Securing a Small Community College-A Case Study

By: Bobby Hoyle

GSEC Practical Assignment Version 1.4

Abstract: The challenges of securing a community college are formidable. Resources are often limited, the use of computers and software applications vary greatly from department to department, the atmosphere of academic freedom permeates all decisions, exploring and experimenting students can reek havoc on campus networks, and the inherent mission of disseminating information, and providing computer access to a wide variety of users are just a few of the challenges.

This practicum identifies critical computing resources used in a small community college, develops a method of defining risk, presents a network design, as well as, implements security policies to address risks, and formulates a long term strategy for securing vital campus resources.

Background: The basis for this case study is a small community college in Arkansas. The college was formed approximately ten years ago by the merger of a junior college and a vocational technical college. It consists of two campuses approximately three miles apart. The campuses are connected electronically through a dedicated T1 telephone line, and receive Internet service through a state owned and operated frame relay network and ISP. There are approximately 400 pc's on the two campuses, eleven computer labs, and seven servers. The IT department provides a wide range of services to students, faculty, and staff. The following is a list of most of those services; email, remote access, Internet access, application services, print services, distance education, (student, faculty, and college web services), student records management, human resource management, fiscal records management, and access to approximately thirty different software applications.

The college network was a topographically flat network with no firewall as shown in Fig. 1 on the next page. Static Internet protocol addresses were assigned to computers and network equipment from three Class C domains. The academic and administrative networks were combined, causing students, faculty, and staff sharing the same media and application servers. VLAN's were not used, even though, over the last three years all hubs have been replaced with 10/100 megabit managed switches, and a significant portion of the data cable has been upgraded to Category 5e. Remote dial-in is provided through a Perle Remote Access Server, and a twenty-four line T1. Ten Intel based, and one Apple Macintosh lab house most of the workstation on the two campuses. Application servers were located on each campus to provide software for academic and administrative use. A Windows 2000 Advanced Server with Exchange 2000 provides email service for faculty and staff, and a Novell NIMS email server provides email for students. A Microsoft IIS based website was also located on the Windows 2000 Advanced Server. Approximately 30 printers are shared on both campuses using HP JetDirect print servers. Proteon routers on both campuses directed Internet traffic between the campuses and to the outside world. DNS services were shared between the Novell and Windows 2000 servers.

