OFFICE OF THE MANAGER
NATIONAL COMMUNICATIONS SYSTEM

INFORMATION SECURITY BUSINESS CASE

CASE STUDY #2 - EL DORADO

20 December 1996

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 #2-EL DORADO

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 second 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 second case study organization is EL DORADO.

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 EL DORADO Case Study

The first step in performing the EL DORADO 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 EL DORADO 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 EL DORADO. Section 3 depicts the activities that motivated EL DORADO 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 EL DORADO. Section 6 provides the lessons learned by EL DORADO management as a result of the network intrusion.

2. OVERVIEW OF THE EL DORADO ORGANIZATION

2.1 Description of the Business

EL DORADO is a federal government activity involved in human space flight. It has a workforce of 15,000 to 20,000 civil servants and contractors.

2.2 Description of Network and Information Systems Environment

Because of its diverse research communities and directorates, the EL DORADO computing environment is heterogeneous and multi-platform. The environment consists of, but is not limited to, the following technology:

- Hosts and Application Servers:
  - Consolidated business operations are IBM-compatible mainframes (offsite).
  - Engineering/scientific computing is performed on Cray and Digital Equipment Corporation (DEC) systems.
  - Host O/S: MVS, VM, VMS, UNIX®, Unisys.
  - Application server O/S: UNIX, Microsoft Windows NT™ Server, Novell® NetWare.
- Networking and Telecommunications:
  - Terminal Networks: Systems Network Architecture (SNA), Unisys Data Communications Architecture (DCA), Digital Equipment Corporation Network (DECNET).
  - Local Area Networks (LANs): Transmission Control Protocol/Internet Protocol (TCP/IP), Novell Internet Packet Exchange (IPX), and AppleTalk. Routers are used to segment, filter, and control network traffic.
  - Protocol Gateways: SNA-TCP/IP, Unisys DCA-TCP/IP, AppleTalk TCP/IP, IPX-SNA, AppleTalk-SNA, Remote IPX, Remote AppleTalk, Remote TCP/IP, Async-TCP/IP, Async-SNA.
  - Fiber Distributed Data Interface (FDDI) campus backbone that is centrally supported. Building backbones use Ethernet technology. Extensive use of 10Base T (twisted pair) Ethernet technology within the buildings to connect devices to the building backbone.

- Windows 95©, Windows NT, Windows 3.11 and MacOS for peer-to-peer networking.
- Links to other facilities, universities, and contractors.
- Several electronic mail systems.
- Directory for electronic mail.
- Digital Private Branch Exchange (PBX) for voice, voice messaging, and some asynchronous data communications.

2.3 Description of Operational Environment

EL DORADO is organized into 21 operating elements. Each operating element implements and maintains a variety of information technology resources consistent with EL DORADO-wide policies.

The following types of functions are performed at EL DORADO:

- Space Shuttle Operations
- Space Station Operations
- EVA Projects
- Information Systems
- Safety, Reliability, and Quality Assurance
- Technology Transfer
- Flight Crew Operations

The directors and line managers are responsible for security within the individual operating elements.

3. MOTIVATION(S) FOR ESTABLISHING SECURITY PROGRAM

The security program at EL DORADO started as a result of partnerships with the Department of Defense to run classified missions. Though the military s involvement has a long history, it was not until 1982 that classified missions were included as part of the operations of the EL DORADO center.

Mission control and training facilities were created to handle missions classified up to the Secret level. At this time, EL DORADO s personnel were educated in security, as most of them had to be cleared and trained to handle the classified missions. The Challenger accident in 1986 created a heightened concern for security. In 1987 a high-visibility incident occurred in which mission-critical flight software was found to contain several unauthorized changes. Because of concerns about the integrity of mission software, the agency conducted a six-month independent security review in 1988 before the return to flight operations. The study reviewed sensitive unclassified systems.

