Global Information Assurance Certification Paper

GIAC Security Essentials Certification (GSEC)
Practical Assignment
Version 1.4
Option 2 - Case Study in Information Security

"Case Study: A Data Telecom Network Audit in a Large Corporation"

Submitted by David Larsen

June, 2002

Case Study: A Data Telecom Network Audit in a Large Corporation

Abstract

A network audit can present many opportunities for improvement in the security control environment. But before you jump in ready to perform a pen test, or other 'fun' stuff, there are high level concerns that must be addressed. Here are some real-world examples of what to look for, what you may find, what you can recommend, and actual results. Once basic controls are established, the door will open for more detailed review.

Introduction

The purpose of this paper is to describe the process and results of a network audit in a large corporation. In theory, it seems simple to apply standard security constructs to such an endeavor. For many of us the fun is in the detailed exploration of security vulnerabilities through the use of tools and other techniques; however, in the real world there are constraints that can make it difficult for one to use such methods in a meaningful fashion. The challenge then becomes one of maintaining focus on the 'big picture', enabling identification of weaknesses and areas of improvement in the security control environment. The intent of this document is not to supply an exhaustive list of auditable items, although it can provide a basis from which to prepare an audit tailored to the needs and circumstances of another situation. Rather, it is to provide examples of what to look for, and results one may (or may not) encounter. Hopefully, there is benefit to be derived from the experience described herein. Some excellent sources for more detailed information are listed under "References" at the end of this document.

The company examined is a multi-national commodity and service provider, with involvement in several areas of the energy sector, including power generation, natural gas transportation, and related trading activities. Most employees are based in an office tower in the company's home city; however, there are many satellite offices and field locations that utilize the corporate network to varying degrees.

The company relies on the availability and integrity of an extensive wide area private data communications network to support virtually every business activity. This network, and its associated management practices, has been constructed over the life of the company through several mergers and acquisitions, and is the product of a wide variety of components, technologies, and services. It is comprised of a variety of platforms, including NT, VMS, UNIX, Novel and associated hardware components. The situation is further complicated by a recent merger with another large company that employed different management practices and network architecture. The network is protected from external intrusion by the use of standard controls including firewalls and remote access servers.

Objectives

The primary objective of the audit was to provide an assessment of the current network control environment, make recommendations for improvement, and identify areas for more detailed review.

Specifically, the audit objectives were to:

- Determine if the network infrastructure components and servers were appropriately secure from both configuration and operational viewpoints
- Evaluate the effectiveness of management and operations practices and tools.
- Provide recommendations to improve management and operations practices and tools where appropriate;

To address risk that:

- Vulnerability to intrusion may be present due for variety of reasons including configuration, software version and patch levels, and operating practices on the physical network, servers and network devices, and in combination
- Intrusions and unauthorized activities may go undetected
- Vulnerabilities may be undetected, misunderstood, or inappropriately managed.

These risks are fundamental in nature, and may lead to adverse consequences including loss of confidentiality, integrity, or availability (CIA) of data and network resources, and increased cost of network operation. These potential consequences, together with common industry practice, were used to prioritize vulnerabilities for subsequent action or enhanced control.

Scope

The scope of the assessment included:

- Identification of potential vulnerabilities in operating practices on the physical network, on connected servers and network devices, and in combination
- Identification and assessment of current network vulnerability controls
- Prioritization of the vulnerabilities into categories of severity based on potential consequences, and in the light of common industry practice
- Recommendations of tools, processes, and standards based on common industry practice to appropriately manage vulnerabilities.

The scope did not include:

- Identification of specific potential vulnerabilities in hardware and software configuration
- Classification or valuation of the information accessible through the network, or the value of the network infrastructure
- A detailed threat assessment.
- Vulnerabilities to voice communication equipment or services
- Vulnerability to loss of availability caused by environmental incidents or equipment malfunction
- Review of field operations control equipment except as it interacted with the corporate network.

Methodology

The audit was performed using various 'best practices' as benchmarks, including ISO17799 and the COBIT control framework. The approach followed was:

- Through discussion with relevant personnel, obtain an understanding of key business processes supported and associated areas of risk
- Discuss the network history, architecture, future direction, and concerns with IT staff
- Obtain and review current documents, including policies and procedures, architecture specifications, management reports, etc.
- Perform control analysis in light of industry 'best practices'
- Conduct audit testing as appropriate to verify adherence (or lack thereof) to 'best practices'
- Validate findings with IT management
- Prepare a summary report highlighting control weaknesses and recommendations for improvement
- Provide a detailed observation matrix including prioritized risks and recommended mitigation measures.

