Global Information Assurance Certification Paper

GIAC Bookreaders:
Security for a Small Business Planning to Grow

GIAC Information Security Fundamentals+
Practical Assignment
Version 1.0 (November 17, 2003)

Dan Steinberg

TABLE OF CONTENTS

ABSTRACT

GIAC Bookreaders, an organization providing services to independently-owned bookstores, is small and young, but maintains a security program appropriate to its size, needs, and ambitions to expand. Despite its small technical staff and lack of full-time security staff, GIAC manages to conduct risk assessments; to address management, operational and technical security issues; to develop data backup and recovery strategies; and to establish basic Disaster Recovery and Business Continuity Plans. GIAC Bookreaders' security program is an illustration of the basic principle that no organization is too small, too limited in its resources, or too new to incorporate essential security safeguards into its plan of operations.

I. Description of GIAC's Business

GIAC Bookreaders provides services to a membership of independent bookstores, with 75 "client members" in seven states in the Northeast, and with a business-wide main office in Somerville, Massachusetts. While each bookstore is an independently owned and operated concern, they share a database of inventory, an e-mail system, and a financial reporting system. Each client member signs a legally-binding document under which it acknowledges what services it expects to receive from GIAC Bookreaders, and its intention to abide by GIAC Bookreaders' inventory updating requirements and information technology policy; and also agrees to pay an annual fee (on a sliding scale, dependent on each member's profits) for ongoing technical and marketing support.

GIAC Bookreaders grew out of a concern held by some industry participants that small independent bookstores were no longer able to compete with online booksellers such as amazon.com and borders.com; online auctioneers such as eBay, and large chains of bookstores such as Borders and Barnes & Noble. GIAC's business strategy is to address common negative perceptions about independent bookstores by: 1) providing a shared database that lists all titles available at all locations, such that staff can locate titles either in-store or at other GIAC member locations and request they be shipped in; and 2) providing the services of marketing and finance specialists. Online purchasing is not yet an option for GIAC customers, but the CEO is interested in offering that service within the next five years. While joining the GIAC consortium has required most of these formerly-independent bookstores significant initial capital outlay in IT and other restructuring, most have increased their net profits by up to 20% after three years.

After initial investment losses for the first three years, GIAC Bookreaders has also begun to realize a small profit. Net revenues in 2003 were $8.3 million; net expenses were approximately $7.7 million ($5.8 million in salaries and $2.5 million in infrastructure and other expenses).

The size of each member bookstore varies, but for the GIAC business model to prove effective, GIAC recommends that independent stores interested in contracting for GIAC services have, as minimums: an inventory of 200,000 titles, a staff of ten, and gross revenues exceeding three million dollars.

This analysis, however, focuses on the main office, an independent corporation. That office employs a staff of fifty. This staff includes one Chief Executive Officer and general manager with a salary of $150,000; one Chief Financial Officer with an annual salary of $120,000; and eight IT staff with an average salary of $65,000 each. Other staff at the main office perform marketing, training, administrative, and human resources functions.

II. Description of GIAC's Information Technology System Architecture[1]

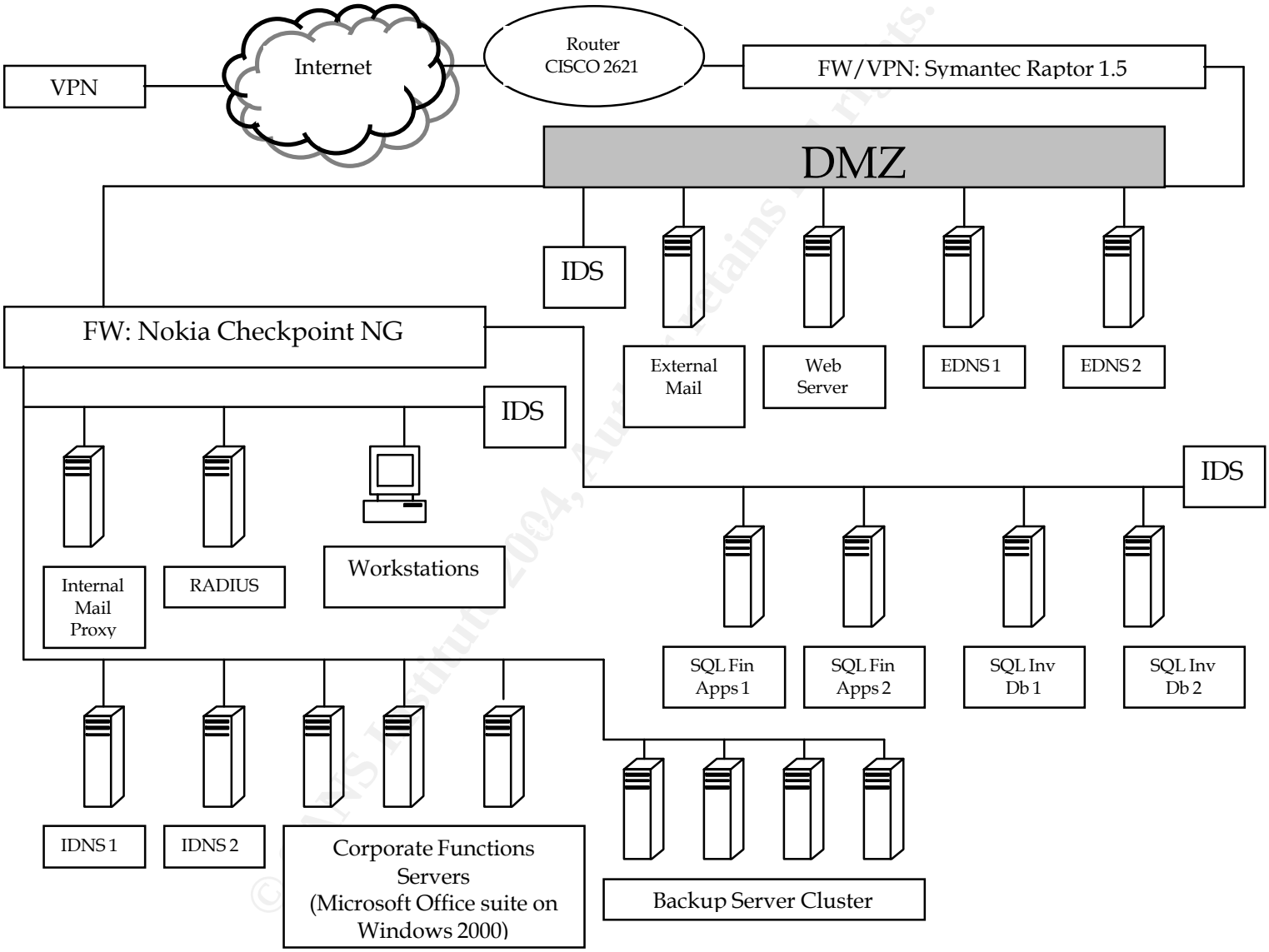

Diagram of GIAC Bookreaders' IT Network. The external firewall is a Symantec Gateway Security Appliance (GSA), configured to allow all properly addressed packets but to deny DoS attacks such as Smurf[2], and which also serves as the VPN appliance.[3]

---

1 For general information concerning network architecture, the author consulted Christopher Negus and Bill Wagner, *The Complete Idiot's Guide to Networking,* 3rd ed. (United States: Pearson Education Inc., 2001).