This security review was conducted on the systems involved in the development of mission critical software to determine the overall security posture. The independent review found that EL DORADO systems were vulnerable in several areas, including access control, management control, and disaster recovery. The extent of vulnerability of access control was highlighted by the ease with which the team was able to gain access to one of the mission critical mainframe machines. Without the benefit of an authorized userid and password, the team still obtained access to the mainframe and gained control of the operating system within 4 hours. The team found that there was little or no control over the controlled elements and restricted elements used by systems programmers in maintaining and modifying the operating system. The team also found that there was little or no review by security personnel of the issuance of userids and access privileges. Several critical systems had no disaster recovery plans in place. Overall, the review team identified approximately 80 specific items that needed technical or management attention.

In response to the findings, EL DORADO management formed a 35-member security team to address the problems in all specific systems and to initiate an action plan that would address the security concerns for all systems throughout the center.

The security review motivated senior management to initiate a center-wide effort to ensure that information security policies and procedures were put in place and that the center was in compliance with Appendix III to Office of Management and Budget (OMB) Circular A-130. While security concerns initiated a specific set of activities, EL DORADO management has noted that the goals of the security program are to provide appropriate, cost-effective levels of integrity, availability, and, as necessary, confidentiality to be based upon an assessment of the risks and security needs for each system.

One of the major activities of the security review was conducting penetration testing. EL DORADO learned that penetration testing could provide extremely useful data about the security resistance of a system and that it could continue to be a useful tool in reviewing other critical systems. The initial penetration testing was done during a time when there was little connectivity between systems and networks, so links were not easy to exploit. However, EL DORADO s security personnel could see the trend in networks and began to consider the impact that networks would have on operations and security.

Several incidents and a recognition of the dynamic nature of security have motivated EL DORADO to keep its security program going. EL DORADO actively conducts penetration tests as a means of identifying and understanding its vulnerabilities. After the penetration test has been completed, a technical briefing is prepared to present the manager of that system with a thorough picture of the vulnerabilities that could be exploited by an intruder. The data from penetration tests and incidents is also used to develop anecdotal security briefings that are used to reinforce security awareness in both employees and senior management. Two examples of EL DORADO anecdotes used in security briefings are provided below:

Anecdote Number One: Government Liability

The director of an engineering research organization argued that this organization did not need computer security. The organization s network was later penetrated and the intruder obtained root (system administrator) privileges on several machines. The intruder then installed a sniffer program to capture information on traffic to, from, and through the network. The sniffer program successfully captured connection data including userids/passwords for 130 other computer systems, some of which were non-government systems (academic and commercial).

Law enforcement officials later caught a hacker they believed had perpetrated the EL DORADO intrusions, but discovered that the hacker was not the EL DORADO intruder, despite a very similar modus operandi. Had law enforcement been able to arrest the EL DORADO intruder, the director of the organization, who had claimed he had no use for security, would have been responsible for testifying in the trial. When conducting these awareness briefings, the EL DORADO Center Computer Security Manager (CCSM) has found that organization directors often relate to this point best: the lack of security leading to an intrusion can affect the director personally when the director must travel to other states to testify on behalf of the prosecution. This incident also raised several liability concerns at EL DORADO. For example, what is the government s liability for intrusions that took place on commercial and academic systems that were compromised as a result of EL DORADO s carelessness? Could EL DORADO, or more specifically the director of the organization that was directly compromised, be found negligent for lack of adequate security?

The EL DORADO information security manager uses this true anecdote to raise awareness and to remind senior-level managers that they are responsible for their systems/networks and that their actions or inactions can have tremendous consequences.

Anecdote Number Two: Data Integrity

An EL DORADO engineering research facility had a LAN of 12 computers that contained all of its research. On a Tuesday morning after a long weekend, during which the network was left unattended for 3 days, the system administrator found 1.5 megabytes of data that was not on the machine the previous Friday. An intruder had hacked the machine and was using it to store domain data for .mil (military) and .gov (government) systems. A 4-day investigation was conducted, requiring 7 man-weeks of labor. In addition, the lab was shutdown for 2 weeks while data integrity was examined to make sure that no unexpected changes had been made.

In an interesting sidenote, by examining audit logs, it was discovered that the hacker had gained access to the computer when a new userid was created, with root access, for the installation of a new CD-ROM device. The product installation instructions called for the creation of the account, but did not remind the installer to remove the account when installation was complete.

