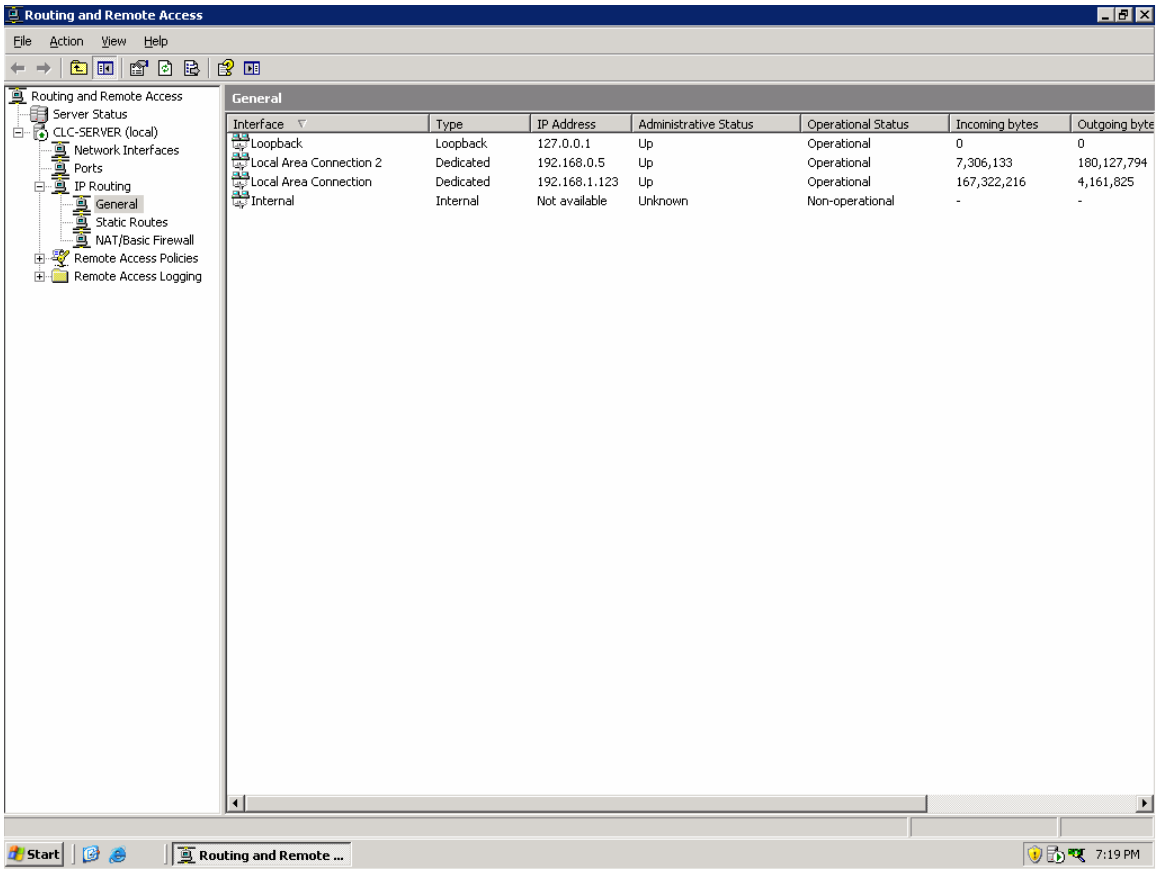


Figure 6: Configuration of Server with 2 Networks (Student and Manager)

Next, the routing and remote access service was configured to enable both the public and private networks, and to use the public interface (whose network card was configured with DHCP from the firewall/router). Simply enabling both interfaces was all that was required.

Wireless Security

The center had a functioning wireless access point, which was used for Internet access from both desktops and laptops. However, the wireless network was open and unsecured, even visible from the parking lot. All systems were moved from the wireless to a wired network, which is much more secure, except for a single laptop that is sometimes used from classroom to classroom for training purposes by a tutor. This training involves visiting actual websites, but is only done occasionally when the tutor is in the room.

Wireless networks are never as inheritably secure as wired Ethernet connections. In particular, WEP encryption can be broken in less than three minutes with commonly available tools. A sophisticated hacker can monitor wireless traffic and determine the encryption key used with WEP due to its weak and frequently repeating encryption algorithm implemented [9].

While WEP is considered very weak encryption, it was all that was supported by their current wireless access point, and after moving all of the systems to wired connections except for a rarely used laptop, it was determined that the wireless access point could continue to be used with the laptop until a more advanced access point that supports better encryption could be purchased. The settings listed below were able to greatly reduce the risk of unauthorized wireless network access.

Wireless Access Point Access – The access point was configured not to allow any inbound connections from the Internet. All access to the access point's management functions had to be made from a wired connection on one of its internal wired Ethernet connections. Also the default password was changed to something known by the managers but not easily guessable.

SSID name – If the SSID of the network is easily guessable, it is easy for an unauthorized user to make a connection to a protected wireless network. Therefore, for the center, the SSID name was changed from "default" to a unique and hard to guess yet easy to remember name.

SSID broadcast – If the SSID is broadcast, it means that other computers in range of the wireless access point can view the name of the wireless network and then attempt to connect to it. By not broadcasting the SSID, it makes it more difficult for wireless devices to see that they are in range of a wireless network. Therefore, for the center, SSID broadcast was disabled.

MAC address filtering – By allowing only specific MAC addresses to connect to the wireless network, it is possible to reduce the risk of unauthorized devices connecting to the network. In order to do this, the MAC address of the authorized laptop needed to be identified (in a MS-DOS prompt, one can type "ipconfig /all" to obtain the MAC address). Then, this address must be entered into the wireless access point's configuration, in an allowed device list.

The MAC address filtering for the center was configured to allow only the specific MAC address of the authorized laptop, and WEP encryption was enabled to make it somewhat more difficult to intercept and read the wireless communications. Due to the weakness of the WEP encryption, and the possibility that a determined and sophisticated hacker could quickly break into the wireless network, these security controls are considered a short-term solution. In the long term, it has been recommended to replace the existing wireless access point with one that supports the more secure WPA encryption standard.

To help mitigate the risk of using this insecure wireless network, there is a policy not to use the wireless for any business or for use with sensitive information, but only to visit the particular educational websites required. Wired Internet connections are to be used for access to any websites requiring a username and password, or for remotely accessing any other computer within the center.

Server and Desktop Security

Some of the server services, such as file and printer sharing, could also be accomplished with Linux. However, since the Lexia software database required installation on a Windows based server, and to minimize both the complexity of the network and the number of servers required, it was decided to use just the single Windows based server for all required network services, including file and printer sharing, domain authentication, and auditing. Figure 7 shows the Dell Server that was purchased for the center. In most organizations, it is a best security practice not to have all critical servers on a single box, for several reasons. Finding a security vulnerability in any one particular service could lead to a compromise of the entire computer, and also risks a single point of failure for the organization. Having multiple servers, each running separate services, helps isolate against a security incident or hardware/software failure taking down too many critical services in an organization. However, very small organizations such as the center may not have the budget for additional server hardware or the resources to manage a larger, more complicated network.

