Part V
Example

20 A Hypothetical Case Study

20.1 Introduction

This chapter illustrates how many of the concepts described in this Handbook are applied in a "real world" situation. In particular, the Example shows how the concept of risk management is applied to an actual system. To do this, a scenario concerning a *Hypothetical Government Agency* (HGA) is presented.[92] The chapter defines the system, describes some of its security problems, and the security safeguards which have been selected.

This chapter presents a discussion of how a hypothetical government agency deals with computer security issues in their operating environment -- it is not a paradigm of security. This chapter is provided for illustrative purposes only -- and should not be construed as guidance or specific recommendations to solving specific security issues. No single solution can solve similar security problems in all environments *nor are the security measures taken necessarily the best that could have been taken*.

In the real world, many solutions exist for problems -- this example necessarily simplifies the issues presented. This section also highlights the importance of management acceptance of a particular level of risk -- this will, of course, vary from organization to organization. It is management's prerogative to decide what level of risk is appropriate given their operating and budget environment, and other applicable factors.

This example can be used to help understand how security issues are examined, how some potential solutions are analyzed, their cost and benefits weighed, and ultimately how management accepts responsibility for risks. Finally, note that, because of the nature of a hypothetical example, many details are omitted.

The example addresses some of the major types of processing platforms linked together in a distributed system: PCs, LANs, WANs, and mainframes. This was done to highlight the similarities and differences among controls in the different processing environments. The example does not show how to secure PCs, LANs, WANs, or mainframe computers.

Organization - This chapter is organized around a risk analysis performed at HGA. Section 2 begins by presenting the computer systems used by HGA and in the basic security procedures. Sections 3 introduces the risk analysis. Sections 4 through 6 describe the risk analysis in greater detail: Section 4 summarizes relevant high-level policies, section 4 identifies HGA's high-level assets and threats, and section 6 describes selected risk assessment results and HGA's risk mitigation decisions. Section 7 provides a short summary and conclusions.

A comprehensive example attempting to illustrate all Handbook topics would be inordinately long. Instead, this chapter provides an *illustrative sampling* of topics, *none of which is*

[92] While this chapter draws upon many actual systems, details and characteristics were changed and merged. Therefore, any similarity to real systems is illusory.

treated exhaustively. For continuity of exposition and focus, most of the discussions center on HGA's *Time and Attendance* (T&A) application.

20.2 Computer Architecture Description

This section briefly describes some aspects of HGA computing (as it exists *before* addressing security) so that this case study can proceed. Many vulnerabilities exist in HGA systems, some of which will be discussed later.

HGA relies on the distributed computer systems and networks shown in Figure 1. They consist of a collection of components, some of which are systems in their own right. Some belong to HGA, but others are owned and operated by other organizations. This section describes these components, their role in the overall distributed system architecture, and the ways in which they are used by HGA.

20.2.1 Architecture

Frequently Used Acronyms

CIO:	Chief Information Officer
COG:	Computer Operations Group
CP:	Contingency Plan
HGA:	Hypothetical Government Agency
I&A:	Identification and Authentication
LAN:	Local Area Network
PC:	Personal Computer
T&A:	Time and Attendance
WAN:	Wide Area Network

Most HGA users (a mix of clerical, technical and managerial staff) are provided with personal computers (PCs) located in their offices. These PCs are used for word processing and other common applications including spreadsheet and project management tools. Each PC includes hard disk and floppy disk drives.

The PCs are connected to a local area network (LAN) so that users can exchange and share information. The central component of the LAN is a *LAN server*, a more powerful computer that acts as an intermediary between PCs on the network and provides a large volume of disk storage for shared information including shared application programs. The server provides logical access controls on potentially sharable information via elementary access controls lists. These access controls can be used to limit user access to various files and programs stored on the server. Some programs stored on the server can be retrieved via the LAN and executed on a PC; others can only be executed on the server.

In order to initiate a session on the network or execute programs on the server, a user at a PC must log into the server and provide a user identifier and password known to the server. Then they may use files for which they have access.

One of the applications supported by the server is *electronic mail* (e-mail), which can be used by all PC users. Other programs that run on the server can only be executed by a limited set of PC users.

Several printers, distributed throughout HGA's building complex, are connected to the LAN. Users at PCs may direct printouts to whichever printer is most convenient for their use.

