OFFICE OF THE MANAGER
NATIONAL COMMUNICATIONS SYSTEM

INFORMATION SECURITY BUSINESS CASE

CASE STUDY #1 - SEBRING

25 October 1996

Further distribution only as directed by
Office of the Manager,
National Communications System (OMNCS)
Customer Service and Information Assurance Division
Information Assurance Branch (N53)

ABSTRACT

This case study was prepared as part of a larger effort to develop a business case approach to justify funding for network security programs. The case study participant was selected by the Government sponsor of the project from a list of candidates developed by the SAIC project team. The case study presents an overview of the participant organization to include its technical and operational environments; discusses the motivation for establishing a security program; describes the organization's Network and Information Security Program; overviews the participant's business case process; and presents senior management's view of several network and information security issues.

TABLE OF CONTENTS

TABLE OF CONTENTS (Continued)

LIST OF TABLES

DCA100-95-D-0104
Delivery Order No. 10
Information Security Business Case
Case Study #1-SEBRING

1. INTRODUCTION

In recent years, information and telecommunications technology and services have expanded at an astonishing rate, in terms of the technology and implementation. The public and private sectors increasingly depend on information and telecommunications systems capabilities and services. In the face of rapid technological change, public and private organizations are also undergoing significant changes in the way they conduct their business activities, including the use of wide area networking via public networks. These changes include mandates to reduce expenses, increase revenue, and at the same time compete in a global marketplace. Even under prosperous economic times, security has not been easy to sell to upper management unless the organization has been the victim of a major security incident. In today's business environment it is even more difficult to obtain senior management approval to justify the expenditure of valuable resources □ yet, this expenditure is necessary to "guarantee" that a potentially disastrous event will not occur and affect the ultimate survivability of an organization.

SAIC has been tasked by the Office of the Manager, National Communications System (OMNCS), Customer Service and Information Assurance Division, Information Assurance Branch (N53) under the Defense Information Systems Agency (DISA) contract DCA100-95-D-0104, Delivery Order 10, to provide the Government with a report and briefing supporting the justification of funding network security related programs. The purpose of Task 2 of this delivery order is to research, develop, produce, write, and publish three individual case studies of organizations which have been the victims of significant intrusions and have initiated significant programs afterward to improve security within their networks. This report represents the first of the three case studies.

To protect the anonymity of the organizations in the case studies, a code name has been assigned to each organization. The code name of the first case study organization is SEBRING.

1.1 Purpose of the Project

The overall purpose of the Information Security Business Case project is to research, develop, produce, write, and publish a Business Case for Security. The project consists of performing research on three organizations that have been the victims of significant network intrusions or have initiated significant programs to improve security within their networks for other reasons such as deregulation of an industry sector or direction of a corporate board of directors. The final product will be a “generic” approach/methodology for justifying network and information systems security expenditures.

1.2 Approach for SEBRING Case Study

The first step in performing the SEBRING case study was obtaining the consent of the organization’s senior management to be a participant. The case study point of contact was the Director of Network and Information Security. Once an oral agreement was obtained, SAIC and the participant executed a non-disclosure agreement to ensure the organization’s anonymity. SAIC developed a questionnaire guide to be used during the initial data collection effort. A team of three SAIC personnel conducted a 1 day on-site visit to the participant organization and interviewed the point of contact using the questionnaire guide. During the interview, the SAIC team identified several documents and requested copies. Documents collected during the interview included policies, procedures, code of conduct statements, and business case procedures. Several follow-up telephone conversations were held between the SEBRING point of contact and the SAIC principal investigator to answer questions and to obtain additional data relevant to the case study. Background material concerning the participant organization was obtained both from the participant and from open sources.

1.3 Overview of the Report

Section 2 describes the business services and the technical and operational environments of SEBRING. Section 3 depicts the activities that motivated SEBRING to develop a network and information security program. Section 4 provides a description of the evolving network and information security program, including the security organization and the security policies. Section 5 describes the current business case analysis process used by SEBRING. Section 6 provides the lessons learned by SEBRING management as a result of the network intrusion.