2 For a comprehensive discussion of secure router settings, see Vanessa Antoine *et al*, *Router Security Configuration Guide version 1.1* (National Security Agency, November 21 2001). http://www.nsa.gov/snac/cisco/download.htm.

The DMZ contains the external mail server, Web server, External Domain Name Servers and an Intrusion Detection system (SHADOW). The border router is a Cisco 2621XM, a low-bandwidth, low-cost, low-maintenance router[4] set consistent with SANS and CERT recommendations. The internal firewall has three connections: the external connection, the database servers for financial and inventory databases (with another IDS), and the business functions subnet housing the internal DNS servers, RADIUS authentication server, internal mail proxy server, workstations (IBM Thinkpads), corporate functions servers, backup server cluster, and a final IDS. This structure was put in place with growth in mind: If and when GIAC has the resources available, it would ideally like to provide greater security by screening off each subnet behind a separate firewall. The firewall protecting the subnet housing the databases could then be configured extremely restrictively (allowing no packets in or out not addressed to those databases, from addresses on the ACL, and sent to the correct ports). Office tools are operated on a Windows 2000 operating system with Service Pack 3, with workstations running Norton Antivirus. Web browser is Internet Explorer; e-mail is Netscape Messenger. The IT lab environment—a small local area network with no Internet connection or connection to the rest of the IT infrastructure, on which patches, upgrades, new software, and data backups are tested—is not shown.

III. Description of GIAC Bookreaders' IT Department

The Information Technology Department at GIAC Bookreaders consists of eight staff that reside in the Somerville, MA office. Its mission is "to implement, maintain, and amend as necessary all IT infrastructure necessary for the continuing successful function and future intended business growth of GIAC Bookreaders." The total budget for the office is approximately $750,000. Of this, $580,000 is salary plus benefits, and the balance is used for all infrastructure, software licenses, and travel expenses. As described in the introduction, GIAC Bookreaders is currently operating on a narrow profit margin of approximately five hundred thousand dollars.

The Director of Information Technology, who reports to the Chief Executive Officer, performs primarily managerial roles. His tasks include: reviewing reports on IT system performance, including system log reviews, system configuration analyses, incident reports, security plans, and capital investment plans; managing the budget for the IT Department; handling all human resources issues within the IT Department, including hiring, termination, performance reviews, and schedule coordination; tracking inventory (including hardware); and reporting system and Department performance issues to senior staff.

The Strategic Planner reports to the Director. Her tasks are: developing a strategic vision for the Department aligned with the corporate business vision; acting as central vendor liaison; coordinating with the marketing Department on promotional campaigns aligning vision with technical capacity; and monitoring the IT and publishing markets to identify potentially profitable trends and synergies of benefit to GIAC Bookreaders.

---

[3] Sidel, Scott. *Symantec Gateway Security Appliance: The Swiss Army Knife for SMBs.* Information Security Magazine: August 2002. http://infosecuritymag.techtarget.com/2002/aug/testcenter.shtml.

[4] For product specifications, see http://www.cisco.com/en/US/products/hw/routers/ps259/ps4832/index.html.

The Systems Analyst also reports to the Director. His duties are to manage system configuration; maintain access control lists for clients and staff; review audit logs of system activity, including IDS reports; update virus catalogs and install all system patches; maintain backup firewalls and routers; communicate IT Department policy and critical alerts to all GIAC staff; and make allocation requests and system investment recommendations.

The Senior Technical Specialist/Security Officer is the Director's third and final direct report. She is one of the five tech support specialists described below with additional duties, including drafting IT security policy to be approved by senior management and incorporated into the employee handbook; assisting HR in conducting of all new staff on IT security policy and procedure; promoting security through ongoing training and awareness, performing nightly backup of all mission critical data, including data stored on the financial and database servers; and assuring that monthly offsite backups are performed.

The responsibilities of the five tech specialists are described below.

IV. Description of Duties of a GIAC Bookreaders' Tech Specialist

There are four GIAC Bookreaders' technical specialists. They report to the Security Officer, and earn $55,000 per year. Each technical specialist has two chief responsibilities:

Handling technical support for both GIAC Bookreaders staff, as well as for client members using GIAC Bookreaders technical services. Requests normally come via phone, and if the client is in-house, technical specialists go to the staff member's workstation if necessary. Calls from GIAC Bookreaders clients are handled via phone. Because GIAC clients purchase and maintain their own computer equipment, technical concerns vary greatly with the clients' hardware, knowledge of technology, and training. Technical specialists can usually help personally with concerns that involve GIAC servers or services; problems that are not within GIAC's control, such as viruses on equipment it does not own, normally require staff to provide advice as to where the client must redirect his or her call. Technical specialists are evaluated at this task on the basis of their analytical skill in determining the problem, the speed with which they resolve the problem, and their courteousness and professionalism in the manner with which they resolve it. This task frequently involves security issues, including advising client members to prevent future problems by implementing security measures, such as by upgrading or updating their virus software or installing, at minimum, personal firewalls.

Traveling to GIAC Bookreaders client sites approximately once a month to inspect their IT infrastructure, advise improvements, and educate old and new staff about the use of GIAC Bookreaders applications and resources. This service is provided to all clients shortly after they become members of GIAC Bookreaders and at the request of any client member for an additional charge. At the end of each visit, technical specialists asked to distribute a minimum of two feedback forms to client staff technical specialists have dealt with directly, which allows clients to deliver feedback on the basis of their

efficiency, knowledge, courtesy, and ability to communicate. Other factors considered by technical specialists' supervisors include how well they implement and advise clients on security controls to anticipate and prevent security breaches.