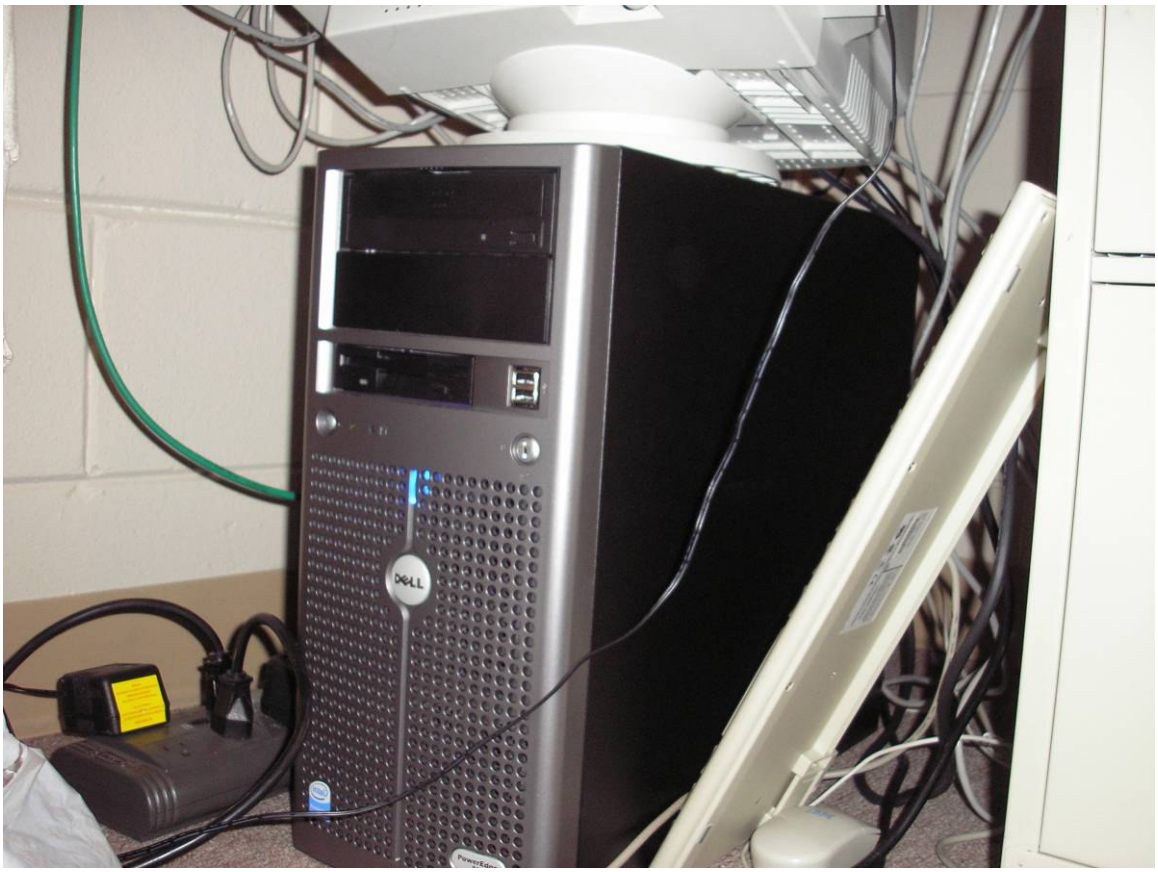


Figure 7: Close up of Server in wiring closet

Based on the risk assessment, it was determined that the risk of failure of the single server was fairly small, and if the server had failed, it was not critical that services were immediately restored. The tutoring software, while important, was not an essential part of the student's curriculum, and downtime of a week or longer was considered acceptable, in case the server had to be rebuilt or replaced. It was determined that as long as there were adequate backups, the risk of a failed server containing multiple services was acceptable to this particular organization.

RAID

RAID (redundant array of inexpensive disks) can be used to provide redundancy in hard drives, so that a failure on the server's disk doesn't result in the loss of data. RAID can be described as two or more disks working in parallel that appear as one drive to the user, providing better performance, security, or both [10].

RAID software and hardware to manage the disks are managed by the computer's onboard hardware controllers with the operating system or by a separate hardware RAID controller card. Modern versions of both Windows and Linux server software contain built-in RAID management software. However, despite the additional cost of a hardware RAID card, there is much greater performance with hardware RAID than with software-

only RAID, since it offloads the management of the disks from the Computer's CPU, freeing up the computer's processor for other tasks.

There are different RAID levels which are used for different purposes, each with their own advantages and disadvantages. While currently RAID levels 1 and 5 are most popular, RAID 1 is mentioned below in detail since it was the RAID level chosen for this particular project.

In a RAID 1 configuration, shown in figure 8, data is written in blocks to two separate disks at the same time. Also, the disk controller can use either drive if either of the disks fails, and can continue to operate.

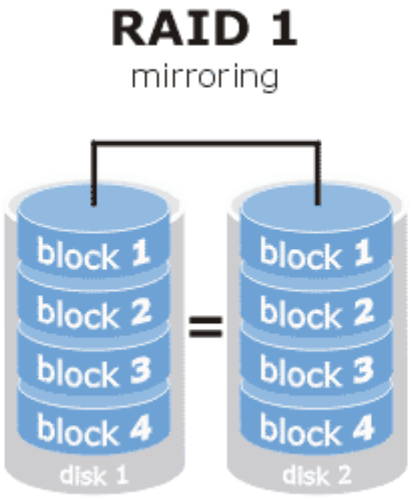


Figure 8: RAID 1 configuration with 2 disks

The advantages of a RAID 1 configuration are the fast read and write speeds that are close to having stand-alone drives, and the fact that you only need to buy two hard drives. The disadvantage is that you only can use half of the full storage capacity of the two drives (one of the two drives), making it not as cost efficient especially for larger storage requirements.

It was decided to use a RAID-1 configuration for the center, as it allowed the purchase of only two drives for the server, and since the amount of data to be stored on the server was sufficiently small. Therefore, two large hard drives were considered to be sufficient for their current and future storage needs.

To configure the hardware RAID-1, which is managed by the RAID controller card attached to the two drives, in the BIOS of the RAID card, both hard drives were selected and then the option to create a RAID-1 configuration was given, using the two drives. The RAID array was then formatted and ready for use by the operating system.

During system installation, the RAID'ed disks were partitioned into a separate operating system partition and data/application partition. For security, it is often recommended to separate the operating system from the data. This simplifies the backup process, so that for regular data backups, only the data partition would need to be backed up or restored. Dell's server assistant software, which is used to install Windows on Dell server hardware, makes it easy for such separate partitions to be installed as part of the operating system installation.

Security Permissions

Security permissions on files and folders prevent unauthorized access to resources such as data shares or printers. There are group-based permissions for students, tutors, and administrators of the center, and each group is given permissions on the appropriate shares that that group needs to be able to access.

Groups could be local to the server, or part of an entire domain. However, since there was only one server, the groups for the center had been initially created as local to the server. In order to create a group on the server and add users to it:

- In the management console (right click on "My Computer", go to "manage"), click on "Local Users and Groups".
- Right click on "Groups", and choose "New Group".
- Type a name for the group.
- Double click on the group you created, and choose "add" to add users from the domain.
- Add each user needed for that group in the form "domain\username".
- For the purposes of the center, they are in the form "clc\username", since "clc" is the name of the domain.

To set the appropriate permissions for the folder you want to share:

- Right click on the folder that you want to share
- Choose "sharing and security"
- Under the sharing tab, choose "share this folder"
- Give the name that you want to use for the sharing.
- Click the "permissions" button
- Click the "remove" button to remove "everyone" from the access list
- Click "add"
- Add the name of the group that you want to give access to, then "OK"
- With the group highlighted, choose the appropriate permissions required for that shared folder, usually "full control" or "read only" under "allow", and click "OK"

Accounts

Centralized domain computer accounts have been setup for all users of the center. This allows access to shared resources like printers and network drives from any computer in the center, without the need for maintaining separate computer accounts on each system. This is also necessary so that each user of the computer can be identified for security auditing purposes, since it was requested that each user of the center have their login times logged, so they could find out who was using which computer and at what time.