2. OVERVIEW OF THE SEBRING ORGANIZATION

2.1 Description of the Business

SEBRING is a worldwide company with a diverse range of information processing systems. Originally, SEBRING was a local telephone company. It now offers a wide range of information, wireless and wireline telecommunications, and information and entertainment services. SEBRING serves approximately two million customers in its current base and plans to expand that customer base within its serving areas, as well as expanding into national and international markets. The company provides local and global calling services, wireless communications, network and information management services, and publishing and advertising services. SEBRING is at the leading edge of the broadband video revolution. SEBRING has approximately $3.5 billion in assets and $2.0 billion in annual revenue and is listed on the New York and Pacific Stock Exchanges.

SEBRING is organized into eight business units. Table 1 shows these units and their primary services.

Table 1. Business Units

BUSINESS UNIT	SERVICES
Mobile Unit	Provides wireless services such as cellular phone and paging.
Multimedia Services	Provides information, communications, and entertainment services.
Long Distance Services	Interstate and international calling services.
Network Services	Builds, repairs, and manages telecommunications network, wholesales network/database/billing services. Network architect for AIN and SONET technology.
Business Group	Assists small and medium-size businesses in applying emerging technologies.
Consumer Services Group	Serves residential customers with telephone and related offerings.
Custom Business Group	Packages advanced voice, data, and video services for large businesses.
Publishing Services	Publishes yellow pages, business listings via CD-ROM, and audio information services for yellow pages.

2.2 Description of Network and Information Systems Environment

The information and network technology used to support SEBRING's Corporate backbone network environment and that of the core businesses units is a heterogeneous, distributed, outsourced environment. That environment consists of, but is not limited to, the following technology:

- Intel-based Personal Computers running DOS and Windows™
- Lotus Notes Server
- Welfleet 7.X Routers
- Sun Solaris 2.5 Workstations
- IBM AIX® 4.1.4
- Firewall 1 Firewalls
- Analog modems, cellular packet data modems, and modem pools tied to PCS, Local Area Networks and networked outsourced vendor environments
- AT&T Starkeeper Network Access Controller (NAC) with token-based access control and authentication for user access
- Frame Relay Wide-Area-Network with dial-up Points of Presence.

The SEBRING corporate backbone network is a subset of various applications and enterprises including the business units identified in Table 1. The backbone network includes connectivity to mainframe legacy systems, and commercial information and services network providers. The information technology applications include a number of telephony business-critical functions such as Enhanced-911 and Loop Maintenance Operations Systems (LMOS).

2.3 Description of Operational Environment

Historically, SEBRING has acquired, provisioned and operated its total information and network technology environment in a single data center. In the late 1980s and early 1990s, SEBRING acquired a second data center facility as part of its normal growth and to provide some level of data center backup operations. In the 1991/1992 timeframe, however, SEBRING could no longer economically justify two separate data centers and migrated most of its operations to its newest facility. In the 1994/1995 time frame, SEBRING management conducted a business case analysis and determined that it would be financially advantageous to outsource its data center operations. The overall reduction in data center operating costs to SEBRING was estimated at 20 percent over a 7-year period. The final move to the outsourced mode of operation was completed in mid-1995.

Under the terms of the outsource contract, between 100 and 150 SEBRING employees were transferred to the outsource organization. While the outsource organization manages the mainframe and mid-range computing systems, SEBRING continues to handle its own applications and network administration. The outsourcer purchased the main data center and is completing the consolidation of the two SEBRING data center facilities. The vendor currently is negotiating the disaster recovery of critical outsourced SEBRING applications. Under the terms of the outsourcing agreement, the vendor is responsible for the security of the outsourced SEBRING information technology environment and applications and for providing logical audit rights to SEBRING to test, evaluate, and report on the overall state of security as provided by the vendor.

In mid-1996, SEBRING outsourced its desktop, local area network, help desk, and support services. Under this contract, the outsource vendor is responsible for the following:

- Setup of desktop and notebook computers and/or docking stations, and of standalone printers/plotters/scanners
- Adding, changing, or moving the above equipment including LAN connectivity
- Upgrading desktop software
- Repairing of desktop computers and printers/plotters/scanners
- Providing ongoing in-warranty repairs
- Configuration, installation, and upgrading of LAN services such as Lotus Notes
- Providing ongoing on-site and remote LAN administration services, including adding, changing, and removing users and associated rights and maintaining security
- Providing help desk services to include all standard and custom software applications
- Providing on-line access for SEBRING’s audit of services, questions and trouble reports
- Providing an initial inventory of desktop and LAN hardware, software, and passive devices
- Providing life-cycle asset management of hardware and software

- Developing, implementing, and managing a Disaster Recovery Plan
- Providing new technology evaluation and migration planning support.