This anecdote demonstrates the effects an intrusion can have on business operations and critical data. The fact that all of the lab s research was contained on a single network meant that the integrity of all data had to be examined after the system was compromised.

Incidents in general

EL DORADO senior management is very sensitive to incidents that could be embarrassing or have legal implications for the organization. Misuse is high on their list of concerns as increasingly, organizations inside and outside of government are finding that employees are using computer systems to access, store, and distribute inappropriate material or are using computing resources for non-government business activity.

4. EL DORADO S NETWORK AND INFORMATION SECURITY PROGRAM

The EL DORADO information security program is based on a risk management approach that places the responsibility for risk acceptance on the line managers most familiar with the data, applications, equipment, and facilities. The program addresses the basic objectives of information technology security (ITS): (1) integrity, the ability to ensure that system software, applications, and data, the hardware/configuration, the connectivity, and the status of privileged settings cannot be altered during storage or transmission; (2) availability, the ability to ensure that systems, applications, and data are there to be accessed when needed; and (3) confidentiality, the ability to ensure that information is disclosed only to those who have a valid business need to use it. The program also implements the requirements contained in Federal and Agency guidelines such as OMB Circular A-130.

4.1 Organizational Location and Reporting Chain

The EL DORADO Center Computer Security Manager (CCSM) reports directly to the Chief Information Officer (CIO). The CIO is responsible for Information Technology (IT) policy and standards. The CIO is a member of the Center Director s Staff.

4.2 Network and Information Security Staff

The total information security staff, including the CCSM and Deputy CCSM (DCCSM), is 6. Historically, contractor personnel performed the EL DORADO network and information security support functions. However, as EL DORADO moved to a completion form contract, they found that the security functions did not adequately protect this type of contract vehicle.[1] At this point, EL DORADO began transitioning information security positions to civil service staff. The staff now comprises civil servants with the exception of the virus response team, which is still staffed by contractor personnel. With the exception of the CCSM, all information security positions report to the Business and Information Systems Director (BISD).

[1]Under a completion form contract vehicle, the Government identifies a set of requirements and performance metrics to the contractor. The contractor internally determines how to meet the requirements and performs the work. The contractor is only judged on how well the requirements were met. Completion form contracts differ significantly from task order form contracts in that the Government does not have the opportunity to review the approach or methodology, only the results.

4.3 Organizational Interfaces

4.3.1 Internal Interfaces. EL DORADO has an internal security committee that serves as the primary forum for debate of security policies and practices. This committee discusses potential policy changes and is the prime means of communication between the network and information security personnel and the EL DORADO senior management. The committee is made up of the CCSM, DCCSM, and the Computer Security Officials (CSOs) from each directorate, program/project, or staff office at EL DORADO. Each member of the EL DORADO senior staff appoints at least one civil servant to represent his or her interests in matters dealing with computer security. The representative is responsible for voting the director s position on the interpretation and implementation of network and information security policy.

4.3.2 External Interfaces. EL DORADO participates in the agency-level ITS Working Group, which operates on a lead center/expert center concept. This mode of operations enables the agency CIO to keep staff at a minimal level.

4.4 Center Information Security Policies and Procedures

EL DORADO has issued a set of ITS policies articulated in an information security manual dated October, 1992. The summary provided below is taken from this manual.

The security program is based on a risk management approach that places the responsibilities for risk acceptance on the line managers most familiar with the data, applications, equipment, and facilities requiring protection. The manual is divided into sections by program elements. An overview of the sections provides a global overview of the program as well.

- **ITS Management Responsibilities** describes the roles and responsibilities of line management, CSOs, support personnel, and users.
- **ITS Management** identifies and describes ITS management processes.
- **Introduction to ITS Risk Management** provides a risk management methodology by describing an integrated approach to application security and DPI security.

- **ITS Risk Management** describes administrative requirements and how to accomplish the ITS risk management task, including sensitive application (SA) security certification, risk management planning, contingency planning, formal and abbreviated risk analysis, and management response to risk analysis.
- **ITS Requirements** establishes technical and physical requirements for ensuring a baseline acceptable level of ITS.
- **ITS Awareness and Training** describes how the ITS awareness and training program will be conducted at EL DORADO.
- **Personnel Security Investigations** provides guidelines and administrative requirements for the development and operation of a personnel screening process that meets the intent of Federal law and is sufficient to protect sensitive ITS resources.
- **ITS Incident and Reporting** provides guidelines and administrative requirements for the response and reporting of ITS incidents.