In order to setup user accounts in the domain for each user:

- Log into the server
- Go to start -> programs -> administrative tools ->"active directory users and computers"
- Under "users", right click and choose "new user"
- Enter the student or tutor's name, choose a unique id and a temporary password

For the center, a list of student names, userids, and assigned passwords were provided.

Group Policy

Group Policy is the primary tool used in recent versions of Microsoft Windows to do centralized management of the computers, users, and other Active Directory objects. This makes enterprise change and configuration management possible.

With group policy, many aspects of the desktop or server's Windows operating system can be managed centrally, including the registry, security permissions, software distribution settings, and logon scripts. Group policy objects are used to store these policy settings. A single group policy can be linked to a one or many sites, domains, or organizational units, making the security policy and configuration changes to large numbers of computers easy to manage.

Objects in the active directory including computers can have multiple group policy objects apply to it. During system startup, the Windows operating system will check and apply the relevant group policy settings to the computer, and will periodically check for new group policy updates and changes at a regular, preconfigured interval.

Group policy is therefore the foundation for managing Windows system security centrally for a large, or small, number of computers, including any systems running Windows 2000, XP, 2003, or Vista. This centralized group policy is not available for systems running most Home Edition versions of Windows, as it requires the computer to be joined to a Windows Domain in order to receive the group policies. However, such standalone systems not joined to a domain can apply local security policies on the system from a preconfigured template file, but must be applied to each system manually. Smaller organizations without a server with limited numbers of desktop systems might want to

consider this option, as it is better than taking the default security settings, which usually are not restrictive enough to face today's computer security threats.

Since a server was provided in the budget for the center, and since the pricing for the academic version of the Windows 2003 server was extremely reasonable, it was decided to use group policy on a central domain for the computers in the center. The domain group policy is able to lock down all of the system settings for the server as well as the student's desktop computers. This includes setting the password policy and lockouts.

There are a number of common group policy settings that are recommended for basic security. These settings have been tested and found not to interfere with the operation of the computers in the center, so they were applied to the entire Windows computer domain, which has a special group policy called the "Domain Security Policy" for this purpose.

To configure settings for the domain security policy:

- On the domain controller, open "active directory users and computers"
- Right click on the "clc" domain, and go to "properties"
- Click the "group policy" tab
- Right click, and choose "edit"
- The Computer Management console will open, allowing you to configure any required domain group policy settings. When finished making modifications, click "OK"

It is also recommended to download and install Microsoft's Group Policy editor which makes it easier to review all of the group policy configuration settings at a glance. It is available at no charge from the Microsoft website.

Anti-Virus and Spyware Protection

There are many desktop anti-virus products currently available. Many studies have been done that rate the effectiveness of each of these products. While different test results have given better ratings to different products, it's true that some of the more inexpensive anti-virus packages perform decently, though not quite as good as the more expensive or widely used products. It's also true that many of these products do not effectively protect against today's Trojan and malware threats, many of which can mutate to escape detection [11].

Some marginally rated anti-virus products such as AVAST and Grisoft AVG are free for home users, but their license agreements explicitly state that they cannot be used for non-profit or educational organizations without a separate, paid license. Both of these vendors do provide a very inexpensive academic/non-profit license for multiple copies of their product. However, since a McAfee based anti-virus and anti-spyware product, which did get very decent scores in many of the reviews, was available for free, this software was

installed and configured to download and install new virus pattern updates every few hours for all the computers in the center. Of course, the systems on the private student network are not normally able to access the Internet and thus cannot receive the regular updates. However, during downtime maintenance periods (breaks) the systems are patched and the anti-virus definitions are updated at this time by temporarily connecting the systems to the Internet for updates. The risk of infection on these systems was considered very small, since removable media are not supposed to be introduced on these systems by students, and since there is no Internet connection normally on these systems.

Some industry analysts have recently argued that the traditional antivirus methods of detecting and removing viruses, trojans, and spyware using signature based detection are completely ineffective, because signature based detection can't keep up with number of variants being released by hackers [12]. This is happening even though signature based detection is more popular because it risks far fewer false positives than other types of detection such as anomaly based detection systems. Some suggest that anomaly based intrusion detection or virus detection systems would be better suited to protecting against today's virus threats, utilizing mail gateway and network rather than just the desktop.

Of course, no anti-virus solution is very effective against zero day exploits where there is no recognized virus signature downloaded to the client anti-virus scanner, and this sort of attack is unfortunately all too common. Fortunately, to mitigate this risk, many commercial e-mail services, including the Yahoo e-mail accounts currently being used by members of the center, have integrated anti-virus protection, and due to the widespread use of these accounts, the managers of AT&T Yahoo and other large internet service providers are often at the forefront of virus protection for their customers. However, such protections should not be considered all that is necessary to ensure safety from today's Internet threats.

A layered security approach is best for providing desktop security from such online threats. Besides the e-mail security provided by the e-mail service provider, up to date anti-virus protection software should also be installed on the desktop computer itself, and users need to be educated to not open unexpected or unusual attachments. In addition, normally logging into the computer with an account that is not a member of the local administrator's group on the PC can also help prevent extensive damage to the operating system from a successful exploit from the Internet, as can making sure that the computer is patched with the latest security fixes from Microsoft, to prevent malicious code that is accidentally run from being able to exploit a known system vulnerability.

Intrusion Detection

Such a combination of factors helps lower drastically, but not entirely remove, the risk of a virus exploit. Procedures need to be in place to quickly identify and rebuild a machine that was compromised. Such instructions for rebuilding the network were given to the center, and they know to contact a computer professional if they suspect some sort of successful virus attack. In their computer awareness training, the center's tutors were

trained on how to identify signs of a successful virus attack, so they can act as a first line of defense.

Small organizations are at a disadvantage for detecting compromised machines without their own in house or outsourced intrusion detection service. However, as long as sensitive information is properly protected, with proper layers of commercially available technical as well as management and operational controls in place, such risks can be definitely reduced to the point that they are manageable for small non-profit organizations, without the need for such expensive technologies as intrusion detection systems.

Host based Intrusion Detection Software is generally in one of two categories. Some are centralized products that are designed for an enterprise and need a fair amount of configuration to weed out "False Positives". They are probably not a good idea for a small network with no dedicated IT department. The second variety of software is integrated as part of host based firewall product such as ZoneAlarm or BlackICE. They are designed for the non-technical computer user, but provide few benefits and the potential for system problems when the network. Their firewall capability is not as important when the network is already behind a hardware firewall. While some would argue that it is good to have an additional layer of firewall defense besides the hardware firewall, experience has shown that these products can cause too many false positives, system performance problems, and other end-user problems compared with the limited additional security benefit they provide.

System Patching

The systems on the "manager" network are configured for automatic Windows updates, so that critical security updates are downloaded and installed automatically whenever they appear, and that patches are applied nightly.

To configure automatic Windows updates on these systems (Windows XP and 2003):

- Right click on "My Computer" and go to "Properties"
- Click on "Automatic Updates" tab
- Click on "Automatic", and chose "Every Day" to install updates , pick a time
- Click OK

A screenshot from the Windows update dialog box is shown in figure 9.