Under the terms of the contract, the outsourcer is required to develop a disaster recovery plan that ensures the continuity of the help desk operation. SEBRING will be financially responsible for procuring and outfitting the alternate site with furniture and telephone equipment, cabling, and wiring, and for the purchase price of additional machines and desktop/LAN software. The vendor is responsible for adhering to and enforcing compliance by all SEBRING users with SEBRING Corporate Information Security Policies (see Section 4.4). The vendor is also required to furnish employee dishonesty and computer fraud insurance to cover its employees.

3. MOTIVATION(S) FOR ESTABLISHING SECURITY PROGRAM

One of the primary motivations for the establishment of SEBRING's network and information security program was an intrusion that involved a commercial internet platform. The user-ids and password were cracked on two UNIX® workstations normally used by systems administrators. The intruders used Rootkit, a stealth hacker tool that is freely available over the Internet. Rootkit replaces normal administration and security programs with trojan horse versions that makes detecting intrusions difficult. Other trojan horse programs were also found later by a network forensics team. In early 1996, the SEBRING internal EDP auditor briefed the Board of Directors at the request of the Chief Financial Officer and the Chief Information Officer.

The briefing to the Board of Directors addressed the following points:

- SEBRING's technology is moving from centralized mainframes to a highly distributed client-server data environment; therefore, security is required for the network as well as for the data.
- SEBRING's Internet offering is growing exponentially. Since the Internet is wide open for access, there is a need to protect the technology that serves the customers.
- The threat to SEBRING increases significantly as the distributed architecture increases. The latest available information from our industry resources such as the President's National Security Telecommunications Advisory Committee's (NSTAC) Network Security Information Exchange (NSIE) and the Federal Bureau of Investigation (FBI) indicated that SEBRING is one of many companies that has been targeted by a coordinated group of intruders looking to penetrate the public switched network. The latest intrusion into SEBRING is believed to be the work of this group.
- In March 1966, SEBRING was notified by one of the major computer emergency response teams that there had been an intrusion at SEBRING. After an intrusion analysis by an outside independent organization, SEBRING's administrators checked their computers and found that two machines contained a log left by a "sniffer." The sniffer had been surreptitiously installed by the intruder. Since SEBRING's administrators had logged into the Internet server computers via the network, it was assumed that the server passwords had been compromised.
- All customer information stored by SEBRING is in a computer protected by a firewall. It was believed that customer information was not compromised.

- One of the major tools of potential intruders is "social engineering," which is cultural to the telecommunications industry. SEBRING's employees are probed daily by outsiders attempting to gain sensitive information.
- Protection of information and network resources requires adequate monitoring by software and hardware tools and adequate resources to use those tools.

The briefing to the SEBRING Board of Directors provided an action plan that included the following steps:

1. Consolidate all computer hardware in the data center and require security levels to be consistent across all systems.
2. Use outside experts to conduct quarterly routine security reviews.
3. Install software tools to identify all nodes connected to a network. The tools will permit monitoring of network connections to determine when unauthorized connections are made.
4. Use firewall technology to segment networks.
5. Implement a security awareness program by the fourth quarter of 1996.

In the third quarter of 1996, responsibilities for Corporate disaster recovery were also assigned to the new Director. The Director has been tasked to develop a security policy by the end of the third quarter of 1996.

4. SEBRING's NETWORK AND INFORMATION SECURITY PROGRAM

The objective of SEBRING's information security strategy is to ensure that security has been considered adequately within the competitive business environments of SEBRING's strategic markets. The goal is to implement security solutions in an efficient, automated, customer-friendly approach that can be anywhere, at any time.

4.1 Organizational Location and Reporting Chain

The Director of Network and Information Security reports to the Director of Information Technology (IT) Operations who, in turn, reports to the Chief Information Officer (CIO) or Vice President. The CIO reports to the Chief Financial Officer, who is a Senior Vice President in the Office of the President. The CIO is charged with providing updates on security to the Audit Committee of the Board of Directors. Frequently, the CIO tasks or queries the Director of Network and Information Security directly concerning security issues.

In addition to network and information security responsibilities, the Director of Network and Information Security is also responsible for disaster and recovery planning and for policy for information classification and proprietary information protection.