The manual is currently being revised and updated by the Network and Information Security Staff. The new manual parallels the old manual in its philosophy (risk-based as opposed to compliance-based), features a new chapter on appropriate use of EL DORADO's computers, and is being completely revised to accommodate the new Appendix III to OMB Circular A-130.

4.4.1 ITS Management Responsibilities. All EL DORADO and contractor personnel who manage, use, program, or operate automated information systems or telecommunication resources are responsible for ensuring appropriate levels of integrity, availability, and confidentiality.

ITS management responsibilities are specifically called out for the following positions: Center Director, Chiefs of Staff Elements, Director of Information Systems, CCSM, ITS Security Program Manager, Director of Center Operations, Director of Human Resources, Director of Administration, Data Processing Installation (DPI) Line Manager, SA Line Manager, Staff Element CSO, ITS Security Committee, DPI CSO, SA CSO, and the EL DORADO Security Division.

4.4.2 ITS Management. The EL DORADO staff elements are responsible for management control of the security for individual applications, DPIs, and telecommunications facilities. The

CCSM and the ITS Program Manager are responsible for the overall management control of the Center ITS Program. Implementation is decentralized through the EL DORADO staff elements. The CCSM and Program Manager perform the following functions to ensure that the ITS security program is implemented and maintained consistent by accordance with Federal and Agency requirements:

- Establishing the overall direction and structure of the program
- Developing and promulgating ITS policy, requirements, and guidelines
- Performing periodic management reviews, evaluations, and independent ITS audits and tests
- Maintaining a database to monitor risk management activities.

EL DORADO is also required to provide the agency headquarters with an annual ITS Security Plan. The purpose of this plan is to summarize the status and direction of activities throughout the center and at DPIs under the cognizance of the center. The intent of the plan is to consolidate EL DORADO s goals, objectives, and activities into one document.

4.4.3 ITS Risk Management. The EL DORADO ITS risk management process integrates SA evaluation and certification activities and functions with DPI risk analysis and continuity of operations activities. This integration allows management to view security from a total system perspective and ensures that risk management plans are developed and maintained consistent with Federal- and Agency-level requirements.

4.4.4 ITS Requirements. ITS requirements are based on four levels of information, as defined in Table 1. Application line managers assign the sensitivity and criticality level of data or applications. The level assigned will be at least as high as the most sensitive or critical data that will be processed by the application.

Table 1. ITS Requirements

ITS CRITICALITY LEVEL	EXPLANATION Automated information, automated applications, or computer systems, the inaccuracy, alteration, disclosure, or unavailability of which:

3	▪ Would have an IRREPARABLE impact, permanently violating the integrity of the agency s missions, functions, image, and reputation. The catastrophic result would not be able to be repaired or set right again; or ▪ Would result in the loss of MAJOR tangible asset(s) or resource(s), including posing a threat to human life.
2	▪ Would have an ADVERSE impact actively opposed to agency s missions, functions, image, and reputation. The impact would place the agency at a significant disadvantage; or ▪ Would result in the loss of SIGNIFICANT tangible asset(s) or resource(s).
1	▪ Would have a MINIMAL impact on agency s missions, functions, image or reputation. A breach of this sensitivity/criticality level would result in the least possible significant unfavorable condition with a negative outcome; or ▪ Could result in the loss of SOME tangible asset or resource.
0	▪ Would have a NEGLIGIBLE impact on agency s missions, functions, image, or reputation. The impact, while unfortunate, would be insignificant and almost unworthy of consideration; or ▪ Probably would not result in the loss of a tangible asset or resource.