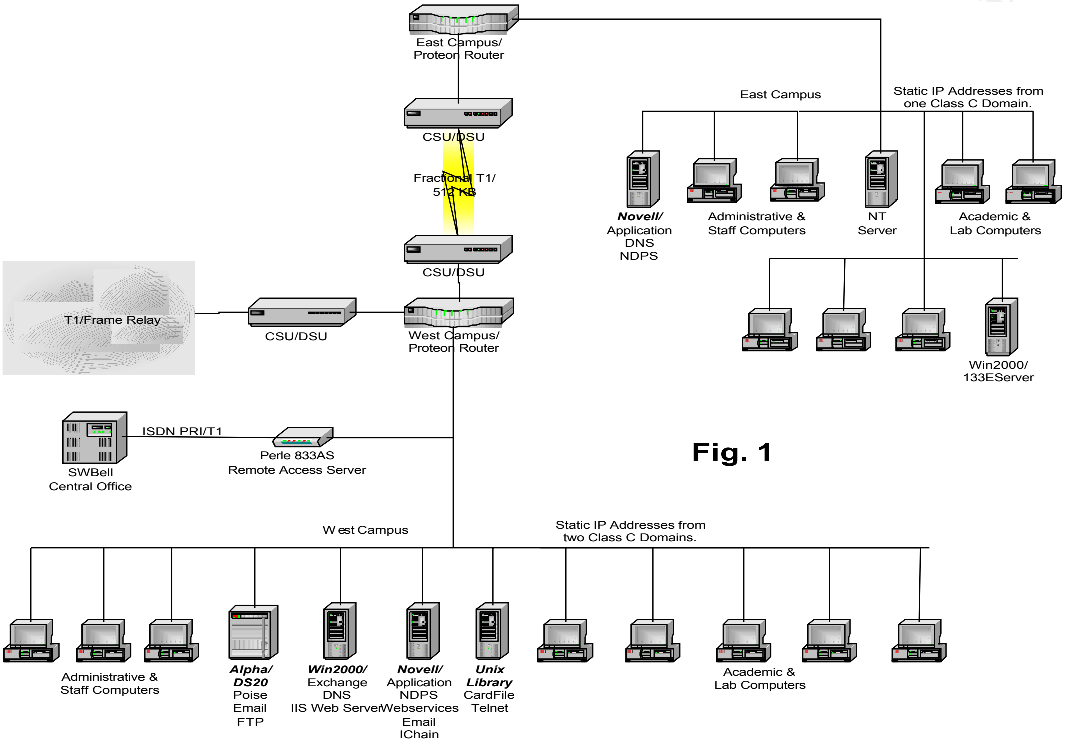

Fig. 1

The majority of mission critical modules are provided by proprietary database management software designed specifically for educational institutions. The software runs on a Compaq Alpha under Open VMS. Open VMS has a reputation of being very reliable and secure. The database modules include, but are not limited to, the following; student financial aid, electronic purchasing, recruitment, student academic records, accounts payable and receivable, leave, payroll, and inventory.

All servers are maintained by the Computer Services Department, except for Windows NT and 2000 servers on the East Campus. The NT server is maintained by the Industrial Electronics Department, and the 2000 server is used in a student supported graphics lab.

Risk Assessment: The first step in securing a network is to identify key informational resources, and the threat to those resources. Interviews with department heads from both campuses were conducted, to see where they were at and where they wanted to go with technology. Community colleges traditionally have had low Information Technology budgets. Recognizing vital informational resources can help in determining where the money, time, and computer staff's energy will be best spent. After each resource was identified, a value from one to ten was assigned each resource based upon how important the resource was to every day functioning and long-term goals of the college. While some resources get a lot of attention like email, the campus could function without it. However, the college could not function long without making payroll, finding financial aid for students, or providing academic records as needed. Certain services like computer training could not be performed if computer labs were not available. The value of some resources is harder to assess, because they pertain to the development and maintaining of the overall image of the college (i.e., Web Site). Some resources like switches and routers work in the background receiving very little attention, but are critical to the delivery of more visible resources like email.

The second part is to identify particular threats and determine how vulnerable the campus is to them. Each resource has unique threats and vulnerabilities. While some resources share threats because of the operating system and/or hardware platform they run on, others are at risk because of the very nature of there function (i.e. Web and Email Servers). Some operating systems have reputations of being more secured than others. Everyone has heard of the unending parade of security bulletins for windows products, while Open VMS garners the respect of military and high security personnel. Because of this, some resources you have to work harder at protecting than others. Table 1 list key resources, their value, and the type of threats they are vulnerable to. Below is the rationale for five of those reviews.

1) A proprietary database engine running under Open VMS on a Compaq Alpha server manages the institutional database. While its value to the school, as mentioned above, is great (a rating of 10); it is resistant to outside attack, because of the platform it runs on, and because Open VMS is not as visible as Windows. While all programs and operating systems are hack-able, those that catch the attention of the most hackers run the risk of being compromised most often. Past experience has shown us that the institutional database is most vulnerable to access by unauthorized personnel. As personnel move from position to position throughout the college they acquire rights to different modules in the database, allowing them access to information that may not relate to their present job function. Two other risks involve the need for remote access, and unattended open sessions on staff computers. These threats will be addressed later.
2) The email server is the most visible and popular service on campus. Most employees and students think they could not function without email; however, that probably is not the case. The email server runs under Microsoft Windows 2000 Advanced Server on a Dell PowerEdge box. It shares the operating system, and hardware platform with a Microsoft IIS web server, and DNS server. The Win 2000 platform has been compromised twice in the last year by viruses and worms, even though operating system and applications patches are installed within two days of release. It has been hacked once during that time also. While exploring and experimenting students pose a threat, the greatest harm comes from outside attacks. While the data transmitted by and stored on the server is sometimes sensitive in nature, it is not mission critical. The likelihood of compromise is high,

but the effects on 'day-to-day operations' are moderate. The greatest concern is that the server will be used in Denial of Service attacks on someone else's computers, or to spread worms, viruses, and Trojans to other computers. Nothing harms the reputation of an institution faster than to be linked to the spread of malicious code.