The audit was segmented into the following areas of examination:

1. Policy and Management Practices
2. Outsourcing
3. Architecture
4. Logical Security
5. Monitoring
6. Incident Response
7. Change Control
8. Remote Access.

Areas of Examination

I. Policy and Management Practices

Risk

Without clearly defined and communicated policies there is no framework from which to derive security practices and procedures. In the absence of such guidelines, and consistent management practices, security measures may not be applied comprehensively (if at all), and responsibility may not be defined.

Examples of Audit Criteria

- Is there a clear and concise security policy?
- Does in incorporate standard elements (e.g., purpose, background, scope, policy statement, responsibility, action)?
- Has it been successfully communicated (i.e., are people aware of, and familiar with it)?
- Has it been used as a driver to develop lower level policies, risk assessments, and procedures with input from appropriate personnel?
- Is there evidence of upper management commitment to promoting and supporting information security?

- Are security responsibilities clearly defined, communicated and understood, including those for heads of business units/functional areas?
- Do management practices reflect the policy?
- Is there a process for review, update and approval of policy?

Key Findings

1. A policy covering corporate information management and security is required in order to provide substance and direction to all IT areas including telecommunications operations and management. In this case the policy had been drafted and tentatively approved but had not received final approval or been published.
2. A risk assessment of the telecommunications environment and infrastructure had not been conducted to evaluate business risks and threats presented by the architecture, configuration, and operating practices. Common industry practice recommends such an assessment as a critical step in ensuring that the correct controls are implemented in an appropriate manner to deal with those risks and threats which pose the greatest threat to the company.
3. There was a lack of clarity and consistency in operating practice and direction from IT management. This created a situation in which operational staff, support staff, infrastructure and other groups followed practices that varied by individual and/or group, and thus were not consistent. Examples of this were found in areas including change control, backups, granting of remote access, and others.
4. Communication and coordination between the various groups whose roles impact telecommunications security was inconsistent. This resulted in initiatives being undertaken without participation or input from all affected groups. Examples of this were found in the definition and implementation of an out-sourcing of security operations.
5. The process for resolution of identified telecommunications vulnerabilities and operating practice deficiencies did not facilitate the timely application of remedies. This could result in slow response to vulnerabilities that are immediately known and exploitable on the Internet.

Recommendations

1. The IT Security policy should be finalized, approved, and communicated.
2. A complete telecommunications risk assessment should be conducted, and appropriate controls evaluated to address the risks and threats identified. This should be done in addition to regular vulnerability scans performed on the network.
3. Operational and security practices should be standardized, integrated, documented, and enforced across operational, support, infrastructure, and other relevant groups. Notwithstanding the need for the IT Security policy, this effort should begin immediately from a day-to-day operating point of view and be adjusted to accommodate the policy when it is published.
4. Processes should be established to ensure all stakeholders are informed and involved in all aspects of security, operations, and management in a timely fashion.
5. Vulnerability and operating practice deficiency management processes should be coordinated and streamlined so that fixes for identified security problems can be

implemented in a timely manner. Good practice recommends that the time to fix be within 2 to 3 days from detection or notification of the problem.

Results

Management agreed to take steps to address all of the recommendations, including a detailed risk assessment for which budgetary approval was obtained. However, it should be noted that significant time has now passed, and some action plans have not been completed. Most notable is the risk assessment, which is only now being developed. This means the company has been exposed to risks associated with the audit observations in the interim, as well as those yet to be identified in the risk assessment.

II. Outsourcing

Risk

The company has an outsourcing relationship for many of its critical IT functions. This can lead to security practices that are not consistent, as the outsource company may follow its own standards. Roles and responsibilities may not be clear and there may be overlap of responsibilities between the two entities. The service provider may be unwilling to share its procedures as they are often proprietary. Lack of day-to-day involvement in security matters may result in unclear direction from IT management. All of these factors can contribute to security vulnerabilities.

Examples of Audit Criteria

- Is there an executed contract that delineates the responsibilities of both parties, including adherence to good security practice and standards?
- Have security responsibilities been communicated and accepted?
- Are there documented security standards that the outsource provider must follow?
- What do personnel from both sides see as their security responsibilities at an operational level?
- Is there clear guidance for security matters from an appropriate level of management?