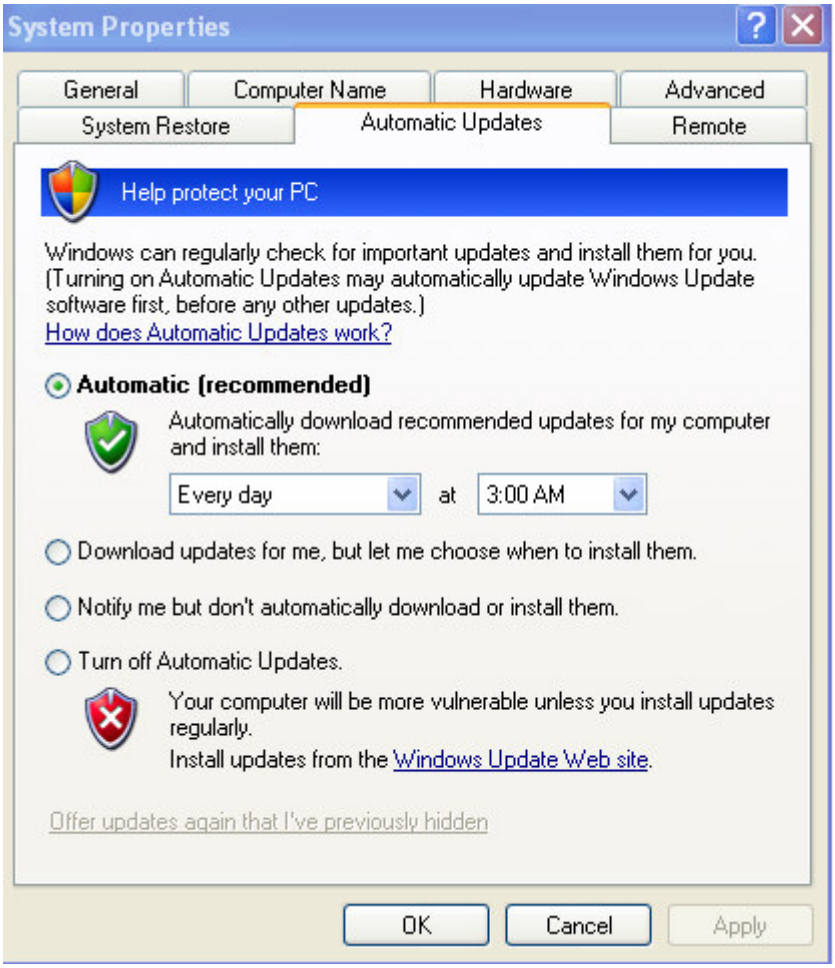


Figure 9: Windows Update Settings for manager's desktop

Systems that are turned off during the scheduled time will not have the critical patches installed automatically, but will notify the user that there are critical patches to apply the next time they log into the system. The staff should be therefore trained to install these patches when they are notified of them, or there should be a policy to log off of systems when not in use, but to keep them turned on at night. Another option is to set up group policy settings to force a reboot if there are new patches to install after the specified patch install time. Configuring the automatic patching through group policy settings is considered a best practice, as it ensures that the patches will be applied with or without user intervention. This is how the systems in the center are configured.

The systems on the internal student network, as well as the server, are patched manually during the scheduled downtime periods, so as to prevent cause disruption due to a problem with a patch during student use periods. Since these systems do not have any Internet access, except for the server, and since all are behind the center's hardware firewall, and do not normally use removable media, it is considered very low risk that an unpatched system could be compromised.

In order to manually patch these systems with critical updates:

- Open a web browser to http://windowsupdate.microsoft.com
- Click on “Express”. The system will check for the latest update for the computer.
- If any updates are available, click “Install Updates”. This will install the critical updates on your computer.
- If prompted to reboot the computer, do so immediately if possible.

Administration Rights

The principle of least privilege is the concept that user accounts on a system should only be given the specific level of permissions needed to be able to do the tasks normally expected for that user on that system. Microsoft operating systems were initially designed where the user of the computer had full control of the system (administrator rights). Windows NT, 2000, and XP began to change this model by allowing the establishment of user accounts with a more limited set of permissions on the system. Permissions in Windows are being changed from a default “allow” to a default “deny”, where users must prove their identity before being authorized to run a privileged command. This can help prevent hackers from trying to get the end user to run code that may compromise the system by running the code to exploit the system with the privileged, currently logged in user’s account permissions [13].

In order to configure systems for least privilege operation, simply create regular domain user accounts for each user of the system, and do not put them in the local power users or administrator’s group on the desktop PCs. Most modern applications will work fine even without the logged on user having administrator rights on the computer.

Application Security

Lexia’s suite of software uses a common Microsoft SQL based database and has its own account management system. Each user of Lexia has their own username and password to the Lexia database. The same username and password is common across all of the Lexia applications. This restricts the administration and management of the application. There is also a system-wide administration account for management of the Lexia server. This is the “sysadmin” account.

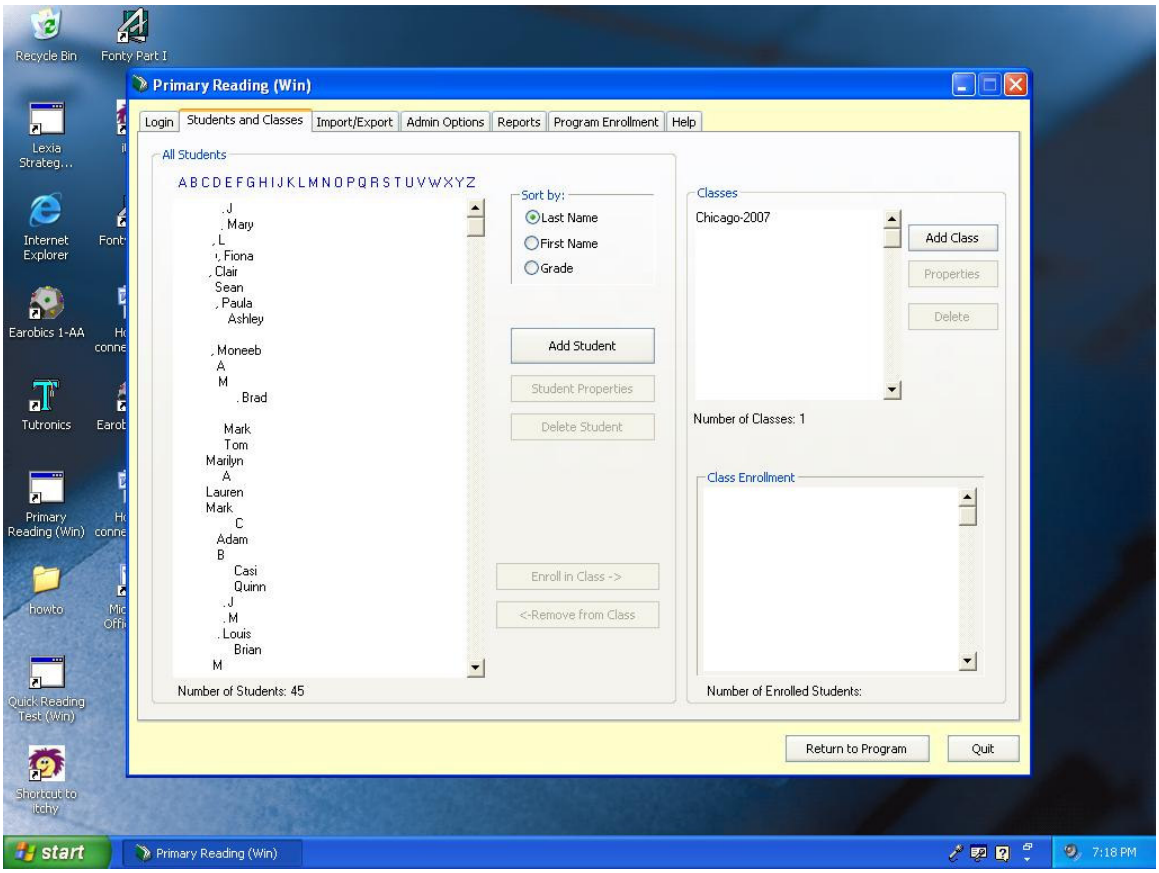


Figure 10: Student management screen within Lexia Management Console (student names removed)

There is extensive documentation on setting up and configuring the Lexia database security in the "Lexia Administrator's Guide". This guide is included in the manager's share on the server, and is also available as a download on the Lexia website free of charge.