3) Routers and switches will be dealt with together, because they share common threats and vulnerabilities. Switches and router share the following vulnerabilities; SNMP protocol, web services management (IIS based), and telnet. Switches and routers do not store sensitive and vital information, but they are critical to the routing and transmission of said information. Because some switches use IIS based web management there were some reports of failures do to the Code Red Worm. The greatest threat comes from hacked switches and routers being used to deny service to valid user.
4) Computer Labs are most vulnerable from viruses and worms carried by students and faculty. While most students would consider their files mission critical, they are replaceable. Since most applications are provided from a server, the greatest risk is corruption of the operating, which leads to a Denial of Service. The loss of one computer lab for one hour can result in the loss of up to 30 man-hours of class work. Malicious altering of computer settings is common in most computer labs. It is difficult, however, to distinguish between accidental (in the pursuit of learning) and intentional vandalism sometimes. While workstation can be locked down to prevent modification, most teachers resent the frustration it causes. The value of computer labs to the function of the college is moderately high, and risk of being compromised is moderately high.
5) Office Computers have the most diverse group of threats and vulnerabilities. They face a double peril of loss of service and lost or corrupted information. Considered as a whole they contain a considerable amount of information. To complicate issues, most community colleges do not have the time or personnel to make periodic backups and disaster recovery disk. Office computers are almost equally at risk from outside and inside threats. The very user themselves can be a formable menace to the well being of the office computer, by loading unproven programs, engaging in chats, downloading contaminated programs, accessing off campus email sites, bringing infected disk from home, creating insecure remote access points, and removing sensitive information from the school premises. One staff person was responsible for sending out over 500 copies of the 'I Love You' virus. Because of the habits of most office workers, their computers are at a high risk from outside intrusion, Trojans, and worms, also.

In Table 1 a Mission Critical Value is generated to help identify which resources are most important to the functioning of the college. This information helps point out the resources that need to be secured first, and where to allocate limited resources. Column 1 list the key resources identified through interviews with department heads.

Column 2 contains relative replacement cost (in time and materials). Column 3 list the amount of confidential information housed on the resource. Column 4 contains an integrity value. Column 5 shows the relative effect on school function, if a loss of availability occurred. The Confidentiality, Integrity, and Availability columns are summed and then multiplied by the Value column. The number generated in the Mission Critical column is relative a value. It helps rank resources in order of importance. It is somewhat subjective, but it does correlate with expected results. The Institutional Database is the most valuable resource on the campus. The email services has a very high perceived value, and office computers play an important role in the everyday functioning of the college.

Mission Critical Value Table1

		Confi-		Avail-	Mission
Resource	Value	dentiality	Integrity	ablility	Critical
Web Site	5	0	5	5	50
Institutional Database	10	9	10	7	260
Application Servers	7	0	6	10	112
Email Servers	8	6	8	9	184
Print Servers	5	0	0	8	40
Switches	10	0	0	10	100
Routers	10	0	0	10	100
Communication Lines	8	0	5	10	120
Lab Computers	7	0	6	10	112
Office Computers	8	8	8	6	176
ISP Services	6	0	0	10	60
Remote Access Server	4	0	0	10	40

Table 2 is a summary of different types of threats against each of the resources. By knowing which threats resources are vulnerable to, helps define a defense strategy. Firewalls, email and packet filters, and intrusion detection may be most effective against external attacks, while education and security policies may help deal with internal threats. Some resources are more vulnerable to Denial of Service than others.

Threat Summary Table 2

			Threat		
Resource	Internal	External	Virus	Hacker	DoS
Web Site	3	7	8	8	9
Institutional Database	5	5	0	6	4
Application Servers	3	8	4	4	6
Email Servers	1	9	8	6	9
Print Servers	4	6	2	7	4

Switches	3	7	2	7	9
Routers	3	7	2	7	9
Communication Lines	1	9	0	4	9
Lab Computers	8	2	8	2	9
Office Computers	5	5	8	8	6
ISP Services	0	10	3	8	9
Remote Access Server	0	10	0	10	5

Security Policies: According to the *Sans Security Essentials II: Network Security* manual "Security Policies protect both people and information."(pg. 2-4A). Now that the most valuable resources have been identified, policies can be developed to protect those resources and the people who use them.

All community colleges are required by law to have some form of a policies and/or procedures manual. Security policies should follow the accepted school format as long as the purpose, background, scope, policy statement, action, and responsible parties are spelled out. Policies should be submitted for acceptance, modification, or rejection to appropriate administrators, committees or councils. Security policies are living documents and should be reviewed often. The Policy Summary Table below was created to help Computer Services staff understand how Security Policies complemented the overall strategy of securing the campus.