Other technical specialist responsibilities include assisting with configuration, version, and patch updates to network elements; assisting in incident handling procedures; and monitoring the GIAC databases and updating its coding, as appropriate.

V. GIAC Bookreaders' Flow of Business

Enrollment of client members. GIAC Bookreaders is in a growth phase wherein it gains approximately two new client members per quarter. Solicitation of contracts is relatively limited, and occurs most often through telephone solicitation and follow-up contacts, and client-initiated contact. Once the client and marketing staff have agreed to the terms of a contract (normally a standard agreement), the client contracts with GIAC Bookreaders. Contracting with GIAC Bookreaders entitles the client member to two types of services: Marketing and Database services. It also requires each client member to fulfill two types of obligations: To maintain the accuracy and integrity of the inventory database, and to accurately and timely report its sales and financial performance.

Marketing services. Having contracted with GIAC Bookreaders, client members are entitled to four visits a year from a member of GIAC's marketing services division. Marketing services inspects the facilities and business operations of member bookstores, and advises as improvements member bookstores can make to displays, organization, staffing, inventory, and local advertising. Marketing has also been responsible for a number of special projects, including appearances at member bookstores by popular authors that support GIAC Bookreader's mission of promoting independent bookstores.

Database services. Each client member is individually responsible for ordering and maintaining its own inventory. Each client member must, however, submit a daily report of changes to its inventory to the GIAC Bookreaders inventory database. The database characterizes each item number by title, author, ISBN number, and category; at present, the database can accept entries for books, periodicals, CDs, videotapes, and DVDs. Client member staff may also access this database to locate items in the inventories of other client members; they then may arrange privately to order from each other, or may re-direct clients to those locations. Because GIAC Bookreader client members are geographically distant from each other, this service proves practical predominantly for those member bookstores whose inventory consists partially or wholly of used or rare books. Integrity of input data is also the responsibility of client members; one of the GIAC Marketing aqnd Sales Department's recent deliverables, however, was an advisory on best practices related to inventory control.

Financial services. Each GIAC Bookreaders client member submits, via computer using a GIAC Bookreaders custom web-enabled application, a daily financial report itemizing sales made by category of item, and overhead expenses. It also submits a quarterly financial statement that includes statements of overhead expenses including facilities, utilities, repairs and improvements, insurance, and other periodic costs. GIAC

Bookreaders reviews this documentation for three purposes. First, it uses this data to calculate the performance-improvement based portion of the annual fees client members owe GIAC Bookreaders. Second, working in conjunction with marketing services, Financial Services analyzes sales and financial performance for each location to identify trends and propose strategic plans to improve performance. Finally, it uses this information to form the basis for biannual audits conducted of each client member to verify accuracy of client submissions.

VI. Enabling Applications and Services

e-Mail. E-mail service is provided for communication among GIAC Bookreaders' staff and GIAC client members. Outlook Express is operated off of a single external mail server in the DMZ, which processes both incoming mail as well as mail sent and received within the internal private network. E-mail facilitates communications between and among virtually all departments and clients. Communications facilitate many different GIAC Bookreaders business functions, including GIAC-client interactions ("external" communications):

- Soliciting new clients;
- Negotiating terms of contracts and contracting with new clients;
- Coordinating site visits;
- Communicating news relevant to the industry and GIAC Bookreaders policy;
- Coordinating special events or initiatives; and
- Resolving problems related to access to GIAC information technology services.

Communications between and among internal GIAC staff ("internal" communications) include:

- Communicating regular reports on departmental activities up the change of command;
- Coordinating budgeting and capital planning activities;
- Coordinating human resources activities; and
- Disseminating information concerning company policy and practices.

Internet use. Internet services support the web-enabled Oracle Financial and Sales Applications used, and to maintain a minimal Web presence, consisting primarily of an explanation of GIAC Bookreaders' mission, philosophy, and services and contact information for the firm (and clients that agree to be listed, which currently all do). Internet service also supports secondary business functions such as market research; identification of vendors for office supplies, equipment, and IT; receipt of news related to the book and general retail industries; and other functions. Personal use of the Internet is tolerated, although an attempt is made via policy and managerial oversight to minimize it.

Financial application. The financial services reporting application is a customized version of Oracle's Financial and Sales Application. Access is restricted via the use of User IDs and password access only. GIAC client users report sales and expense reports daily via the VPN. Executives have "read-only" access to the database, and Financial Department staff with a business need has access to the information to develop market and sales analyses and forecasts.

Database application. Updating the inventory database is a function performed at individual client locations. Read-write access is granted only to individuals whose user IDs are added to a database access control list. The GIAC database specialists also have access to the database and update its configuration and investigate problems related to client access and verify the database's integrity.

VII. "Crown Jewels" of GIAC Bookreaders

Customer Identities and Related Information. The identities of the organizations that are GIAC Bookreader's client members are public information, and are in fact posted on the website, with links to each member's website if they have one. **Contact information,** however, is slightly more sensitive than the client member list, because it includes names of individuals, e-mail addresses and phone numbers as well as the names of companies. This information is widely-available within GIAC Bookreaders, as it is distributed by administrative staff in hard copy once a month. Of greater concern, however, is the highly sensitive **financial information** GIAC clients submit to the database on a daily basis. That information is available to members of the Financial Services and human resources departments in order to analyze sales trends and performance. Client members have "read-only" access to their own previously-submitted information, but may only modify submitted information upon notification to the financial department, and must explain the reason for the change (error, new information received, delayed submission, etc.).

Company Contracts. Standard agreements with GIAC client members are on file with human resources. In a few cases, modifications to the standard agreement have been granted if a particular clients' needs or structure justify such a modification; these changes are reviewed by retained counsel, which also retains a copy of the agreement. Contracts for goods and services are handled by administrative staff. Purchasing methods are done in one of several ways. For most low-cost consumables like office supplies, ordering is done online through well-known vendors such as Office Max. For office equipment such as printers and copiers, most purchasing is done through vendors that have approached the company. Those contracts have been signed face-to-face by GIAC executives, whose administrative assistants file copies of the contracts. For other technology investments, procurements are made on the basis of analyses and recommendations by the IT Department's strategic planner (with input and support of the rest of the Department). These purchases are then made via online vendors. Copies of receipts for all company purchases are submitted to the Financial Services department in hard copy.