Key Findings

1. The company had not provided sufficient direction or operational procedures to the outsource provider to ensure secure operation of the telecommunications network. This resulted in inconsistent application of security across the network.
2. There was no formal documentation of procedures to be followed by system administrators to fulfill their roles and responsibilities relating to administration, operation and maintenance of the network.
3. There were no documented job descriptions for individual support staff positions. High level job requirements were documented; however position details were still evolving and were not documented.

Recommendations

1. The company should work with the outsource provider to build a mutually agreeable set of common IT security working practices as part of a larger process to ensure

consistency across IT. The IT security policy should be the driving factor in determining the detail and extent of security practices to be followed.

2. The company should work with the outsource provider to implement and document current procedures followed by network administrators based on existing practices and procedure documents. Once this is complete and a gap analysis has been performed, additional procedures should be implemented to fill any identified shortcomings.
3. There should be formal job descriptions for each position within the outsource provider operations group that provides support for the corporate network. Documenting the job description will assist in defining the roles and responsibilities of each individual. Security responsibilities should be clearly outlined in employee role descriptions.

Results

Both parties agreed to review and document practices and procedures, and adopt the best of each. However, this proved to be a time consuming task and progress was slow. Once again, exposure was ongoing throughout the process, albeit minimized as time progressed. Interestingly, there are now legal disputes as to which party's intellectual property the resultant procedures are.

No agreement was reached on formal job descriptions, as the contract with the outsource provider was service based, not role based. This created something of a 'black hole', where personnel were interchangeable and it was not always clear that familiarity with responsibilities, and knowledge of the systems were intact.

III. Architecture

Risk

If due care has not been exercised in network architecture design, implementation, and modification, there may be points of vulnerability that allow unauthorized access and other compromises of network security. Further, if periodic review does not occur, the network may be susceptible to new exploits and threats.

Examples of Audit Criteria

- Is there current network configuration documentation including network diagrams, and a process to update them on a timely basis as changes occur?
- Is there evidence that appropriate consideration has been given to security in the network design (i.e., has the architecture been reviewed and approved by personnel with the necessary security skills)?
- Have points of access been minimized?
- Is the network configured to limit access to only those areas required?
- Is there a process to stay apprised of updates, patches and newly discovered vulnerabilities?
- Do plans exist to address known weaknesses?

- Do processes exist to evaluate and address security effect when changes to architecture are made?
- Is configuration information included in backups?

Key Findings

1. In most cases observed, the amalgamation of networks required during the corporate mergers and acquisitions appeared to have been done using the most expedient methods available. The result of this is a complex network infrastructure derived from the overlaying of opposing network architectures. This complexity creates the opportunity for gaps in security and operational controls, and makes the network difficult to manage and potentially easy to penetrate.
2. Some business partners had access through frame relay connection to the internal network. The control over this access was not clear.
3. The field operational control systems were not completely segmented from the internal network.

Recommendations

1. To the extent possible, the network should be standardized and simplified, utilizing standardized hardware and software platforms. Internal network segmentation should be implemented with traffic filtering, scope limitation, etc., to prevent network-based attacks.
2. All business partners should enter the network via the firewall in order to impose restrictions on access rights and provide a log of the business partners' activities on the network, which may be audited at a later time, if necessary.
3. Field control systems should be segregated from the corporate WAN to avoid cascading of problems or intrusions from one subnet to another. Approved connections should pass through links that enforce strict network traffic segregation.

Results

IT Management agreed to standardize and simplify the network in conjunction with an impending move to a new building. However, segmentation of the internal network is a significant deviation from the company's existing principle of providing unlimited internal access. They agreed to review the viability of this approach, and to review the operating cost impact with the business to determine if it is acceptable.

Business partner access was routed through the firewall.

IT Management believed the networks were adequately segregated, and thus did not agree with that last recommendation. Their current practice was reviewed and endorsed by the business, primarily from a cost/benefit perspective.

IV. Logical Security

Risk

Without adequate logical security controls, there is the risk of unauthorized access to system resources, applications, and data; and that access rights may not be commensurate with need.

Examples of Audit Criteria

- Are unique IDs used for each individual?
- Are appropriate approvals in place for accounts and associated access rights?
- Is access appropriate for the business purpose?
- Does assigning of rights/permissions follow the principle of 'least privilege'?
- Is there a process for granting, reviewing, and removing access on a timely basis?
- Are password practices adequate (e.g., minimum length, special characters, enforced periodic change, etc.)?
- Is strong authentication used where appropriate?
- Are password files encrypted?
- Is there lock-out after unsuccessful log-in attempts?