4.2 Network and Information Security Staff

The network and information security staff currently consists of the Director and one security analyst. The security analyst is primarily responsible for developing and executing auditing tools on the network. The security staff was temporarily augmented by two additional personnel to support the additional tasking for disaster recovery.

4.3 Organizational Interfaces

4.3.1 <u>Internal Interfaces</u>. Internally, the Director of Network and Information Security has a very good liaison, and usually weekly contact, with the Vice President, Internal Audit.

SEBRING's risk management organization is located in the Finance Department. The information technology risk management organization focuses on business continuity and insurance.

Before establishing the office of the Director of Network and Information Security, SEBRING had an Information Security Committee. The Committee was responsible for the maintenance of security policies. That responsibility has been transferred to the Director for Network and Information Security. While the Committee is no longer a formal organization, the members still meet periodically to discuss security issues of mutual interest across the company. The committee usually meets informally immediately before and after meetings of Bellcore Telecommunications Security Awareness, Research, and Standards (TSARS) group, of which SEBRING is a member.

The Director maintains additional informal liaison with the business operating units on a frequent basis. The Director is called upon to assist operating units when they need to discuss security issues pertinent to their business activities.

4.3.2 <u>External Interfaces</u>. SEBRING belongs to a variety of external forums. The primary groups are the TSARS sponsored by Bellcore, the NSTAC's NSIE through Bellcore, and an ad hoc industry group known as International Information Technology Users Group (IITUG). The IITUG is chaired by the CIO of Bethlehem Steel and was created in 1995 to pool issues and best practices solutions across information technology companies. The IITUG includes membership from the aerospace, information management, automotive manufacturing, aviation, banking, telecommunications, electronic commerce, and other industries. The SEBRING Director of Network and Information Security is currently the co-chair of the IITUG Security Subgroup and chair of the Disaster Recovery Subgroup. The current plan is to develop an ad hoc user-driven type of forum to address high risk, low probability issues such as Disaster Recovery and security where tasking might be developed and resources obtained to help the IITUG members.

4.4 Corporate Information Security Policies and Procedures

SEBRING has issued a set of Corporate Information Security policies. These policies govern the use of and information on all computing platforms. The policies are based upon the Bellcore Generic Requirements on security such as the Operating Systems Security Requirements. The set of policies states the fundamental security policy, the employee's responsibility to be aware of and to comply with all of the stated policies, and appropriate disciplinary action for non-compliance. The document outlines:

- Definitions for classification of all corporate data
- Use of userids and passwords for access to all systems
- Authorization (need-to-know) criteria for information and systems access
- Appropriate security logging and auditability
- Operating system controls and conformance to standard operating environment
- Physical security for all computing platforms and corporate buildings
- Software use and copyright protection
- Virus protection
- Proprietary information.

The policies address 13 specific areas. The major points of each policy are summarized in the following sections.

4.4.1 Fundamental Corporate Information Security Policy. The fundamental policy statement states that information is a corporate asset. The policy states that the integrity of SEBRING's business and customer information is to be ensured and protected by all employees. The information must be maintained in a complete, whole, unimpaired state and protected from all forms of interference. Further, employees are accountable for understanding their obligations to protect corporate assets and are responsible to carry out security practices. The policy requires the reporting of variance from policies and procedures. Non-compliance with security policies and standards is a serious violation and will result in disciplinary action.

4.4.2 Information Classification. This policy identifies and defines three data classifications that are to be used to categorize all corporate data. The categories are: General Availability; Limited Availability; and Restricted Availability. Table 2 defines these categories.

Table 2. Information Classification

CLASSIFICATION	DEFINITION
General Availability	▪ Internally originated, and available to the public ▪ Internally originated, and whose availability is neither limited nor restricted
Limited Availability	▪ Information and data that are confidential and proprietary ▪ Specific and identifiable to customers, employees, or investors ▪ Specified by customers, employees, investors, or vendors as confidential or proprietary ▪ Provide business direction or a competitive edge ▪ Financial data, whose availability is neither general or restricted ▪ Provide strategic or action plans, statistics, or analysis of any corporate option, operation, or process ▪ Necessary for the effective and efficient provisioning of service to customers
Restricted Availability	▪ Information and data that are highly confidential or proprietary ▪ Provide financial results or plans, and whose availability is neither general or limited ▪ Concern proprietary technical developments ▪ Control the major functions of an electronic switching system ▪ Designated restricted by an Officer of the Corporation, the General Internal Auditor, or a governmental agency

4.4.3 Computer Systems Security. This policy requires various types of security controls on corporate computer systems. Specifically included are the requirements for individual user accounts (userids) for employee and customer accessible computer systems; periodic renewal of user accounts by system administrators; automatic logoff for systems at idle; and periodic re-registration of accounts. Requirements for passwords to include length and expiration limits, retries, and aborted logon attempts are also included. Restrictions on “super-user” type privileges are delineated. Additional requirements include a “need-to-know” statement; security logging and audibility; encryption; and operating system controls.