In order to add password protected student accounts for Lexia, do the following:

- Click "admin" in any Lexia application's select a student name startup screen
- Click on "Add Student".
- Enter the student's first and last name, as well as unique username.
- The current setup does not have grade levels or demographics assigned to any students.
- A password field is filled in for each student and each password is recorded.
- Click "OK".

The management console for Lexia is shown in figure 10.

Database Security

A Microsoft Access database had been developed for business management functions of the center; including student and tutor rosters, salaries, and other financial and HR related information. The database is password protected since only a few managers in the center need to have access to the database. Also, the database was moved from a stand-alone desktop PC to a special share on the file server with access permissions to allow access to the file share only from the users who need access to it and who have authenticated themselves over the network.

To set up the password protection in Microsoft Access 2003,

- Go to Tools -> Security -> Workgroup administrator, and create a new system database.
- Go to Tools -> Security -> User and Group Accounts
- Click “Change Logon Password”, and “Apply”
- Click the “Users” tab. Create a new user and add the account to the “Admins” group, cick “OK”
- Click the “File” menu and “Exit”.
- Restart Access and logon as the new admin user you created
- Go to Tools -> Security -> User and Group Accounts
- Click “Change Logon Password”, type a new password, and click “Apply”
- Under “Tools” -> “Security” -> “User and Group Permissions” click “Permissions” tab
- Select “Groups” under the “List” options to display group names in User/Group Name box.
- Click “Users”, select object type to display objects, and remove default users group permissions for <current database>, <New Tables/queries>, <new forms>, <new reports> , <new macros>
- Under “Tools” -> “Security”, choose “Encrypt/Decrypt Database” to encrypt the database
- The database will now be encrypted, and accessible only to the user account specified.

Since there is sensitive information in the database (student records and financial information), there is also a policy in place to keep the data on the server and not on removable drives or laptops. It is accessed from the manager’s PCs but the data is kept on the server at all times.

Auditing and Evaluation

In order to enable event auditing (including user logons) on Windows systems, which can help the administrator what events caused a security incident, the following group policy settings can be configured either from a group policy template applied to an Organizational Unit within a Domain, or on individual computers, using the “gpedit.msc”

command. In order to minimize effort, it is easier to group the computers within the Active Directory and force the auditing through group policy.

The policy settings required for this are as follows:

- Under the group policy or local security policy template, choose “Computer Configuration” -> “Windows Settings” -> “Security Settings” -> “Local Policies” -> “Audit Policy”
- Select “Audit account logon events”, “audit logon events”, and on the domain controllers, also enable “Audit Directory Services Access”. You will probably also want to audit “account management”, “policy change” and “system events”, as an intrusion could flag any of these sorts of events.
- Click both “Audit Successful Attempts” and “Audit Failed Attempts” for each category.

In order to build a successful security program at an educational institution, all current “processes and plans should be reviewed as part of an annual procedure or as the result of emergent threats/risks, errors, inefficiencies or ineffectiveness. A formal review process should be part of the strategic planning cycle. The plan review process should include the overall review of the strategic plan and the steps needed to change the plan and adjust its direction based on the review and outside input. The revised plan must consider emergent strategies and changes affecting the institution’s intended course” (Gatewood, 2007).

Clearly, it is necessary to periodically review the security plan, review and revise the risk assessment, and review and test the security controls in place for effectiveness [14]. Since this system is new, it has not yet been necessary to review everything again, but it should be done at least once a year, or whenever there is a major change to the system. However, since the center’s new computer network is limited in scope, performs limited functions and services, and has fairly limited attack vectors, it would not be expected that many major changes to the security plan would be needed.

Configuration/change management can also prevent security incidents, because an unauthorized configuration change can introduce security vulnerabilities into the network. Therefore, there is a policy to allow changes or connections of new computers only by authorized personnel, and that changes to the network are announced in advanced, and have the changes documented in a change log file, shown in figure 11.

Date	Change	Procedure
3/14/2007	Applied Windows 2003 Service Pack 2 to clc-server	Go to windowsupdate.microsoft.com Install Service Pack 2 from list
3/18/2007	Configured numlock on student desktops to remain on Prior to system logon	Run regedt32.exe HKEY_USERS\.Default\Control Panel\Keyboard Value changed from 0 to 2

Figure 11: Excerpt from Configuration Change Log

In addition, major changes to the network are made only during downtime periods (during school breaks) so as not to cause disruptions, and are tested before being put into production.

Disaster Recovery

Even small organizations need to consider the potential impact of computer disasters in their computer security policy and take appropriate precautions.

Disaster recovery plans are the plans to resume access to critical computer hardware, software, and data after a natural or manmade disaster. Having a disaster recovery plan is critical for any organizations, including small non-profits. However, the extent of the plan will probably not need to be as comprehensive as for larger organizations, or organizations with more critical or complicated systems. Most non-profits, including the Valley of Chicago Learning Center, use commercially available off the shelf software, which simplifies the disaster recovery process greatly, since the software can be easily reinstalled in most cases. A disaster recovery plan, at a minimum, should define a backup strategy, and a contingency plan [15].

Once again based on the risk assessment, which indicates that the computer network does not need constant availability, since non-computer based training alternatives are available, the disaster recovery plan doesn't need to be as extensive as it might otherwise be for a larger system or organization. The risk assessment will determine the extent of the disaster recovery procedures required.

For this system, it was determined to do regular weekly backups of the server data including the Lexia database on the server. As part of the procedure, these backups are burned to DVD and are stored offsite. By storing the backups offsite, they would be available even in the event of damage to the room containing the server.

Detailed instructions for doing these backups have been made available to the managers, and are included in the appendix.

The data on the server is actually fairly small, making the DVD archives a quick and easy possibility. For more extensive amounts of data, backups to external storage or high density tapes may be necessary.

In addition, there is documentation of the configuration of the software, hardware, and network, and how to rebuild everything, including software configuration and file restore of data, so that the network can rebuilt if necessary.

Project Results:

The initial setup of the computer network and initial configuration and testing of its security settings was successful and went faster than anticipated. However, there were

unexpected challenges in completing the project on time, due to requests for features and options that were not initially requested or anticipated in the initial project plan and requirements document, and were not mentioned in the initial project proposal.

The largest problem encountered in the project was the issue of "feature creep". The original proposal attempted to describe all of the requirements for the project. However, after the project had already been partially implemented, additional requirements were identified that had an impact in the scope of the project as well as the time and effort necessary to fulfill the security requirements. One example of this an extensive auditing capability not provided by Windows, and not mentioned in the original proposal. The director of the center "assumed" that the system would be able to centrally audit how long each student is using each application on the system and when this occurred. This level of software usage auditing exceeded what was possible within the Operating System, as it was desired for all applications on the system, not just the Lexia software.