Management Information. All GIAC Bookreaders' staff, including senior staff, receive an annual assessment from supervisors. A standard form, developed and distributed by the Human Resources Department, is used. Staff have an opportunity to review assessments and comment. Raises are awarded based on performance. Promotions, given the size of the company and its relatively low profit margin, are available only following vacancies. All of this information—Salaries, evaluations, and raises for all staff—is available to the Human Resources Department, which maintains electronic files and also hard copies of these documents. Supervisors also have this information available for their employees only. Employees are provided with hard copies of their own evaluations. Human resources develops an annual summary of these evaluations

and delivers it to the Financial Services department, which calculates raises depending on availability of revenue and relative evaluations of performance. On rare occasions, such as considering the termination of an employee for poor performance, evaluations may be made available up the chain of command in order to get consensus on the decision to terminate.

GIAC Bookreaders Inventory Database. Perhaps the most critical service GIAC offers is access to the **inventory database** that each member updates with a record of the contents of their stock. Client members have read-write access to the database in order to update and correct their listings. While most entries and updates are made via UPC code scans, the database also has the capacity for manual entries. In addition to read-write access, all client member sales staff have read-only access to the database in order to assist customers seeking to locate particular titles. The IT department also has access to the database to verify its integrity and availability, and to verify effective updates to the database as patches and upgrades become available from the vendor.

VIII. Insider Threat Vectors to GIAC Crown Jewels

In this section, common insider threats to the Crown Jewels identified are discussed. Any of the "hacks" (attempts to gain information) discussed could be used against any of the Crown Jewels identified. The IT Department has attempted, however, to identify the hack most appropriate to each Crown Jewel, i.e., the hack most likely, most devastating, or easiest for an attacker to use against that particular Crown Jewel.

Customer Identities and Related Information. Passive sniffing would be sufficient for any GIAC Bookreaders staff member with access to the network to gain access to customer financial information. Because the GIAC Bookreaders network uses shared bandwidth hubs rather than a switched network with the additional security packet switching provides, any staff member could switch their Ethernet card—the piece of hardware that connects the workstation to the Local Access Network (LAN)--to "promiscuous mode," meaning that the workstation would receive all transmissions over the subnet. Normally, the Ethernet card is configured to only receive data packets destined for the particular workstation. This configuration is a matter of both security and efficiency. "Promiscuous mode," however, is a setting available both for network administrators who with to analyze traffic over their systems, and to potential hackers attempting to violate security.

Because transmissions to the financial and other databases occur daily, passive sniffing alone could allow the collection of information potentially harmful to GIAC and its clients. Access to the hard disks of other workstations would not be necessary to access this information, and more sophisticated attacks, while still possible, are not necessary.

Motivations for an individual to conduct such activity could range from curiosity about activity conducted by the company; self-assessment of his or her own technical ability and computer skills; desire to access information about him or herself in company records, files, or exchanged e-mails; or legitimate tests by IT department staff of network security and configuration. The most potentially devastating possibility, however, would be if an individual believes, rightly or wrongly, that collecting financial information about GIAC Bookreaders' customers could be resold for financial gain.

GIAC Bookreaders business strategy is to add value to current businesses and allow them to compete with larger and more established businesses; analysis of the financial, sales, and/or marketing information submitted to GIAC could conceivably allow a larger corporation to steal business from these smaller competitors, or could allow them to determine if buying their smaller competitors out would be possible and practical.

Company Contracts. Many of the contracts GIAC has with its client members and with its vendors would need to be accessed physically. This would not be exceptionally difficult for most contracts and GIAC staff: Most file cabinets are unlocked and in unlocked offices, and entering it is not unusual for staff to leave their offices open for lunch or meetings (although most offices are locked at night). Potentially more threatening would be access to the contracts GIAC has with its vendors, especially because these contracts contain GIAC's credit information, allowing purchases to be made with company funds for personal use.

One insider threat to this information would be access via misappropriated personal authentication information. This threat is a special concern here because the degree of technical knowledge necessary for the hack is low, but the benefit to a malicious hacker-access to credit information—is high. The motive and opportunity for the attack could therefore be attributed to virtually all GIAC staff members.

To conduct this hack, a GIAC staff member without responsibilities for purchasing goods and services could learn the user ID and password of another staff member who does. User IDs at GIAC follow a standard format, and are easy to determine. Passwords are relatively easy to discover, and could be obtained by guessing, social engineering, trying to locate a written record of the password, or watching the staff member type it in ("shoulder surfing"). Then the staff member could log into the network using that identity and, for example, access his or her e-mail account to retrieve a company credit card number from an e-mailed electronic receipt for goods ordered over the internet. The thief could then use that information to order goods and services for their own personal use. The motivation here would be obvious: personal financial gain.

Management information. In electronic form, management information theoretically resides only on the hard drives of the workstations of authorized personnel. It is not transmitted often enough for sniffing techniques alone to be an effective method of inappropriate access. A slightly more sophisticated attack known as a "Monkey in the Middle" attack might be necessary.

The "Monkey in the Middle" attack relies on passive sniffing to intercept communications between two other computers. Then the attacker resets his or her computer to "spoof" one or both of the other computers. This can be done by altering the source address of data packets transmitted to match the address of the other computer. Then, using authentication information gained while sniffing a legitimate session, the hacker initiates contact with one party to the legitimate connection and pretends to be the other party, and requests information.

This type of attack is especially effective to access management information because the information is not on a shared server. Access to another staff member's hard drive

is especially difficult, and may require physical access. With a Monkey in the Middle attack, the information is sent directly.

The motivation for this attack could include an attempt to alter a poor performance review. The "Monkey in the Middle" could be an employee who received a poor evaluation. In the data gathering phase, the employee could learn enough information to spoof his or her supervisor's computer, and which human resources employee was processing the evaluation. He could then contact the human resources employee, pretending to be the supervisor, and request to redo the evaluation, having had a change of heart. This series of events would bear a high risk of discovery for the employee, but is certainly possible and similar events are not uncommon.

GIAC Bookreaders' Inventory Database. The database is vulnerable to all of the previous types of inappropriate access, plus other attacks such as session hijacking. Session hijacking is a relatively sophisticated attack involving sniffing. The GIAC staff member sniffing traffic would need to wait until he has identified a session between another user and the database. For maximum damage, he may select a session in which a GIAC client is updating its information on the database. Then, the hacker would spoof his computer to match that of the user. Then, he would block the original connection using a Denial of Service (DoS) attack, a broad category of attacks that may include malicious code, Ping of Death, or Smurf attacks. Finally, the hijacker assumes the position of the user that was connected to the database. The advantage of this attack in this situation is that it sidesteps the need to gather authentication information, which might be more difficult for an attacker to access for a geographically distant, external client.