4.4.4 Network Security. This policy requires that the security, privacy and integrity of information transported or processed on corporate networks be ensured. Network access to information systems shall be provided such that only authorized users will be permitted access and all others will be denied. Table 3 delineates network access security controls.

Table 3. Network Access Controls

LEVEL	NETWORK ACCESS CONTROL	INFORMATION CLASSIFICATION
1	Network password or dial-back without password	General Availability
2	Access control device, such as a Smartcard on dial-up lines	Limited and Restricted Availability
3	Private (dedicated) Lines	Limited and Restricted Availability

The policy requires that local area networks be protected with level 2 or 3 controls. The policy also requires the use of a warning banner indicating that it is a private network and that unauthorized access or use will lead to prosecution.

4.4.5 **Microcomputer Security.** This policy includes requirements for physical security, access controls, microcomputer telecommunications, backups and off-site storage, micro-mainframe file transfer, and file servers. Table 4 describes the microcomputer security requirements.

Table 4. Microcomputer Security Requirements

SECURITY CONTROL	REQUIREMENTS
Physical Security	Employees are responsible for taking reasonable and prudent measures to protect against unauthorized use or removal of microcomputers (PCS), to including software, diskettes, and printer output.
Access Controls	Additional controls are required for fixed disk storage media that process or store Limited or Restricted information: ▪ Copy information to removable diskette or tape, label and store in locked drawer or cabinet, and erase from hard disk. ▪ If retained on hard disk, microcomputer must be equipped with approved access control software that includes userid and password facilities, disk partitioning, data encryption, and a complete audit trail. ▪ Microcomputer must be logged off when unattended.
Microcomputer Telecommunications	Passwords are not permitted in automatically key logon scripts when telecommunications software is used to connect a microcomputer to another computer system.
Backups and Off-Site Storage	Microcomputers containing Limited or Restricted information must be backed up every 30 days. Two sets of backups will be retained with one being stored in a secured area other than the user's immediate work area.
Micro-Mainframe File Transfer	Corporate data is to be transferred only by authorized personnel with a business need and who have received explicit, documented permission from management. Users must have approved file transfer tools.
File Servers	Microcomputers used as file servers must conform to all security policies.

4.4.6 <u>Software Use and Copyright Protection</u>. This policy restricts the copy or use of software developed or purchase by SEBRING without authorization. The policy expressly forbids the use of code-breaking devices that allow copying of proprietary software and notifies employees that illegal copying could lead to criminal prosecution. Further, the policy notifies that all software developed by and for SEBRING and resulting files, databases, and other data are designated as trade secrets of the corporation.

4.4.7 <u>Computer Virus Prevention</u>. This policy requires that all software obtained from one of four designated sources. Further, software change control procedures and audits shall be instituted to enable detection of unauthorized code. All software, regardless of source, must be scanned by an approved virus detection program before loading into any computer or computer network.

4.4.8 Physical Access Security. This policy requires that physical access to corporate buildings that contain computers and networks that process or transport Limited or Restricted information be protected by appropriate devices such as security guards, card-key access systems, intrusion alarms, or tamper-proof door locks.

4.4.9 Identification Card. This policy requires that employees, authorized contractors, and authorized visitors be issued an identification badge and display the badge in a clearly visible location. In areas where card readers are used to control entry and exit, "tailgating" is expressly prohibited. Employees are also required to challenge and/or report persons who fail to produce ID badges.

4.4.10 Proprietary Information. This policy requires the protection of proprietary business information, including computer or network-related documents such as user guides, programming manuals, computer printouts contain Limited or Restricted information, logon procedures, and command sequences or transactions. Further, non-disclosure agreements must be signed by each employee who has access to Corporate information, and especially those responsible for the administration of information security, such as data base administrators and data set security administrators.