4.4.4.1 Network Security Requirements — Management Guidelines. These guidelines are the basis for host network security requirements. The guidelines apply to all EL DORADO networks:

- EL DORADO will protect its network resources to a level commensurate with their importance to network functions and with their importance to the hosts and data they support.
- EL DORADO will implement safeguards to defend its networks against misuse or attack.
- The architecture of EL DORADO s networks will be flexible enough to enable effective defense against attack on any node through selective isolation or filtering.
- EL DORADO networks will be implemented or modified only after ITS security implications have been considered.
- EL DORADO s priorities regarding network security are the following:
  - Protect Government resources
  - Minimize disruption of service
  - Support legal or administrative enforcement efforts.

- EL DORADO will develop and implement a Network Emergency Response Plan which delineates specific actions to be taken in the event of a security incident to limit the impact of a network attack or disruption.
- Some networks or network segments may have higher security requirements than others. Each host will comply with all of the security requirements of the network(s) or network segment(s) to which it connects. This does not require all hosts of interactive workstations on a network to have the same sensitivity/criticality level.
- The ultimate responsibility for the security of any node on any EL DORADO network will reside with the node owner, not with the network.

4.4.5 ITS Awareness and Training Program. The ITS Awareness and Training Program is a diversified program sponsored and conducted by Center-level organizations, staff element-level organizations, and support contractors. The nature and type of awareness and training required are determined by the sponsoring organization. In general, Center-level organizations sponsor and conduct awareness briefings and training courses that apply across the EL DORADO community. Staff elements sponsor and conduct awareness briefings and training courses specific to their organizations. Support contractors conduct briefings and training that apply to their organizations and contractual requirements. The following are examples of training and awareness sessions at EL DORADO:

- Center-Level Training
  - Risk management training
  - Annual security refresher briefing
  - Security seminars
- Staff Element-Level Training
  - Awareness briefings
  - System-specific training
- Training Provided by Contractors
  - ITS awareness and training programs
  - Job-specific and system-specific training

4.4.6 ITS Personnel Security Investigations. Personnel security investigations are initiated to ensure that only reliable individuals have access to Government data, applications, and systems. Every line manager is responsible for ITS resources under his/her control, including sensitive/critical data, applications, systems and personnel. Every user who has privileged access to a computer operated by or on behalf of the government must be investigated. Privileged access is meant that the user can bypass significant security processes and controls.

4.4.7 ITS Security Incident Response and Reporting. The EL DORADO security manual requires that all incidents, whether in contractor or Government facilities, will be reported. The security manual states that the response to an incident should limit the adverse impacts of the incident and quickly alert other organizations with similar technical vulnerabilities to the possibility of a similar threat. The reporting of an ITS incident will include adequate information for a complete investigation. The reporting process includes the gathering of information and forwarding of a summary document with appropriate details to security officials. Incident reporting is the responsibility of all EL DORADO and EL DORADO contractor employees, including computer users, operators, security personnel, and managers.

4.4.8 Other EL DORADO ITS Security Guidelines. EL DORADO has several updated guidelines articulated in documents produced after the 1992 manual was issued. These include guidelines for the use of government resources, access to government information, security of workstations, password management, and virus incident recognition and reporting.

4.5 Information Security Program Costs

4.5.1 Costs Associated with Studied Incident. EL DORADO does not track incident cost specifics unless an intrusion or incident results in a prosecution. However, the research team was able to assess the cost of the studied incident in which unauthorized changes were made to mission critical flight software, at roughly $1,000,000. It is highly likely that the actual cost of the incident was much higher than the research team estimate. The specific costs associated with this single incident are listed in Table 2.

Table 2. Cost of EL DORADO Incident

DESCRIPTION	COST
Independent review team (expenses for five people for 2 weeks)	$4000 - $5000
EL DORADO Security Team (35 people for 4 months, average GS-12 level)	$400,000 - $450,000
Contractor support to committee (3 to 5 man years)	$300,000 - $400,000
Intrusion detection tool	$100,000 - $150,000
Blockade software	$25,000 - $30,000
Smartcard access control system	$40,000
TOTAL	**$869,000 - $1, 175,000**

4.5.2 Cost for Sustaining the Information Security Program. The cost of sustaining the EL DORADO information security program is estimated at roughly $400,000. This estimated cost includes only staff salaries. Other relevant expenses, such as the cost of printing manuals, etc., are inseparable as line items in the EL DORADO budget and have been left out of the cost estimate. Table 3 provides a breakdown of staffing cost data.