The motivation for this attack could be a curiosity about the contents of the database, a test of the hacker's ability and resources, or something more sinister, such as the intent of a disgruntled employee to alter or destroy information in the database.

IX. Outsider Threat to GIAC Crown Jewels

One of the more serious potential threats to GIAC Bookreaders is the possibility of a sequence prediction attack. The end result of such an attack may be to gain access information for any and all servers. A sequence prediction attack begins with reconnaissance on both the intended victim's computer, such as the financial database server, as well as information on a computer with which the victim's computer has a trust relationship, such as that of a GIAC Bookreader client member. Information gained on the financial server would include Initial Sequence Numbers (ISNs) used to establish connections with other computers. ISNs are a number generated at the start of a TCP/IP session, and are supposed to be generated randomly. If the attacker is able to discover a continuous series of numbers used, however, it would be possible to make a prediction on the next number used.

The attacker then attempts to initiate a session with the victim's computer. First, it disables the trusted computer to prevent it from communicating with the victim computer, disrupting and possibly exposing the attempt. Then, it opens a connection with the victim's computer. The victim computer will attempt to send out an acknowledge ("ACK") message to the computer it believes the communication is coming

from. That computer will not respond, but after waiting long enough for the victim computer to send out the ACK message, the attacker will send out the final ACK message that constitutes the last part of the "three way handshake" that constitutes the end of opening the connection. Now, the attacker can send messages and instructions to the victim computer.

The motivation for a sequence prediction attack could be based on a number of interests, including an attempt to change entries in the financial database. A disgruntled customer or former employee of a GIAC member could, for example, change records to make it appear as if the member had under-reported its sales in order to commit fraud for tax purposes or to defraud GIAC itself. It is important to note, however, that another possible motivation would be to gain full access to a database server by perpetrated the attack on a server that contains access information, and then request that the information be routed to the attacker's computer. Indirectly, then, the attack could result in full access—not merely blind one-way communication—with the other machine. The motivation here could be to gain full access to the database to destroy it, consume GIAC resources by requiring them to spend significant time restoring it, ultimately damaging GIAC's reputation and ability to compete in the market.

X. Malicious Code Threat Vector

The most severe malicious code threat to any Windows system of the last year was the MSSQL Server worm, also known as the "SQL Slammer," "SQL Hell," and "Sapphire Worm." Extensive damage to accessibility and server connections due to Slammer was first noted on the morning of January 25, 2003, and it spread at a rate hundreds of times faster than previous notorious malicious code such as the NIMDA worm.[5]

Key to the worm's destructiveness is its ability to propagate passively. It is sent to server computers that use Microsoft's SQL Server or Server 2000 Desktop Engine (MSDE). SQL and MSDE are involved in connecting requests from users to databases on networks appropriately. Requests come into SQL or MSDE, and are sent out using User Datagram Protocol (UDP) data packets. UDP packets differ from TCP/IP packets in that no functionality verifies receipt of the packet to the original user; they are sent off to a particular destination and assumed to have arrived appropriately. SQLServer UDP requests arrive through port 1434. The Slammer enters the server as a single packet of 376 bytes through that port, and then attempts to make copies of itself. It then sends out those UDP copies. If the copies reach another server running MSSQL or MSDE, the cycle begins again.[6] Unfortunately, GIAC Bookreaders uses MSSQL to operate both of the client services databases in its architecture, and GIAC was vulnerable to the worm.

The primary effect of worm was merely bandwidth consumption. The excessive traffic flow caused system performance issues, and GIAC eventually had to suspend services while implementing a recovery strategy. Another vulnerability of the SQL Server, however, is a previously-documented vulnerability called a stack buffer overflow. The

---

[5] See Paul Boutin, Slammed! An inside view of the worm that crashed the Internet in 15 minutes. WIRED, Issue 11.07, July 2003. http://www.wired.com/wired/archive/11.07/slammer.html

[6] See Internet Storm Center, "Analysis: Port 1434 MS-SQL Worm," http://isc.incidents.org/analysis.html?id=180.

"stack" is a protocol that orders the sequence of actions an application takes to execute its activity. A "buffer overflow" is a vulnerability in which it is possible to deliver more information into an area of memory than the program can handle. In the case of the SQL Slammer worm, this vulnerability was used to allow propagation of the worm. It is theoretically possible, however, to design a worm that would exploit this vulnerability to also execute a program that would give an attacker access to the server at the administrator level, which could allow further compromises of the network.

The potential harm to GIAC Bookreaders from the Slammer worm or future similar attacks is a DoS that would prevent use of system resources. A shutdown like this would result in lost productivity of GIAC, inability of GIAC clients to use the inventory database, and loss of trust and goodwill of GIAC to its clients. If future iterations of the Slammer worm are modified to provide access to an outside user, the damage could be even more severe: Compromise of the financial database containing confidential information about GIAC clients' sales, market position, and economic vulnerabilities.

XI. Identification of the Most Severe Threat

While all of these threats are substantial, and that many are of nearly equal severity, the GIAC Bookreaders IT Department considers the threat of access by an insider to client financial information via sniffing is the most severe.

The National Institute of Standards and Technology (NIST) calculates "risk" based on two factors: the likelihood of a threat, and the damage it would inflict.[7] While several of the attacks described pose both a credible threat and the possibility of significant damage, the sniffing attack raises grave concerns for both reasons.

In terms of likelihood of attack, at least three aspects of the attack raise the likelihood of its occurrence. First, the opportunity exists for virtually any employee to conduct the activity. Switching the computer's Ethernet card to promiscuous mode is relatively easy, and requires no special hardware or extensive training. Second, the motivation is relatively plausible. Corporate espionage is a relatively rare occurrence, but not unheard of, and in any case a GIAC employee may believe he or she could gain from confidential information obtained, whether or not this belief is accurate. Finally, sniffing is somewhat more difficult to detect than some of the other activities discussed. Stealing credit information or introducing malicious code into the system would be difficult if not impossible to hide, and response to the incident would be rapid; a GIAC employee that wished the company harm may be more willing to attempt an unethical activity if he or she believed she could operate without the changes in traffic being noticed by the parties intercepted of by the system administrator.