Policy Summary Table 3

		Policy	Plan of	
Resource	Risk	Purpose	Action	Responsibility
Web Site				
	Web site modified by staff.	Limit modify authority to approved personnel.	The President's Cabinet must approve Web Site editors.	President's Cabinet
	Web site modified by intruders.	Restrict edit/modify access.	Place Campus Web Service in a DMZ.	CSD
Institutional Database				
	Data compromised by staff.	Restrict access to individual modules to authorized personnel.	Vice-presidents approve access to modules for which they are responsible.	President's Cabinet

	Data compromised by intruders.	Insure strong passwords.	Change passwords every six months, be at least 7 characters, and unique.	Everyone
	Data compromised by students.	Prevent access from lab computers.	Place Institutional Server in Administrative V-LAN.	CSD
Application Servers				
Administrative/ Academic	DoS from Virus attack.	Restrict the spread of Viruses.	Scan all files entering the server. Periodic scans of all data volumes. Update pattern files regularly.	CSD
Administrative/ Academic	Data compromised by intruders.	Insure strong passwords.	Change passwords every six months, be at least 7 characters, and unique.	Everyone
Administrative	DoS from student attack.	Restrict access to administrative app servers.	Provide separate app servers for Administrative and Academic V-LANs.	CSD
Academic	DoS from student attack.	Restrict access to academic app servers.	Remove all guest accounts, and require individual logins.	CSD
Email Servers				
Administrative/ Academic	DoS from Virus attack.	Restrict the spread of Viruses.	Scan email entering and leaving the server.	CSD
Administrative/ Academic	Data compromised by intruders.	Insure strong passwords.	Change passwords every six months, be at least 7 characters, and unique.	Everyone
Administrative	DoS from student attack.	Restrict access to administrative email servers.	Provide separate email servers for Administrative and Academic V-LANs.	CSD
Academic	DoS from student attack.	Restrict access to academic email servers.	Remove all guest accounts, and require individual logins.	CSD
Print Servers				
	DoS due to unauthorized access.	Restrict access to CSD staff.	Change passwords every six months.	CSD

Switches				
	DoS due to unauthorized access.	Restrict access to CSD staff.	Change passwords every six months.	CSD
	DoS due to virus attacks.	Reduce susceptibility to viruses.	Download and apply updates monthly or as needed.	CSD
Routers				
	DoS due to unauthorized access.	Restrict access to CSD staff.	Change passwords every six months.	CSD
	DoS due to virus attacks.	Reduce susceptibility to viruses.	Download and apply updates monthly or as needed.	CSD
Lab Computers				
	DoS due to virus attacks.	Reduce susceptibility to viruses.	Download and apply updates daily or as needed.	CSD
	DoS due to unauthorized access.	Restrict access to registered students.	Remove all guest accounts, and require individual logins.	CSD
	Distributed DoS attacks.	Prevent the use of lab computers in the attack external computers and networks.	Filter IP traffic at the firewall.	CSD
Office Computers				
	DoS due to virus attacks	Reduce susceptibility to viruses	Download and apply updates daily or as needed.	CSD
	DoS due to unauthorized access.	Restrict access to employees.	Remove all guest accounts, and require individual logins.	CSD
	Trojans and unsolicited monitoring.	Prevent the disclosure and modification of sensitive information.	Install intrusion detection and personal firewalls on administrative computers.	CSD and users

	Distributed DoS attacks.	Prevent the use of office computers in the attack external computers and networks.	Filter IP traffic at the firewall.	CSD
Communication Lines				
	DoS due to severed trunks.	Encourage trunk line provider to provide redundant circuits.	Lobby legislature to require redundant circuits to southern region.	President's Cabinet and DIS

Once specific threats are identified security policies can be developed to address the risk. Below is a sample policy using the college's APM format concerning unauthorized access of Institutional Database modules.

Administrative Procedures Manual
APM 11.6
Access of Institutional Database Modules
Introduction: The Institutional Database is the most valuable information resource of ABC Community College. To protect this information and the people who use it, access to specific modules must be restricted to those who need access to perform job duties.

Background: As personnel change jobs within ABC Community College and as new staff is hired they sometimes need access to modules in the Institutional Database. The following policy statement addresses how to request and receive those rights.