Key Findings

1. There was no process in place for periodic review of user accounts and associated access rights. The number of user ID's with 'superuser' access was excessive. As well, there are many accounts for users who no longer require them.
2. ADMN and ROOT accounts were in some cases used for daily administration and maintenance. Knowledge of these passwords by current and former staff was excessive. Therefore, changes made with these accounts could not be traced to a specific individual.

Recommendations

1. A review of all accounts and privileges should be performed to establish a current baseline. A process should be implemented for regular review of user ID's and associated rights, to ensure that access to is limited to the minimum required to fulfill the user's job function, and that access was removed or modified when a person's role changed.
2. Knowledge of the administrator/root password should be restricted to a limited number of people, such as the manager of operations or security, senior IT management or individuals with similar responsibilities, and only used in extreme circumstances. To ensure limited knowledge of the password, it should be changed regularly, and when anyone entrusted with the password leaves. Given the rarity of its use, the password should be written down and secured in such a way that its recovery will be noticed.

   Individual accounts should be used to access systems at all times, with assumption of administrative or root capability only when required. Users with administrative or root privileges should also have normal privilege accounts to be used for day-to-day activities. Privileged accounts should only be used for tasks requiring that privilege. Root partitioning software should be installed.

Results

As it would be difficult to present a case to the contrary (i.e., common sense should prevail!), all of these recommendations were acted on.

V. Monitoring

Risk

Without sufficient monitoring tools and mechanisms in place, there isn't the ability to detect potential or actual malicious intrusions and other unauthorized activities; or to assess and optimize network performance.

Examples of Audit Criteria

- Is there logging and review for key events and operations such as unauthorized access attempts, log-on/off by user ID, successful/unsuccessful log-ons, all privileged operations, system alerts, access policy violations, and network traffic load and patterns?
- Is the network regularly scanned for known vulnerabilities?
- Are file integrity tools are used?
- What mechanism is used to control and monitor external access to internal resources?
- Is there a process for regular update of virus signatures, vulnerabilities, etc.?
- Are there appropriate intrusion detection systems in use?

Key Findings

1. Policy compliance and intrusion detection software to ensure system and user compliance with security policy had not yet been completely installed.
2. Virus protection software was not present on all servers.
3. Some aspects of system logging were inadequate to provide sufficient information for the investigation or re-creation of events surrounding a security incident. For example:
   - Log entries for access via modem pool were overwritten after approximately 90 minutes
   - There was no logging of VPN connections made to the Intranet
   - Log files of user access to the Internet did not easily associate Internet connections to specific users
- Logs generated by some network devices, including the firewall, were not reviewed on a defined basis for irregular activity.
4. There was no centralized process for collecting, reviewing and distributing various vulnerability updates.
5. Vulnerability scans were not performed in a timely fashion.

Recommendations

1. Policy compliance and intrusion detection software should be installed. A program of upgrades and training for these packages should be maintained.

2. Anti-virus software should be installed, monitored and maintained on all servers, including those at the network perimeter to scan any incoming traffic for possible virus infections.
3. Logging should be installed and monitored at a reasonable level on all servers and infrastructure components, including routers and VPN devices. The log files should be able to accommodate a minimum of one week's events. Log files should be retained in a location to which the administrator of the service being logged does not have write access. Procedures should be implemented for the timely review of log files, and investigation of any identified irregular activity.
4. Network administrators should develop and maintain a centralized repository of vulnerability information to further enable the system support function. This should be a corporate initiative covering all aspects of IT security.
5. Vulnerability scans should be performed on a regular basis to ensure that:
    - network security is maintained at the level dictated by the IT security policy
    - identified vulnerabilities have been patched
    - new vulnerabilities are discovered and fixed before they can be exploited.

    The frequency of these scans should be determined by the rate of change within the network infrastructure, increased scans performed with higher levels of change. Vulnerability scanning should include password testing to reduce the number of weak passwords and those which do not meet the requirements of the IT security policy.

Results

Most of these recommendations were implemented in a reasonable time frame. However, the state of IDS deployment remains somewhat unclear.

VI. Incident Response

Risk

Without appropriate procedures, response may not be sufficient to prevent unauthorized access or other incidents, and minimize their effect on organizational resources and processes.