The magnitude of harm, too, is much greater than for some other exploits. Unlike the theft of credit information, the information to and from the database might represent more than the one-time loss following a theft: It could provide information to competitors that would harm GIAC's ability to compete in the marketplace. Also, the compromise of

---

[7] See Stoneburner, G. et al., *Risk Management Guide for IT Systems: Recommendations of the National Institute of Standards and Technology (NIST Special Publication 800-30).* (NIST, January 2002), p. 21-24. http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.

its information systems would cause damage to GIAC Bookreaders ' reputation with its current and future client members, which could create a loss of goodwill and business. Finally, GIAC might be held liable for not securing information that it has contractually agreed to keep confidential. While a determination of negligence or breach of contract would ultimately be a question of law, even the threat of litigation would be severely damaging to GIAC's financial viability.

While space prohibits a detailed analysis of the other threats considered, the sniffing threat earlier identified is the one that GIAC believes poses the greatest risk to its corporate well-being, and is its highest security priority that it wishes to address.

XII. Countermeasure to a Sniffing Attack

While a number of solutions are available to GIAC Bookreaders to mitigate the risk of sniffing detection, the GIAC IT Department recommends that GIAC focus its efforts on establishing a form of encryption for all network traffic. Encryption does not prevent a sniffer from intercepting and receiving packets intended for another destination,[8] but it renders all intercepted traffic unreadable to any party except the intended recipient.

The specific form of encryption the IT Department recommends is SSH ("secure shell") encryption. SSH is a "public key" form of encryption, meaning that each host and server of a system is assigned a public key and a private key. Each host or server sends out its public key to other parties with whom the first party wishes to establish a trust relationship. In future communications, the sender applies the receiver's "public key"—encryption algorithm—to the transmission. The receiver then decrypts the message with his, her or its "private key." This relationship is not reciprocal: A return message to the original sender uses the original sender's public key—a different algorithm—rather then relying on the algorithms used in the first transmission. This safeguard can be used for transmissions in all formats.

Implementing a public key infrastructure would take approximately three months. The steps involved would include:

1. Researching SSH and becoming thoroughly versed in implementation options and public key infrastructure (PKI) maintenance (two weeks). IT Department staff has much of this expertise, but would need to coordinate and discuss its options.
2. Selecting a form of SSH to implement (two weeks). SSH is available as an open source resource, but several versions of it are available. GIAC needs to select a version that is hardened through examination and use, but easy to operate and appropriate for its operating system, bandwidth, and equipment.
3. Testing of SSH in a virtual lab environment (one week).
4. Installing SSH on all servers and workstations, including the workstations of client members (one month). This may require writing a simple script for GIAC staff and client members to follow, with clickable links and instructions for installation.
5. Verifying 100% compliance with instructions to install SSH (one week).

---

[8] For further information on SSH, as well as a discussion of the limitations of the technology, see Kurt Seifried, *The End of SSL and SSH?* (2001) at http://www.seifried.org/security/cryptography/20011108-end-of-ssl-ssh.html.

6. Ongoing support of PKI. Doubtlessly, users will require technical help with PKI, particularly if keys are assigned expiration dates (a best practice for PKI). Also, education concerning the use of PKI will need to be incorporated into current ongoing training and awareness efforts.

The resources needed to complete this effort will primarily involve staff time. Responsibility for research and selection will require at least half of the strategic planner's time for two weeks. He will then present his findings to the director. Then, the plan will be rolled out to the rest of the IT Department for feedback and task distribution. One or two members of The IT Department will set up a virtual lab and test the use of the product. Finally, one or two members IT Department will install SSH on all servers and workstations, and advise remote client members on how to install it on theirs. All told, the time involved will cost between seven and eight thousand dollars. Ongoing support costs will include training and tech support efforts and be built into current efforts.

No security strategy, of course, is infallible. SSH involves an initial exchange of keys between two parties, or a host and a server. That transaction is not, itself, a secure transaction, and other safeguards, such as the management of a key exchange by a third party such as Verisign, must be used. For this reason, the IT Department recommends that encryption be used as part of a suite of solutions that also includes:

1. Establishing a clear, enforceable policy forbidding modification of GIAC software or hardware, including attempts to bypass security controls; and forbidding installing personally-owned software without supervisor approval;
2. Regular monitoring of network configuration and traffic via NMAP and monitoring of IDS output.

Note that one common way of preventing sniffing detection, migrating to the implementation of switched bandwidth technology, is not yet recommended by GIAC IT. While switched technology prevents packet sniffing and helps handle high network traffic, GIAC's current information flow, IT usage, and resources do not justify the expense of investing in eight to ten 12-port switches and assigning staff to the maintenance of those devices. This step may be worth investigating, however, if GIAC is successful in its goals of expanding to accommodate more client members and enabling Web commerce in the future.

XIII. Review of Backup Procedures

GIAC Bookreaders has requested that the IT Department implement a backup procedure that will be 100% effective in assuring the backup of users' workstations. Several possibilities exist, including using Windows' Backup Wizard to save to a dedicated server or requiring individual users to backup to media.[9] The GIAC CEO expects the IT department to perform these backups at each individual workstation. The IT Department, however, would discourage him very strongly from pursuing this course of action for two reasons. First, the IT specialist would need to contact each user at his or her workstation while they were in the office and actively logged in, a

[9] For further discussions on how to set up a backup program, see Negus and Wagner, pages 231-246, cited in full at footnote 1.

logistical coordinating nightmare. Second, interrupting each user while actively working once a month would create tremendous pushback to the effort, which would have a strong negative effect on organizational support.

Therefore, the IT Department is recommending instituting a policy requiring each user to back up his or her own data files onto CD/Rs. This solution was selected for five reasons:

1. Centralized backup would require investment in additional hard disks or a tape medium, which is not justified given GIAC's limited budget and its limited dependence on data controlled by each data owner;
2. CD/Rs are the cheapest form of backup media, requiring approximately a $20 investment for a year's supply for each user;
3. All GIAC standard-issue laptops already come with an ejectable CD-ROM drive, so additional investment in hardware will not be necessary;
4. Individual users can be most easily trained to use this medium and method;

CD/Rs require minimal storage space, allowing flexibility for storage solutions.