Policy: The Vice-President in charge of that module will grant Access to Institutional Database Modules in writing, using Form A476. The Vice-President reserves the right to grant temporary or permanent access to other personnel on campus as needed. Employees caught accessing modules for which they do not have written permission may face disciplinary action as deemed necessary by administrators and supervisors.
Revised 3-7-2002

Security Plan: After looking at the individual threats each key resource faces, a comprehensive campus security plan can be developed. One security measure may be able to address multiple threats (i.e. A firewall can help protect multiple devices from several different types of attack.). An outside in approach was taken to designing the following security plan, starting at the outer perimeter of control, the gateway to the state network, and working inward. Figure 2 below shows a graphical layout of the changes made. The security plan is broken into steps for organizational purposes.

However, because of time requirements, and resource management issues, many of the steps were completed simultaneously.

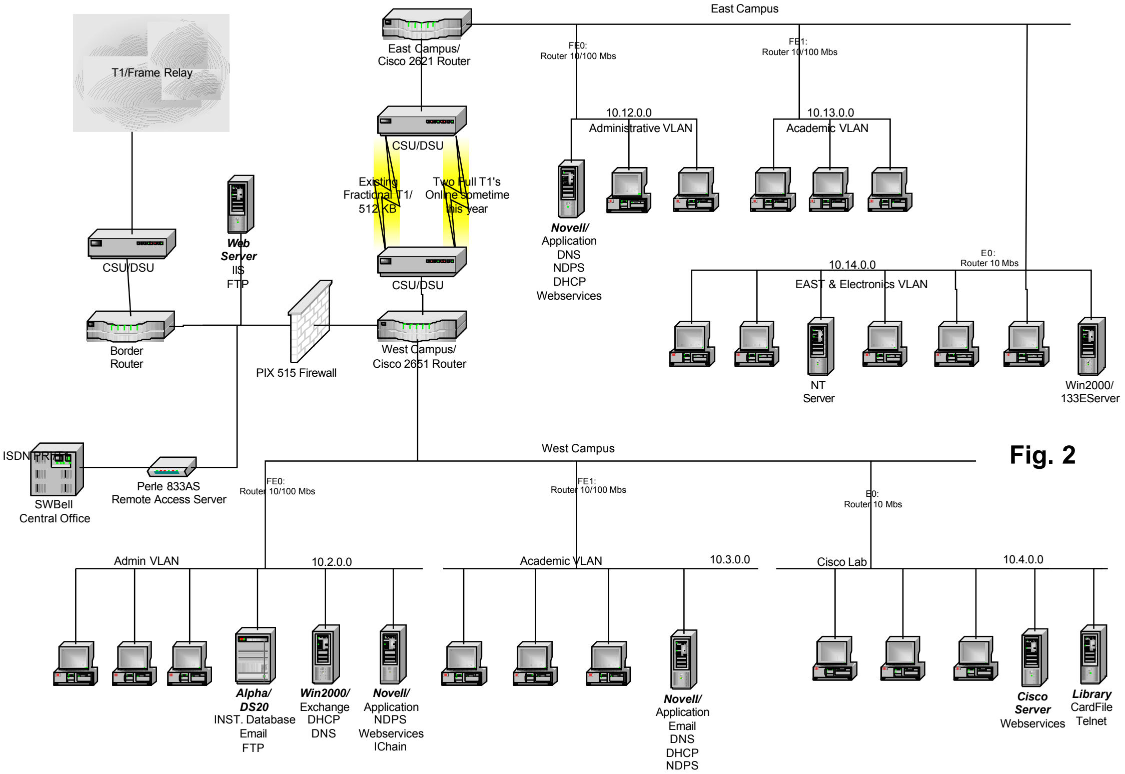

Fig. 2

Step 1: (Firewall and DMZ) Funds were obtained from a mini Distance Education grant to purchase a Firewall. A Cisco PIX 515R was selected because of its industry reputation, and because it is on state contract with a sizable price cut. However, not enough funds were available to add the DMZ option. A DMZ was created between a spare border router and the firewall. The college's website was moved to its own Windows 2000 server, and placed in the DMZ. This helps prevent cross contamination with the email server. The information on the web server is fairly static and can be restored quickly if it compromised. The border router will allow only port 80 traffic to reach the web server from the outside. The Perle RAS was also placed in the DMZ to allow remote users to authenticate through the firewall. The addition of the PIX Firewall allowed the transition from static to a private IP addressing scheme using Network Address Translation. ACL's were created to limit extraneous traffic into and out of the campus network. Providing some protection for the Institutional Database from external scanning. The firewall will play an increasingly important role as new features are added to the operating system, and new ACL's are created to deal with bothersome traffic.