Table 3. Cost of Sustaining EL DORADO Information Security Program

DESCRIPTION	COST
CCSM (GS-14)	$66,711
Deputy CCSM (GS-14)	$66,711
GS-13 - Assessments	$56,504
GS-13 (Committee Communications)	$56,504
GS-12 Assessments	$47,518
GS-6 Assessments	$24,105
Contractor - Virus Response	$75,000
TOTAL	**$393,053**

5. EL DORADO BUSINESS CASE PROCEDURES

EL DORADO does not require the use of a specific business case or economic methodology in its security program. EL DORADO does, however, require that line managers of sensitive applications and data processing installations perform risk analysis. For each sensitive application, the line manager is required to document the results of security tests, list identified risks, indicate whether risks are acceptable or unacceptable, estimate costs of risk mitigation, and provide an implementation schedule. Line managers of installations that process sensitivity/criticality level 3 data are required to perform risk analysis to enable them to make informed decisions about the acceptability of risks. For level 3 systems, the risk reduction analysis should include a quantitative cost-benefit analysis. Additionally, a data processing installation risk analysis report should describe the analysis that was conducted.

6. EL DORADO MANAGEMENT VIEW OF SECURITY

The EL DORADO CIO and Deputy CIO were interviewed concerning security issues. It should be noted that the CIO has no operational responsibilities and is mainly involved in policy and guidance. Also, the EL DORADO senior management prefers to frame the dialogue in terms of "incidents" and not "intrusions." Incidents are defined as " Any event, any suspicion that an event has occurred, or any discovery of a vulnerability that could pose a threat to the integrity, availability, or confidentiality of EL DORADO's information technology systems, applications, or information." Intrusions are defined as a subset of incidents that have originated outside the EL DORADO community. The interview addressed several questions as follows.

6.1 Senior Management Perceptions of the Security Risks

EL DORADO s senior management indicated that the risks are growing faster than the organization's ability to deal with them. There are three reasons for an increased concern about incidents: EL DORADO has increasingly global connectivity; The workforce has increasingly powerful desktop workstations that can make use of that connectivity; Downsizing and uncertainty in the workplace may provide individuals who have very high privilege levels on EL DORADO systems with the motivation to do harm.

6.2 How Much of a "Wake-Up Call" are the Incidents?

From an operational perspective, incidents have provided a wake-up call. Integrity and availability are the security drivers when it comes to mission-critical systems, but security incidents also cause users to become concerned about the potential for a loss of privacy.

The incident regarding unauthorized changes in flight software was a wake-up call in that it attracted attention outside of the EL DORADO organization. The initial penetration testing also provided a wake-up call. Today, internal penetration testing is used as a mechanism to keep people alert and remains the single most important tool for evaluating the security of any given computer system.

6.3 How Much of a Motivation for Implementing an Information Security Program Are Government Regulations versus Perceived Risks?

EL DORADO senior management is definitely shifting toward perceptions and moving from meeting the regulations to understanding the perceived risks. Whether regulation serves as a motivator depends upon where the person is in the bureaucracy or in the operational hierarchy. EL DORADO is far removed from the Washington bureaucracy and the agency headquarters; therefore, they have a little more flexibility in how it chooses to protect its assets. However, no matter how far they are from Washington, they still have to obey the law. EL DORADO takes a conservative view of implementation of OMB A-130, and their strong, proactive program is well supported by senior management. They took great pains in their manual to present security as a good business practice, not because regulations require security precautions, but because taking security precautions is a good business practice.

6.4 What Effects Did Military Classified Programs Have on EL DORADO Security Requirements and Funding?

Overall, the military approach was expensive and contrary to the organization's usual approach to doing business. Classified operations did not fit in well with the EL DORADO organization, which as a public agency was used to conducting business in the public eye. Imposing security for classified operations required extensive retrofits on unique computer systems that had never been designed to accommodate such security. After the discontinuance of military classified programs it was tougher to justify security spending, but having set up security for classified operations helped the organization transition from a compliance-based to a risk-based security program.