Examples of Audit Criteria

- Are there clear, defined, and up to date procedures for responding to an incident, including identification, prioritization, isolation and containment, elimination, return to normal operations, point of contact, and escalation?
- Are relevant persons familiar with their responsibilities in such a case?
- Have procedures been tested?
- Is there a process for updating procedures and applying lessons learned?

Key Findings

1. The only documented incident response procedures observed in this review were for major incidents and viruses.

2. There were no clearly defined channels for the reporting or escalation of security incidents.

Recommendations

1. More extensive incident response procedures should be documented, approved and implemented. These should cover all classes of incidents, and integrated into the major incident response process.
2. A process should be established for reporting, documenting, and following up on security incidents. This should include communication with all stakeholders.

Results

The audit was successful in promoting the development of incident response procedures. However, there has not yet been an opportunity to review the effectiveness of the procedures. In view of the still uncertain state of the company's intrusion detection capabilities, one may wonder if there will be an opportunity to do so!

VII. Change Control

Risk

Formal change control procedures are necessary to prevent unauthorized, inadvertent, or untested changes from being deployed in a production environment. Such situations may lead to loss of network availability or compromise of confidentiality and integrity of network traffic and connected systems.

Examples of Audit Criteria

- Are documented procedures in place for:
  - Identification and recording of changes
  - Assessment of impact of change
  - Approval of changes
  - Communication of changes
  - Testing of changes
  - Rollback of changes?
- Are separate environments maintained for test and production activities?
- Is there a formal migration process?
- Are the procedures communicated, understood, and followed?

Key Findings

1. Happily, this was one area where controls appeared to be adequate in most respects. Procedures were in place for major changes and were being followed. The only audit observation was that there was not a corporate standard. There was more than one recognized change control methodology and toolset in use.

Recommendations

1. A standard methodology, procedure set and software tool should be employed throughout the company. This will reduce cost, promote familiarity, and facilitate support.

Results

The company adopted the tools and methodology of the outsource provider for network related changes.

VIII. Remote Access

Risk

Without stringent controls around remote access to the corporate network, there is the possibility of unauthorized or inappropriate access with the resultant potential for network failure, or loss of data and system CIA.

Examples of Audit Criteria

- Are all entry points to the network identified and documented?
- What processes are used to control and monitor external access to internal resources?
- What are the policies regarding entry to the Intranet via remote access?
- Has operations and support staff been adequately trained on VPN access and security?
- Can remote users connect to the Internet?
- What has been done to harden the VPN server?
- Are the business requirements for granting remote access documented?
- How is it determined what access rights will be associated with remote access connections?
- What is the classification and typical volume of data which is remotely accessed or exchanged?
- How accessible is data on the Intranet to external parties?
- What is the duration of access, by session and by lifespan?
- What is an acceptable degree of exposure for remote access?
- What method of authentication is required for remote access?
- How often are approved remote computing requests reviewed?

Key Findings

1. Dial-up access provided an inadequate audit trail and logging.
2. There was no rigorous process for the approval or review of requests for remote access. Nor was there a defined process for periodic review and update of user rights assigned to remote access user ID's. This allowed user rights to be carried as

employees' positions and job responsibilities changed. There were also active accounts for individuals who no longer required remote access.

3. The Internet access provided by the company to its employees had been configured in such a way that anyone with access to the network could use the company as an ISP.
4. The VPN utilized a 'split tunnel' which allowed a remote PC to be connected simultaneously to the company and the Internet. This created the opportunity for an intruder to gain access from the Internet to the corporate network.
5. The VPN servers were parallel to the firewall. This did not allow the VPN to benefit from the security features of the firewall.

Recommendations

1. Access to the internal network should be captured in log files to provide an audit trail which can be used to recreate the events leading up to and during a security incident.
2. Establish a standardized process for approval of remote access accounts with appropriate review, authorization, and documentation. This includes business justification for analog lines. Also, conduct periodic review of user access, including inactive accounts and access rights. Establish a process for removal/update of rights when people leave the company or their roles change.
3. Re-evaluate the company practice of provision of Internet service as part of a remote access account, recognizing the potential liability which may be incurred by acting as an Internet service provider. If Internet access is to continue to be allowed via a remote access account, guidelines for such usage should become part of the IT security policy.
4. Require all remote PC connections to the VPN to have personal firewalls installed. This will reduce the risk of intrusion from the Internet.
5. Move the VPN servers behind the firewall and configure the firewall to enforce appropriate filtering, etc.