4.4.11 Computer Use. This policy states that SEBRING computer or network resources are for business purposes only and non-SEBRING commercial use is prohibited. The policy also states that all information stored or processed in corporate computers and networks is corporate property and is subject to inspection without notice.

4.4.12 Contract Personnel. This policy states that all contract personnel must follow Information Security policies and face immediate dismissal for non-compliance. The background of all contract personnel shall be investigated, including past work with the corporation. Agencies representing contract employees are required to understand their accountability for the workers they supply.

4.4.13 Compliance. This policy requires that SEBRING maintain an Information Security Committee and that the committee meet on a regular basis to discuss and implement any security policies. The Committee is responsible for the maintenance of security policies. Additionally, any violation of security policies is required to be reported to the Internal Auditing Group so that corrective actions can be taken.

4.5 Information Security Program Costs

4.5.1 <u>Costs Associated with Initial Incident</u>. SEBRING maintains a contractual relationship with Bellcore to address various issues such as security. The annual cost of the Bellcore support is $40,000. SEBRING called in Bellcore's forensic team to determine the extent of the intrusion and incurred an additional cost of $6,000.

SEBRING is also upgrading its Network Access Control equipment with new security features at a cost of $500,000 plus maintenance. The enhanced security features will require an investment approximately $270,000 for new Smartcards.

4.5.2 <u>Costs for Sustaining the Information Security Program</u>. The direct costs for sustaining the Information Security Program at this time are the labor costs of approximately $140,000 for the current fiscal year. The annual cost for the addition of two personnel for disaster recovery will increase the annual labor costs by approximately $100,000.

5. SEBRING BUSINESS CASE PROCEDURES

SEBRING is a commercial enterprise competing in a rapidly changing technological and marketplace environment. In order to survive and compete effectively, potential investments must be based on sound business, financial and economic analyses. In today's information services environment there is increasing pressure on prices and earnings. There is an explosion of new ideas competing for limited investment dollars. The watchword of industry is get organized and work smarter. In the past, SEBRING has used an abbreviated decision support document process in which large investments were made on the basis of an abbreviated, two to three page document. The decision support document included a high-level summary of a project and answers to the following types of questions:

- Why do we want to do this?
- How does it fit with our strategy?
- What is the Net Present Value, Economic Contribution, and Payback Period?
- Is incremental funding required?
- Who are the parties/departments involved?
- Is there any impact on other initiatives?
- Why now?
- Is this a breakthrough project?
- What are the competitive impacts?
- What is our market strategy?
- What is the exit strategy?
- What are the risks and how are they minimized?
- What are the measurements, checkpoints, kill points?

Recently, SEBRING has established a more definitive process, which is based upon the review of key management personnel. In some cases, the decision may be that a decision document is sufficient. In other cases, the reviewer may decide a more in-depth analysis is required. The extended analysis process requires the preparation of a formal business case. A formal business case includes the type of information as the decision document plus a 5-year review of the project in prescribed format. The formal business case analysis typically runs 12 to 15 pages, plus appendices. The analysis addresses the following:

- Project Description
- Opportunity (Marketing, Strategic, Process Improvement)
- Alternative Evaluated
- Analysis/Recommendation
- Implementation
- Consideration of Risks and how to mitigate
- Consideration of Other Departments/Business Units Affected
- Financial and Economic Measurements
  - Net Present Value
  - Modified Profitability Index
  - Discounted Payback Period
  - Economic Contribution.

The formal business case is submitted to financial assurance and internal audit for review. If it is a large project with Corporate strategic importance, it will progress to the Strategy Review Group and preparation of a budget may be required upon approval.

A business case has not been prepared for the Network and Information Security Program. Requests for security measures that meet certain dollar thresholds may require the preparation of a decision support document or a formal business case in the future.

6. SEBRING MANAGEMENT VIEW OF SECURITY

The senior management of SEBRING was interviewed concerning security issues. The interview addressed several questions as follows:

- What are senior management perceptions of the security risks?
- How much of a "wake-up call" was the intrusion incident?
- What security concerns were raised as a result of the intrusion?
- What are the security concerns regarding outsourcing?
- What is the approach for sustaining network and information security over time?
- How will the expense of maintaining the program be justified?
- What is the organization comfort level with what you have done and your plans for the future?
- What is the business model for addressing security risks?
- What are the lessons learned from the incident?