Probably the most significant legacy associated with having had the workforce trained in conducting classified processing was that the workforce, particularly middle management, associated the term "computer security" with the top-down, extremely expensive, compliance-based classified approach. It took a long time and education to get people to make the shift in their thinking from compliance-based to risk-based. Compliance-based memories made it difficult to sell a risk-based approach because the word "security" itself had bad connotations.

6.5 Knowing What You Know Now, What Would You Have Done Differently About Information Security in the Past?

The senior management indicated that had they known the implications earlier, they would have created a more dedicated structure earlier in terms of policy and operations. They would have placed more requirements on networks in the full sense and would not have used UNIX or ad hoc open systems to the extent that they did.

6.6 What Liability Do You Perceive Due to Security Exposures With Respect to Customers, Congress, and the Taxpayers?

The agency is primarily a research and development organization. It is expected to take reasonable risks, but liability is closely tied to funding. There is a significant and visible liability in not accomplishing its assigned mission. That liability could be devastating and could end the space program.

6.7 Security Concerns Regarding Outsourcing

The term "outsourcing" is just a variation of contracting and the agency has been contracting since the beginning of its existence. There are no new concerns in this area because of the historical relationship with contractors and the part they have played in the space program. There are incentives for contractors to enforce the security policies. " Administrator rights" are one of the biggest concerns with contracting because there must be some separation between the contractors and some government materials, such as proposals. Technology is making the issue of separation of even more concern because authentication is taking place at one level instead of many and it is easy to move from one system/network to another.

Contractor compliance with EL DORADO security policies is not viewed as a problem. The contractors perform as directed by the government. The contractor risks may include reduced award fees and contractor reputation within the government community.

6.8 Approach for Sustaining Network and Information Security Over Time

EL DORADO's approach for sustaining the Information Security Program is to ensure continued senior management support, provide a level of independence to the operating activities in the implementation of policy, and conduct a variety of audits such as penetration testing.

6.9 Justifying the Expense of Maintaining the Program

Senior management support for the program is high; however, there is also a realization that spending more does not always equate to spending well. Some replication among different programs is inherent in the lack of centralization, but to centralize would lead back to compliance-based programs. Accountability is maintained throughout the various levels of management.

6.10 Transition from Primarily Government-owned, Provisioned, and Managed Networks to the Public Switched Network

EL DORADO is increasingly utilizing commercial off-the-shelf software to allow for greater standardization. Commercially available telecommunications are also used as the public switched networks provide reasonably robust communications. EL DORADO leases private lines and frequently uses point-to-point encryption to communicate over public networks.

6.11 Organization Comfort Level with What EL DORADO Has Done and Plans for the Future

There is a low comfort level for networks because EL DORADO organizations do not have total control over the provisioning, management, and security of networks. Since networks are centrally provided, security levels are established centrally. There is a higher comfort level with distributed systems, because internal organizations determine the risks and the degree of security they feel is required. Security standards are best applied in a distributed rather than a centralized manner.

6.12 Business Models for Dealing with Network and Information Security Risks

EL DORADO does not currently use any specific or standard business models. Operating organizations, however, are required to perform risk analyses and implement security controls that are cost-beneficial. The managers of high risk systems are required to perform risk and risk reduction analyses.

6.13 Lessons Learned from the Incident(s)

EL DORADO acknowledges that they are their own worst enemy. The greatest threat comes from insiders; controlling authorized insiders is a difficult issue because some users treat computing as a right, rather than a privilege. In an era in which downsizing and uncertainty seem to be inevitable characteristics of the current job environment, EL DORADO realizes that it has many people who have very high levels of privileged access to computers but who, by a stroke of the budget pen, may suddenly be motivated to do them great harm. To some extent, this is a risk EL DORADO has to accept, but they also have an obligation to assess it and to mitigate it.

Education and awareness are absolutely necessary. EL DORADO can learn and profit from the experiences provided from past incidents.

Unclassified information security programs should be risk-based. EL DORADO has tried both compliance- and risk-based approaches successfully, but the risk-based approach works best in the current unclassified environment in which they operate.

The external hacking threat will continue to be a problem as network connectivity increases. System integrity must be based on failure mode and effects analysis.