Step 2: (VLAN's) Semester three of the Cisco CCNA training points out the importance of VLAN's in segmenting internal traffic (i.e. Students should not have access to administrative servers and networks.) Two Cisco 2600 routers were purchased from state contract using renovation funds. Each router contained two serial ports, two 10/100 Mbit Ethernet ports, and four 10 Mbit Ethernet ports. Each campus was segmented into three VLAN's (Administrative, Academic, and Cisco on the west campus, and Administrative, Academic, and EAST/Electronic on the east campus). The Institutional Database, the administrative email server, and the administrative application server were placed in the Administrative VLAN. This will restrict access by students to the Institutional Database. A new Novell server was created and placed in the Academic VLAN to serve applications and email for the students. The Cisco Lab and the Library's Card file Server are managed independently of the computer department. Network traffic is allowed to the outside world, but not to the rest of the campus. On the east campus students, faculty, and staff share a Novell Application Server. Academic and Administrative email services are provided by the two email servers on the west campus. Similarly, two computer labs (EAST/Electronics) are managed independently of the computer department on the east campus; they are granted access to the Internet, but not to the rest of the campus. This allows them to retain their academic freedom without jeopardizing the rest of the network. There are trade-offs, they can continue to manage there networks, but they do not have access to some campus resources like email.

Step 3: (Email and Virus Scanning) Virus and Worm attacks have increased three fold in the last year. Trend SendMail was install on the Administrative email server, and it is doing a good job of stopping most viruses and worms. Email scanning will be added to the Academic email server this year. The Administrative email server is also running Norton Antivirus to intercept viruses introduced into the network by faculty, staff, and students. Each workstation is loaded with personal antiviral software. Because of poor performance, a new antiviral application is being sought out. Lockdown intrusion monitoring software is installed on all upper level Administrative computers. Over the last two years Trojans have been found on several administrative computers, and remote monitoring has occurred from as far away as Norway.

Securing the Future: While the college has made a good start towards protecting its key resources, there is a lot of work still to be done. Listed below are some of the goals that have been set.

1) *Training:* Security and security tools are only as good as the staff that administer them. Security training has been budgeted for all computer staff in the coming year. Some of it will be done in house, as well as, from third party training facilities. A concerted effort is planned to inform faculty and staff to the importance of personal security in the office. Security policies will aid in defining actions and responsibilities.
2) *Firewall:* The firewall will be used more effectively to regulate and monitor traffic as the staff gains expertise, and as new features are added.
3) *Intrusion and Vulnerability Detection:* Active intrusion monitoring devices are

panned for the near future. Scanning for vulnerabilities and weaknesses is planned as the expertise is gained.

4) *Disaster Recovery:* A complete review of disaster recovery policies and procedures is planned. Redundant services are planned for each campus; allowing important data to be saved if a catastrophic event occurs on ether campus (i.e. fire, tornado, or chemical contamination)

References:

National Security Agency. (Feb. 18, 2002). *The 60 Minute Network Security Guide.* Ft. Meade, MD. Author Unknown

Federal Bureau of Investigation. (Aug. 29, 2001). *Congressional Statement on Cyber Security.* Location Unknown. Leslie G. Wiser, Jr.

Security Strategies
URL:http://www.microsoft.com/technet/security/bestprac/secstrat.asp?frame=true#top
(March 27, 2002)

Introduction to Network Security
URL:http;//www.interhack.net/pubs/network-security

OII Guide to Information Security
URL:http://www.diffuse.org/oii/en/secguide.html

Computer and Network Use Policy
URL:http://www.columbia.edu/acis/policy

Network Security Policy: Best Practices White Paper
URL:http://www.cisco/warp/public/126/secpol.html

Keslar, Gary C. (Jan 2001) *Non-technical Hurdles to Implementing Effective Security Policies.* http://www.garykessler.net/library/hard_security_policies.html

Fratto, Mike. (Dec. 17, 2001) Security-The Survivors Guide to 2002. *Network Computing, 15*

Cisco Systems. (2002) *Second Year Companion, Second Edition.* Indianapolis, IN: Cisco Press

Kaeo, Merike. (1999) *Designing Network Security*. Indianapolis, IN: Cisco Press

Allen, Julia H. (2001) *The CERT Guide to System and Network Security Practices.*

Boston, MA: Addison-Wesley

Sans Institute. (2002) *Sans Security Essentials II: Network Security*.
Location Unknown: Sans Institute. Pg 2-4A.