Software expenses. CD/Rs from major manufacturers such as Fuji and Maxell are available in stacks of 20 for as low as $9 from major office suppliers such as Office Max and Staples. Providing all 50 employees with a stack each—enough for monthly backups, plus extras—with a 5% surplus would amount to less than $500, including shipping costs. While larger bulk purchasing could bring the cost down, passing out packs of 20 would be most convenient to the procedure contemplated.

Hardware expenses. The IBM Thinkpad T23 that most employees use was issued with an ejectable CD-ROM drive. To assure that each employee has this drive available, the IT Department recommends purchasing five extras to use in case of loss, destruction, theft, or damage to employees' ejectable drives. The standard ThinkPad CD-RW/DVD-ROM Drive retails for approximately $200,[10] and therefore the ultimate cost of this investment will be approximately $1000. This expense compares favorably with the costs of ZIP drives ($300 to $400 each, an amount prohibitive to purchasing one for each employee, not to mention the cost of cartridges ranging from $8 to $10).

Protection of supplemental backups. The IT Department proposes that employees be required to backup their drives monthly, by the 15th of the month, and to drop off their backup disks physically to the IT Department. A lockbox could be set up to assure that any sensitive data dropped off would not be left accessible to unauthorized personnel. Users will be required to backup their active document folders only (the "My Documents" folder in Windows), but would be required to conduct a full backup each month. The IT Department would keep a roster of employees and note all submitted backups, following up with delinquent employees. The IT Department would "spot check" submitted backups to ascertain that recording was performed correctly and effectively. This activity would be performed with the knowledge and collaboration of the data owner, and structured to preclude inappropriate disclosure of data to the IT Department staff. Submitted CD/Rs from staff are currently slated to be stored on site

[10] See product details at http://www-132.ibm.com/webapp/wcs/stores/servlet/ProductDisplay?catalogId=-840&langId=-1&partNumber=22P7011&storeId=1.

in one of GIAC Bookreaders' two server rooms, physically secured with a combination access lock.

Total cost. The approximate total cost for the first year of this strategy will be $15,000, including. Costs will include the hardware and software media described above, as well as infrastructure for the secure submission and storage of backup media to the IT Department. Staff time required will include: $3,500 in time to train staff to back up their materials; $2500 in time for staff to perform the backups; and $3000 for IT Department staff to collect the CD/Rs, perform spot-checks to verify that users are following the required procedures for backing up their data, labeling it, storing it, and securing all sensitive data appropriately (i.e. in locked cabinets or offices).

XIV. GIAC Bookreaders' Offsite Backup Vendor[11]

Pursuant to a directive from the GIAC Bookreaders' IT Director, the IT Department has been asked to transport the CD/R backups described above to an offsite backup location. Two elements of GIAC Bookreaders' operations will facilitate this activity. First, the IT Department has already recommended that all users submit their CD/R backups to a central location in the IT Department, which will facilitate transferring them to the offsite location. Second, GIAC Bookreaders already has a service contract for offsite storage of its servers, that also has the ability to provide storage for media, and is an otherwise appropriate choice to provide this service. GIAC Bookreaders' contract is with a local service provider, Goldberg Data Storage (GDS). Monthly transfer of data from the servers is via tape backup (on DLT via a mirroring process), and monthly transfer of the DLT media to the offsite facility is usually conducted by the Security Officer, who collects and labels DLTs and then drives them over to their offsite data storage vendors' facility in her privately-owned car.

The IT Department will collect the CD/Rs monthly, verify that they are properly labeled, and then store them in a binder with an index identifying which CD/R came from which Department and employee. The binders will then clearly labeled and dated. These binders will be delivered to the offsite vendor for physically secure, environmentally protected storage.

Startup activities for this procedure are minimally burdensome. There is no need to identify a vendor, as GIAC Bookreaders already has a vendor who can supply these additional services for an acceptable cost. GIAC will need to procure these services through a written agreement, with an acceptable service level agreement and liquidated damage clauses that will hold the vendor liable for any disclosure or damage to the data stored. Standard policies and procedures for this task will need to be written, which should be fairly straightforward and can be incorporated into previously-developed policies and procedures.

The *confidentiality* of the data will be assured in several ways. First, GIAC will employ a known and trusted vendor. This offsite backup vendor has already performed similar services to GIAC in a satisfactory manner, and GIAC has every reason to believe they

---

11 GIAC's backup and recovery plan was developed after consulting Eric Maiwald and William Sieglin, *Security Planning and Disaster Recovery,* (McGraw Hill, 2002), Part IV ("How to Respond to Incidents").

will be able to provide this service as well. Second, GIAC will document the vendor's responsibility to assure confidentiality of the data in a written contract. Third, the transfer of the data will be made promptly and regularly. Either a GIAC or GDS employee will at all times have direct physical control of the media. GIAC has not, however, elected to password-protect the CD/R data. While GIAC acknowledges this represents a limited risk, it believes the chain of custody maintained over the data will be an adequate safeguard to its confidentiality.

To protect the *integrity* of the data, preparation, packaging and transfer of the offsite backups will be subject to rotation of duties safeguards. All members of the IT Department will perform functions related to preparing the CD/R binder for offsite delivery, and will begin rotating responsibility for delivering it to GDS. Rotation of duties will assure that data may not be changed, copied, accessed improperly or destroyed each month unless all IT staff participate in the security violation. Aside from these protections listed above, the integrity of the data can only be assured through testing, as described below.

The *availability* of the data for access in the event of the need for restoration will be protected by the service level agreement. The agreement will specify that the hardware and software stored at GBS's facility will be made available to GIAC within twelve hours. GBS assures this by employing a 24-our emergency answering service that can contact key GBS staff immediately in case of an emergency, and requiring at least two key staff members to be reachable at all times. Additionally, GIAC has verified that GBS has undergoes a rigorous physical and environmental security evaluation on a twice yearly basis. Finally, IT Department staff visits the facility to drop off materials, and is also shown exactly where and how the material is stored to verify that storage is appropriate and secure.

The only reliable way to audit the process is to test it. Testing will involve collecting data from GBS, bringing it into a media lab, and restoring it onto a non-networked computer. File integrity can be checked using a hashing algorithm and via a tool such as Tripwire. Because this activity may involve accessing data not normally available to the IT Department, it must be conducted with specific, documented approval from senior management, preferably the CFO or CEO. This activity should be performed quarterly on backups of several workstations, to ascertain both that users are backing up their data properly and that data can be restored in the event of a disaster.