Windows does have some auditing capabilities built-in, including the ability to register login times for each user, however software application metering, which shows what users are using what software and for how long, is not available within the Windows Operating System. Unfortunately, most third party enterprise software metering applications are designed for larger organizations and are often bundled into more extensive desktop management application suites for managing enterprise desktops. Some smaller vendors do sell software metering products such as Integrity software's Softrack, and Codework's Application Metering solution, at fairly reasonable prices. ($150-$400 for 5 seats). However, these products require a Microsoft server with Internet Information Services installed, and do not yet support the 64bit versions of the Windows operating system. As such, they have not yet been implemented at the center, but are planned as a future upgrade.

Another requirement for the network, not initially mentioned in the requirements phase, was the ability of the new student computers to run some older, legacy software applications such as Earobics and Tutronix. It was discovered that the Earobics software, which was several years old, will not run without the logged in user having administrative rights on the system. Some legacy applications, such as these, require the user account of the locally logged user to have the local administrative permissions on the computer in order for the application to operate correctly (or at all in some cases). Upgrading to the latest version, which will run without the admin rights would cost 10K, and was deemed currently cost prohibitive. While the old version of Earobics would run correctly on Windows Vista even without the admin rights, their Tutronix application doesn't. In the meantime, the students that require the Earobics software have been given admin rights on the desktop computers that have Earobics installed, with group policy settings preventing local changes from being retained on the desktops. This does lower the overall security of the student PCs but is necessary until an upgrade to Vista or an upgrade of the Earobics software can be made.

Conclusions and future directions

Long term support of the computer network is still somewhat of a concern. While the network has been very reliable and "self-managed", from time to time there are some computer questions and problems that are encountered, usually the result of user error or lack of training. It is important for even small organizations to have someone at least fairly computer literate, so that the less difficult problems can be sorted out. Some volunteer centers may want to take advantage of computer mentoring organizations such as CompuMentor which helps assist non-profit organizations with computer productivity. Their nonprofit website TechSoup.org provides free educational resources for nonprofits and distributes nonprofit technology donations to nonprofits in the US, as well as match up mentors to non-profits looking for help. Often just being in touch with a computer professional who can answer questions and offer quick suggestions can be helpful. Among their free online resources, their free guide to Healthy and Secure Computing for non-profit organizations outlines the majority of priority project actions identified in this project required for secure computing, and is written for non-technical people to understand. It's very possible that a small non-profit can get by with at least one person on their staff being computer literate enough to solve day to day problems, and consult with a technical expert who can provide mostly e-mail or voice answers to questions.

While on-site consulting may be at times necessary for major outages or upgrades, its also possible that more and more issues could be managed remotely using an increasing number remote control tools such as VNC (virtual network computing), or desktop sharing applications such as WebEx, which allows users to share their desktop with a remote technical expert or colleague. Consultants brought in even on a per incident basis could use remote desktop sharing applications such as WebEx to remotely fix a particular problem. However, despite a secure model used by companies like WebEx, there are some security concerns with such products because by sharing a computer with someone outside the organization, there are concerns about access to a computer without having the external user sign legal liability wavers, and going through adequate background checks.

One of the future upgrades suggested has been providing limited Internet access to the student's lab computers, so that students can access specifically approved web sites that contain helpful information and educational resources. There are a number of possible ways to accomplish this. There are a number of free open source products that can function as a web content filtering firewall, as well as a number of improved, inexpensive commercial versions of such products. These include Dan's guardian, Smooth wall, IP cop, and Privoxy. Most of these run strictly under UNIX/Linux based operating systems, so setting up a Linux box to function as the firewall/content filter may be necessary. Due to the security and stability of Linux based systems, it may be possible to configure such a box with minimal need for administration. Even though an additional computer would be needed for this purpose, Linux can run on very inexpensive hardware, so even an older computer would probably be adequate for this function. There are also Windows PC desktop based Internet filters such as NetNanny and CyberSitter, or for restricting Internet access to just specific allowed IP addresses, third party shareware such as

Internet Lock. Finally, some hardware routers and firewalls such as the Sonic Wall Pro 2040 has the ability to do content filtering as an add-on product. For somewhat larger organizations, perhaps this option would be more cost effective.

There may also a number of other advantages if the private and public networks were consolidated. It would make it possible to access the Lexia software from the manager's network. (Currently the server can be accessed and managed, but other desktops on the manager's network cannot directly run the Lexia software from their PCs, since the server software is running on the private address of the server). Also, currently, the computers in the tutoring lab cannot connect to printers directly attached to desktop computers on the manager's network, but only printers connected through the print server. This would provide greater flexibility, as some of these printers would provide greater backup redundancy if there is a problem with the main printer if they were accessible by the student network. Therefore, the network consolidation would probably occur once the systems have all been upgraded to Windows Vista. Vista also has a parental control filter built into all desktop versions of Vista. This may be the best option in the future for the center, since their agreement included a free upgrade to Vista for all of their desktops. However, since there is no immediate need for the single network, and since Vista is not yet compatible with all of their applications, such a change is not immanent.

While Vista has better security features than other versions of Windows, including built in parental controls, a built-in anti-phishing filter in Internet Explorer, and better security process isolation for user accounts (user accounts in Vista, even the administrator accounts, do not always run with elevated privileges). However, Vista has significant hardware requirements, and although the new computers at the center would probably run Vista with no problems, a slight performance decrease would be likely [16]. In addition, not all of the hardware at the center, including drivers for some of their printers, is currently available with Vista. Also, since the user interface for Vista is different than XP, it may take additional training for users and managers alike to become familiar enough with it for use without additional problems and questions. Also, being a new operating system, there may be bugs encountered or security vulnerabilities that are not present with more mature operating systems like Windows XP. However, the most compelling reason not to upgrade the Center to Vista at the present time is the fact that some of their software applications, especially Tutronix, do not currently run under Windows Vista. Until an update is made available, it will not be possible to upgrade the systems in the Center to Windows Vista.

In conclusion, it was possible to create a cost-effective, easy to manage and yet secure computer network for a small non-profit organization, without a large commitment of time or effort. The "expectation" gap and "feature creep" experienced may have been alleviated by developing a more detailed requirements document, and by bringing in more technically knowledgeable subject matter experts. Overall, the center implementation of a secure computer network for tutoring was a success and provided a tremendous learning opportunity. A photograph of the completed tutoring lab is shown in figure 12.