Results

Management agreed to, and acted on the audit recommendations, with the exception of the personal firewall recommendation. They determined that the associated risk was not high enough to justify the effort and expense.

Conclusion

Overall, one would have to rate the overall state of the company's security as poor. However, this is based on the somewhat idealistic views that many of us maintain, having more familiarity than management with what 'should' be there. In reality, the situation is probably not as grim as it appears. This is born out to a certain extent by the lack of incidents the company has experienced. But would they know if they had been attacked? Difficult to say. Perhaps in this case, ignorance is bliss.

Sometimes what is needed is a high profile hack to raise security awareness (not that I am in any way promoting such an endeavor). Otherwise, the management view (especially

on the business side, and they sign the checks) tends to be, "Hey, we haven't had any trouble so far, so why worry about it?"

We were fortunate for this review in a couple of respects. First, it was conducted within the auspices of the company's Internal Audit department. As such, management has a measure of responsibility to act on recommendations, as issues can be elevated to the Board of Directors if they are not taken seriously. Second, the events of September 11 have raised everyone's security consciousness, so there was less resistance in some areas than may have been experienced otherwise.

As well, some of the issues identified were just plain embarrassing to management (I would expect my 12 year old daughter to follow better standards than some we encountered). Once risk is clearly identified for management, they will usually act. For these reasons, we achieved good results with our recommendations.

The experience was frustrating to a certain extent. From a personal standpoint, I was hoping to get into the nuts and bolts of the network security. However, it quickly became apparent that there were too many high level controls missing to get into the detailed aspects of information security assessment, such as router configuration, server hardening, etc.

Management also has the right (in most cases) to accept the risk once it has been identified. So, while we may believe some vulnerabilities should clearly be addressed, management may chose not to. At that point, our hands are often tied. 'Best Practices' is a nebulous term; the reality is that business must often practice triage. 'Best Practice' for one company may be excessive for another, based on resource constraints, risk acceptance philosophy, and other considerations.

It is worth noting that management commitment diminishes over time. While we achieved consensus on most of our findings, some recommendations are still outstanding. As other issues come to the fore, others must take a back seat. For this reason it is important to have a follow-up process. Otherwise, action plans may just wither up and go away.

The bottom line is that we were able to contribute greatly to an enhanced state of security. There is ongoing exposure, but controls are now in place. In the future we will examine the effectiveness of the controls. In other words, the building blocks are now in place, and we can return to test the mortar between the blocks. That is, if the foundation doesn't crumble first.

References

1. Information Systems Audit and Control Association. COBIT 3rd Edition. Rolling Meadows: ISACA, 2000.

2. ISO/IEC. ISO/IEC 17799. Geneva: ISO/IEC, 2000.

3. Allen, Julia H. CERT Guide to System and Network Security Practices. Upper Saddle River: Addison-Wesley, 2001.

4. Vallabhaneni, S. Rao. CISA Examination Textbooks, Volume 1: Theory. Schaummburg: SRV Professional Publications, 1996.

5. SANS Institute, GSEC Course Material, 2002, SANS.

6. International Information Security Foundation. "Generally-Accepted System Security Principles (GASSP)". V1.0. June 1997.
   URL: http://web.mit.edu/security/www/GASSP/gassp021.html (June 12, 2002).

7. Information Security Forum. "The Forum's Standard of Good Practice". November, 2000.
   URL: http://www.isfsecuritystandard.com/pdf/FSOGP_2000.pdf (June 13, 2002).

8. BITS IT Service Provider Working Group. "BITS Framework: Managing Technology Risk for Information Technology (IT) Service Provider Relationships". V3.2a. August 17, 2001.
   URL: http://208.184.31.25/FrameworkVer32.doc (June 12, 2002).

9. Boran, Sean. "IT Security Cookbook". 2000.
   URL: http://www.boran.com/security/it10-lan-wan.html (June 13, 2002).

10. Sutton, Virginia. "Change Management Audit Program". 1999.
    URL: http://www.auditnet.org/docs/chngmgmt.txt (June 12, 2002).

11. Lee, Joseph. "LAN Audit Program". Date unknown.
    URL: http://www.auditnet.org/docs/lan2.txt (June 12, 2002).

12. Author unknown. "LAN (Local Area Network) AUDIT PROGRAM". Date unknown.
    URL: http://www.auditnet.org/docs/lan4.txt (June 12, 2002).