6.1 Senior Management Perceptions of the Security Risks

SEBRING's senior management considers the organization to be very much at risk. They have their "finger in the dike" and are trying to mitigate exposures. However, they face significant exposure to the sophisticated hacker. There are some tools in place, but the hackers are getting more sophisticated. It's open warfare — that is the nature of the business. Security, or the loss of it, is a risk of doing business today. It is impossible to isolate yourself and remain in the telecommunications business. Moreover, the marketplace demands that corporations be open on the issue of security with their employees, their vendors, and their customers.

6.2 How Much of a "Wake-Up Call" was the Intrusion Incident?

The intrusion was a wake-up call. The risks are very real and the reality is well understood throughout the company. Before the intrusion, the company was paying lip service to the problem. While they had been the target of intrusions in the past, they did not know that they had been penetrated or to what extent. The incident also confirmed that the company is very decentralized and organizations are very independent.

The incident provided SEBRING with the opportunity to make the Board of Directors aware of the risk. By doing so, management ensured that security will remain an active and ongoing initiative. The Board will continue to inquire about security.

6.3 Security Concerns Raised as a Result of the Intrusion

Business units were acting on their own and were not being held accountable for compliance with a centralized company policy for acquisition and configuration management. They were adding their own equipment to the network and thereby unknowingly introducing new risks. This area will continue to be a concern because enforcing centralized control is difficult and involves changing a long-standing culture of independence. Unfortunately, there is no silver bullet for SEBRING to solve these control problems.

6.4 Security Concerns Regarding Outsourcing

SEBRING management worries less about the outsourcers than they do about internal security. If there is a security problem with the outsourcers, it is fixed that day. Fixing problems is the outsourcer's responsibility and they are responsive. Internally, on the other hand, security is put on a list that contains many other items; and it is not given a high priority. Security items do not get done or, at least, not in a timely manner.

6.5 Approach for Sustaining Network and Information Security Over Time

The Director of Network and Information Security must continue to execute his/her responsibilities and define his/her needs further to do his/her job effectively. There must be an active monitoring of the network, the risks, etc., to stay ahead of the game. SEBRING will need to stay focused on the area of security.

6.6 Justifying the Expense of Maintaining the Program

Funding is not an issue; it is a justifiable and expected expenditure of infrastructure funds. If the company doesn’t spend the money, the stakeholders will want to know why the problem wasn’t fixed. The problem is real; the Board of Directors supports the need for the program, and the funding, as well.

6.7 Organization Comfort Level with What SEBRING Has Done and Plans for the Future

SEBRING management indicated that they were not very comfortable with what had been done in the past. They indicated the organization should be doing more; in particular, needed to be sophisticated enough to detect and contain the professional intruder.

6.8 Business Model for Dealing with the Risk

SEBRING management indicated that they would continue to allocate funding for security initiatives identified by the Director of Network and Information Security.

SEBRING recently issued an Request for Proposal (RFP) for security assessments, penetration testing, and technology assessments, including the following tasks:

- Identify and document points of access to SEBRING’s networks
- Conduct a risk assessment of the present network architecture
- Perform a vulnerability accessibility test of the identified access points
- Assess the impact of inappropriate access to those points

- Provide a confidence level that all access points were identified
- Provide tools to identify and document changes in access points
- Provide possible solutions to reduce vulnerabilities
- Provide input to future network architectures to address security.

6.9 Lessons Learned from the Incident

SEBRING is not as secure as they would like to be and recognize that they are their own worst enemy. Before the intrusion, security concerns were general in nature. Internet connectivity started as a technical whim and it grew very fast. Management failed to recognize and take control of the technology until it was almost too late. People and business units were connecting to the Internet on their own and introducing new risks and exposing the network.

Personnel need to be reminded of the security exposures and the SEBRING security policies that justify the centralized control and the attendant procedures and processes. Centralized control of what is bought and connected to or put on the network/desktop is absolutely necessary.

Networks are being penetrated. The system administrators do not know the degree of the penetrations, and they cannot keep track of what is happening adequately. In reality, a company could be put out of business.

Management has to be willing to tell the truth concerning security exposures. Honesty concerning reasons for downtime must be explained or SEBRING will lose credibility. Security is necessary for customer credibility.

Recognizing the issue of security early and addressing it in plans, contracts, and personnel practices as well as in procurement and performance assessments is of paramount importance if scarce resources are to be used effectively to solve the problem.