Figure 12: Completed student electronic tutoring room

Appendix A: How to back up the server

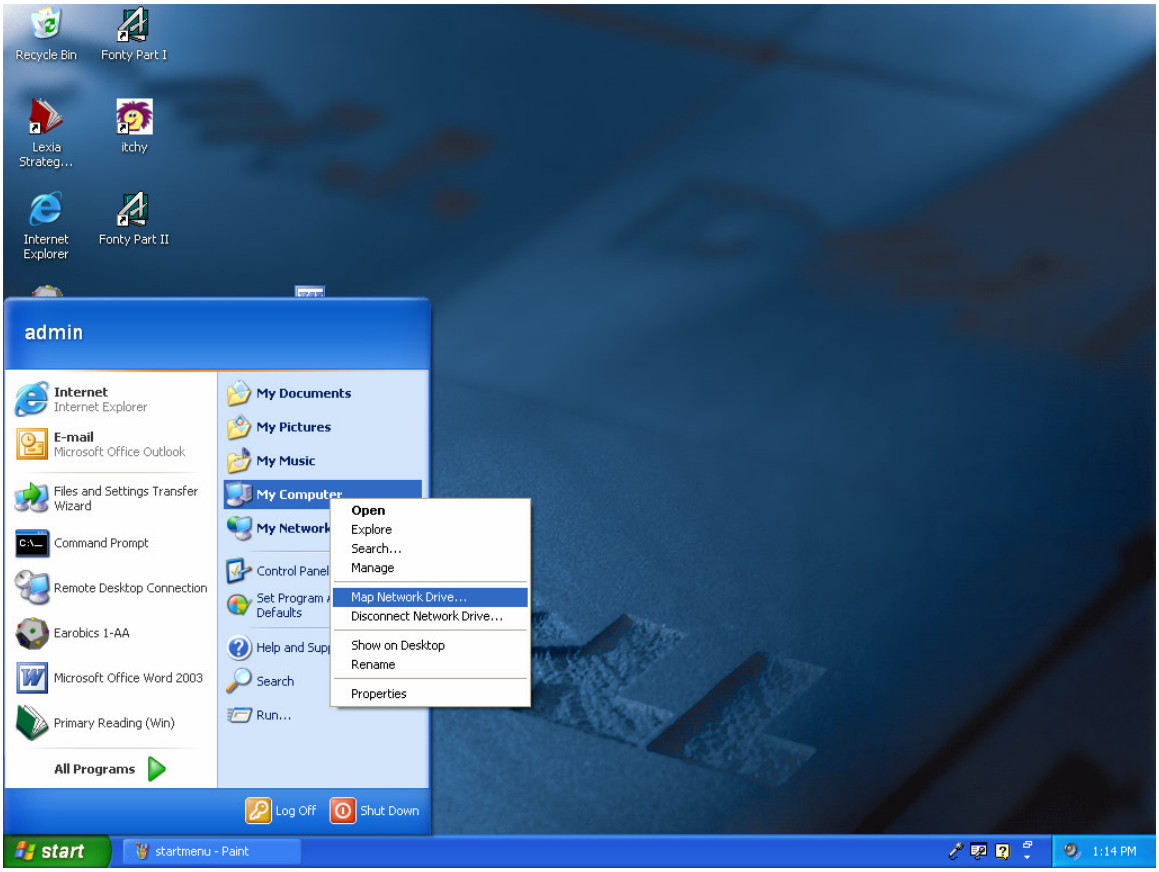
- Open a remote desktop connection to the server
    - Start -> programs -> accessories -> communications -> remote desktop connection
- In the box, type in “clc-server”
- Log in with the administrator username and password
- Double click on the Lexia backup script shortcut “Backup Lexia Server” located on the desktop. This will automatically backup the database into a format and location on the data partition where it can be backed up.
- Insert a blank DVD into the DVD burner
- Open the Roxio Creator CD/DVD burning software by going to:
    - Start -> programs -> Roxio Creator -> burn a data CD
- From the drive selection, choose Data partition, and select all
- Click “Burn”. The DVD backup will burn and indicate when it has completed.
- Eject the DVD from the recorder, and store it offsite

Appendix B: Example instructions to rebuild the network (for disaster recovery purposes):

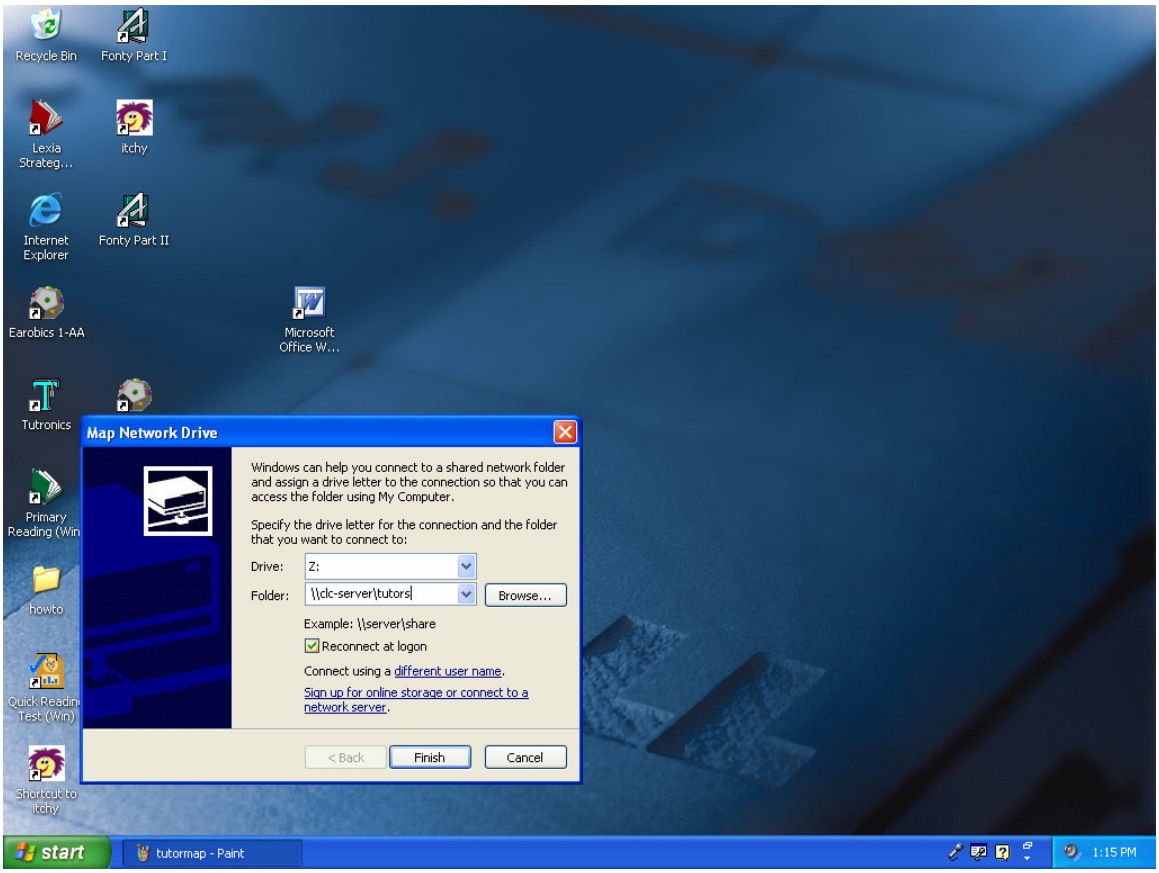
- Configure the network cabling according to the above network diagram.
- Reinstall Windows 2003 standard server and Windows XP Professional on the server and desktop computers using the OEM CDs that came with the systems
- Server name: clc-server, desktop names: student1, student2, student3, student4
- Configure the server with a static IP address on the
- Configure the desktops with private IP addresses starting with:
    - 192.168.0.2, (subnet mask 255.255.255.0, gateway 192.168.0.1)
- On the server, install "Routing and Remote Access Service", Remote Desktop, and Active Directory (which will automatically install other services including Dynamic DNS).
- Configure the server as an Active Directory Domain Controller. Domain: CLC
- Configure the group policy settings for the domain, according to the list above.
- Join the workstations to the CLC domain.
- Install the Lexia server using the Lexia network installation instructions
- Share the network folders listed here:
- Share the network printers here on the server:
- Install the logging service on the server and the workstations
- Using the change log, apply any required configuration changes and patches that were previously made to the network.
- Install the Earobics and Tutronix software applications on the desktop PCs.
- Import the student account list
- Restore the Lexia database using the instructions in the Lexia Installation Guide
- Test all of the applications from a few student accounts to make sure the data is intact.