XV. Guerilla Business Continuity Plan

Pursuant to the request of the GIAC Bookreaders IT Director, GIAC has developed a guerilla Business Continuity Plan (BCP). This plan covers only the essential service that would assure GIAC's continued viability in the event of a fire or other disaster. In this sense, the plan is more of a Disaster Recovery Plan (DRP) than a true plan for the return to normal operations usually contemplated by a BCP. Given GIAC's small size and limited resources, however, it is contemplated that after a major disaster, GIAC may have to resume operations on a more limited scale for an extended period. A true BCP may have to wait until GIAC has the resources to dedicate to fully redundant systems and emergency resources.

The IT Department has identified the availability of the inventory database as the most critical service to maintain following a major loss. This is so for several reasons. First, because almost all GIAC client members access the database daily, it is the most visible service. Thus, it generates the most goodwill and is most valued by the client. Second, increases in client member revenue are most directly attributable to increased sales generated through use of the inventory database.

The first step in preparing the BCP was to assemble GIAC Bookreader's Incident Response Team (IRT). The team has five members: The tech specialist assigned to develop the BCP, the Security Officer, the IT Director, a member of the marketing team (to handle client contact, press releases, and any other communications/PR issues), and another technical specialist with database programming and maintenance skills.

After consultation with the group, a stepwise plan was constructed:

1. In the event of an emergency, ascertain the health and safety of all GIAC employees first. If the incident involved the destruction of GIAC's facilities, determine if any staff were harmed. Work with health and safety officials to respond to the emergency and assess the extent of loss to IT resources and office space. A phone tree was developed assigning all IRT members responsibility for contacting staff, beginning with the team itself.

Action item: Prepare checklist of items to be performed in the event of such an emergency. Assign responsibility to the IT Director to be the central point of contact in the event of a disaster. Compose phone tree and assign responsibility to a tech specialist for keeping the information on it current.

2. Arrange for the IRT to meet. If the GIAC site is unavailable, the IRT will meet at an offsite facility. A list of area hotels with adequate conference room facilities has been collected for this purpose. If these sites are unavailable, the IT Director will select an alternative site.

Action item: Prepare a list of alternative sites to serve as the IRT's Command Center.

3. Restore the inventory database server from the DLT backups at an alternative site. While the current offsite data storage facility (Golberg Backup Services) does not have these facilities available, staff at Golberg has recommended a number of server hosting vendors that may be appropriate service providers. GIAC Bookreaders will evaluate these candidates in the next three months and sign an agreement for services.

Action item: Identify server host for critical GIAC services and sign service agreement.

4. Inform client members of how they can get access to the inventory database. Assuming that both e-mail and Web service will have been rendered unavailable, contact will be made by telephone to each client within 48 hours. The marketing director has developed a modular telephone script that guides callers to provide all key information including how they can access the database; how current the database will be given its restoration from monthly backups; where they can call for updates and further information; and how long other services are expected to be unavailable.

Action item: Prepare a contact list of GIAC client members and subdivide such that three individuals could divide responsibilities for contact. Assign responsibility for updating the list. Prepare phone script for use by those making client calls.

5. Restore other support services such as the Website, e-mail, and the financial database.
6. Return to GIAC facilities if possible; or, identify and establish operations at an alternative site.

Action item: Advise CEO of the need to identify potential alternative sites of operations. While maintenance of a full-time hot or cold site may be beyond GIAC's current financial capacity, as GIAC continues to expand, its first priority should be to establish operations at a second site, to which critical operations could be shifted following a disaster.

As highlighted above, ongoing maintenance of the plan will include updating contact sheets and information on temporary and alternative sites, confirming the availability of servers and data for backup, and testing the plan.

GIAC Bookreaders will test this system in two ways. First, it will conduct "tabletop" exercises in which the IRT is meets, and a facilitator asks the group to describe what their response would be to a hypothetical emergency. Second, the IRT will confirm that the IT Department is regularly evaluating the availability of data and server backups.

This basic strategy can be used for all of GIAC Bookreaders' IT services, including the financial services database, Web site presence, and e-mail services. The IRT recommends, however, that additional staff be added to the IRT to discuss and prepare a disaster recovery plan. This will assure that specific expertise will be available to anticipate and prepare for restoration of the system. In fact, this basic six-step process forms a good approach for restoring all of GIAC's essential business functions. Because GIAC is so dependent on personal relationships, the most critical element of Business Continuity for any of its services would be to re-establish communications with client members as soon as possible, through whatever medium, inform them what services will be available and when, and assure them that GIAC Bookreaders remains committed to its core mission.

CONCLUSION

GIAC Bookreaders has limited resources, limited staff, and a limited budget. Its assets, however, include staff dedicated to the organization's business mission, leadership that sees potential for growth, and a unique set of services. Because GIAC intends to grow in profitability, size, and reputation, it recognizes that it must protect the reputation and resources it has thus far developed. The security of its technology and the information that it contains is therefore an immediate priority that it can't afford not to protect with sensible, basic safeguards.

LIST OF REFERENCES

Antoine, Vanessa et al, *Router Security Configuration Guide version 1.1*. (National Security Agency, November 21 2001). http://www.nsa.gov/snac/cisco/download.htm.

Boutin, Paul, "Slammed! An inside view of the worm that crashed the Internet in 15 minutes." *WIRED*, Issue 11.07, July 2003. http://www.wired.com/wired/archive/11.07/slammer.html.

Cisco Product Data Sheets, 2600 Series Routers. http://www.cisco.com/en/US/products/hw/routers/ps259/ps4832/index.html.

Internet Storm Center, *Analysis: Port 1434 MS-SQL Worm*, http://isc.incidents.org/analysis.html?id=180.

Maiwald, Eric and William Sieglin, Security Planning and Disaster Recovery, (McGraw Hill, 2002), Part IV ("How to Respond to Incidents").

Negus, Christopher and Bill Wagner, The Complete Idiot's Guide to Networking, 3rd ed. (United States: Pearson Education Inc., 2001).

Seifried, Kurt, *The End of SSL and SSH?* (2001) at http://www.seifried.org/security/cryptography/20011108-end-of-ssl-ssh.html.

Sidel, Scott. "Symantec Gateway Security Appliance: The Swiss Army Knife for SMBs." Information Security Magazine: August 2002. http://infosecuritymag.techtarget.com/2002/aug/testcenter.shtml.

Stoneburner, G. et al., *Risk Management Guide for IT Systems: Recommendations of the National Institute of Standards and Technology (NIST Special Publication 800-30).* (NIST, January 2002), p. 21-24. http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.