Appendix C: How to connect to the network document folder

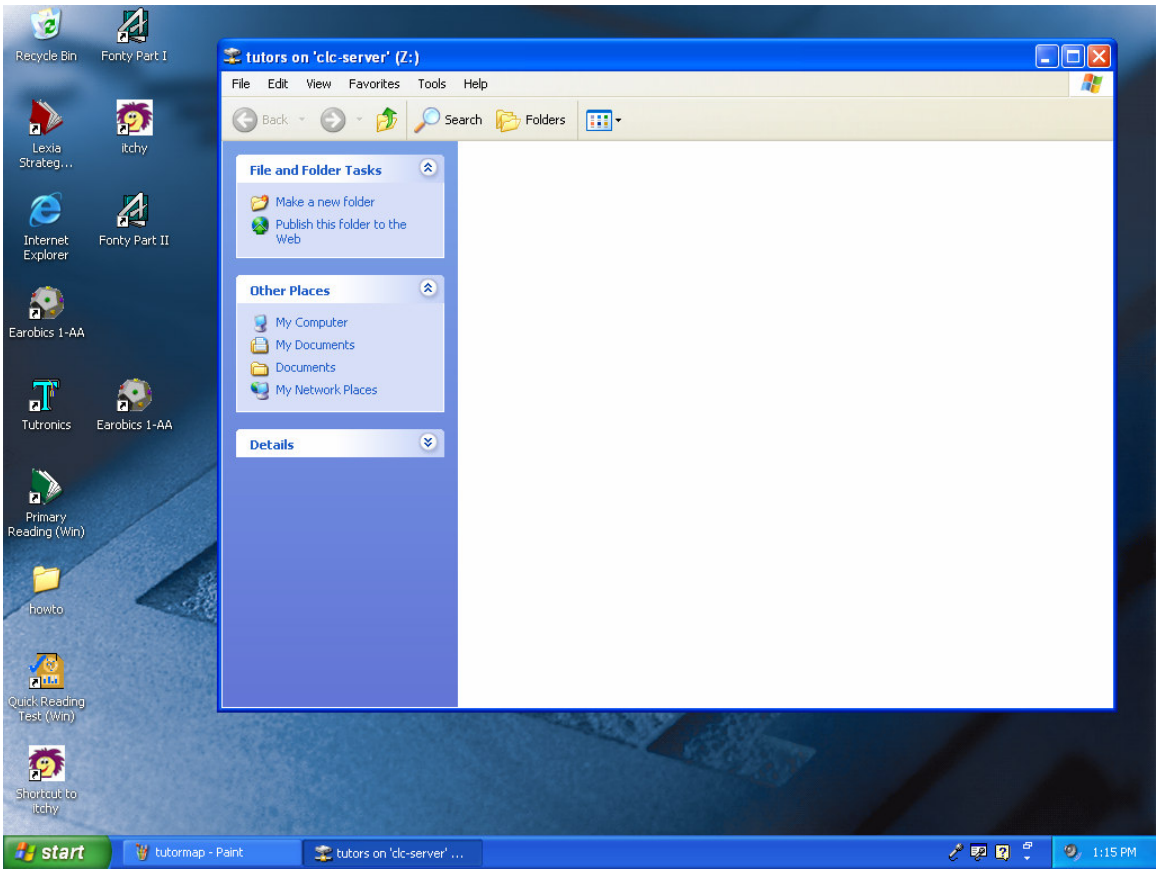
The network document folder is a shared folder on the server where the tutors can store their documents. Subfolders can be created on the file server underneath this shared folder with your name, and keep all of your documents you create there. This way, you can get to the files from any of the four computers in the lab.



From the start menu, right click (right mouse button) on “My computer”, and choose “Map network drive” from the Menu.



In the folder box, type \\clc-server\tutors (without the underline). Check the box "reconnect at logon".



It should show you the “tutors” folder where you can save your files. If it asks you for a username and password, you should type the same username and password you use to log into the computer.

References

[1] Computer Security Practices in Nonprofit Organizations (2003). Retrieved April 24, 2007, from NetAction Web site: http://www.netaction.org/security/summary.html

[2] Stanton, J. (2006, Jan 17). CIA Triangle. Retrieved April 24, 2007, from WikiSec Web site: http://istprojects.syr.edu/~sise/flexwiki/default.aspx/MyWiki/CIA%20Triangle.html

[3] Vogel, V. (2006, Aug 18). Network and Host Security Implementation (Stage 2). Retrieved April 24, 2007, from Effective IT Security Practices and Solutions Guide Web site: https://wiki.internet2.edu/confluence/display/secguide/Network+and+Host+Security+Implementation+(Stage+2)

[4] Effective Practices and Solutions in Security (2006, Aug 15). Retrieved April 24, 2007, from EDUCAUSE Security Task Force Web site: http://www.educause.edu/content.asp?page_id=1246&bhcp=1

[5] Authenticity Consulting, LLC. (2007). Project Management. Retrieved April 24, 2007, from Free Management Library Web site: http://www.managementhelp.org/plan_dec/project/project.htm

[6] National Acadamy of Sciences (2003). Internet Laws. Retrieved April 24, 2007, from NetSafeKids Web site: http://www.nap.edu/netsafekids/pp_li_il.html

[7] Virus Related Statistics (16 Jan, 2004). Retrieved April 24, 2007, from SecurityStats.com Web site: http://www.securitystats.com/virusstats.html

[8] Acceptable Use Policy (2007, March 29). FL: Wikimedia Foundation, Inc. Retrieved April 24, 2007, from: http://en.wikipedia.org/wiki/Acceptable_use_policy

[9] Wireless Security (2007, April 22). FL: Wikimedia Foundation, Inc. Retrieved April 24, 2007, from: http://en.wikipedia.org/wiki/Wireless_security

[10] Leurs , L. (2003). RAID Levels. Retrieved April 24, 2007, from Prepressure Page Web site: http://www.prepressure.com/techno/raid.htm

[11] Anti-Virus and "Security" Products (2004, Dec 7). Retrieved April 24, 2007, from Claymania Creations Web site: http://www.claymania.com/anti-virus.html

[12] Messmer, E. (2007, April 5). Has the end arrived for desktop antivirus?. Retrieved April 24, 2007, from Network World Web site: http://www.networkworld.com/news/2007/040507-desktop-antivirus-dead.html

[13] Fulton, S (2006, June 30). The Principle of Least Privilege. Retrieved April 24, 2007, from Informit.com Web site: http://www.informit.com/guides/content.asp?g=windowsserver&seqNum=232&rl=1

[14] Gatewood, S. (2007). Security Checklist. Retrieved April 24, 2007, from EdTech Focus on Higher Education Web site: http://www.edtechmag.com/higher/august-september-2006/security-checklist.html

[15] Garbars, K (2002). Implementing an Effective IT Security Program. Retrieved April 24, 2007, from SANS Institute Web site: http://www.sans.org/reading_room/whitepapers/bestprac/80.php

[16] Edelhauser , K (2007, Jan 18). Is Vista the right fit, right now?. Retrieved April 24, 2007, from Entrepreneur.com Web site: http://www.entrepreneur.com/technology/newsandtrends/article173202.html