Figure 1

Since HGA must frequently communicate with industry, the LAN also provides a connection to the Internet via a *router*. The router is a network interface device that translates between the protocols and addresses associated with the LAN and the Internet. The router also performs *network packet filtering*, a form of network access control, and has recently been configured to disallow non-e-mail (e.g., file transfer, remote login) between LAN and Internet computers.

The LAN server also has connections to several other devices.

- A *modem pool* is provided so that HGA employees on travel can "dial up" via the public switched (telephone) network and read or send e-mail. In order to initiate a dial-up session, a user must successfully log in. During dial-up sessions, the LAN server provides access only to e-mail facilities; no other functions can be invoked.

- A *special console* is provided for the server administrators who configure the server, establish and delete user accounts, and have other special privileges needed for administrative and maintenance functions. These functions can only be invoked from the *administrator console*; that is, they cannot be invoked from a PC on the network or from a dial-up session.

- A *connection to a Government agency X.25-based wide area network* (WAN) is provided so that information can be transferred to or from other agency systems. One of the other hosts on the WAN is a large multi-agency mainframe system. This mainframe is used to collect and process information from a large number of agencies while providing a range of access controls.

20.2.2 Operational Authority/Ownership

The system components contained within the large dashed rectangle shown in Figure 1 are managed and operated by an organization within HGA known as the *Computer Operations Group* (COG); these include the PCs, LAN, server, console, printers, modem pool, and router. The WAN is owned and operated by a large commercial telecommunications company that provides WAN services under a government contract. The mainframe is owned and operated by a federal agency that acts as a service provider for HGA and other agencies having connections to the WAN.

20.2.3 Applications and Use

PCs on the HGA LAN are used for a variety of word processing and data manipulation tasks. Many of these tasks are concerned with data that is sensitive with respect to confidentiality or integrity. Some of these documents and data are also required to be available in a timely manner.

In the discussion that follows, particular attention is given to a specific set of tasks that involves the entry, verification, and approval of T&A data. The LAN server programs used for this purpose are part of the T&A application. Each week, employees must sign and submit a time sheet that identifies the number of hours worked and amount of leave they have taken. After entering the data for a given group of employees the clerk runs an application on the LAN server that attempts to verify the data's validity. The application compares the data with a limited database of employee information to detect incorrect employee identifiers, implausible numbers of hours worked, and so forth. After correcting any detected errors, the clerk runs another application that formats the T&A data into a report, flagging exception conditions (e.g., negative leave balances).

For each department, there are one or more supervisors who review and are authorized to approve these reports by running another server program that is part of the T&A application. When a supervisor approves the T&A data, this application logs into the inter-agency mainframe via the WAN and transfers the data to a payroll database on the mainframe. The mainframe later prints paychecks or, using a pool of modems that can send data over phone lines, it may transfer the funds electronically into employee-designated bank accounts. Withheld taxes and contributions are also transferred electronically in this manner.

In addition, the mainframe provides storage and retrieval services for other databases belonging to individual agencies. For example, several agencies, including HGA, store their personnel databases on the mainframe; these databases contain dates of service, leave balances, salary and W-2 information, and so forth.

In addition to their use in the T&A application, HGA PCs and LAN server are used to manipulate other kinds of information that may be sensitive with respect to confidentiality or integrity, including personnel-related correspondence and draft contracting documents.

20.2.4 Basic Procedures

This section describes elements of HGA's procedures for use of computer systems, and for the T&A application in particular.[93]

20.2.4.1 HGA System Use and Administration

The HGA's COG is responsible for controlling, administering, and maintaining the computer resources owned and operated by HGA; these are depicted in Figure 1 enclosed in the large, dashed rectangle. Only individuals holding the job title "System Administrator" are authorized to establish login IDs/Passwords on multi-user HGA systems (e.g., the LAN server). Only HGA employees and HGA contract personnel are permitted use of the system, and only after receipt of written authorization from the Department Supervisor (or in the case of contractors, the contracting officer) to whom these individuals report.

Each authorized user is assigned a separate login ID and password. Users are forbidden from sharing their login ID(s) and password(s) with others. Users are expected to comply with all HGA password selection and security procedures (e.g., periodically changing passwords). Users who fail to do so are subject to a range of penalties including reprimands.

Users creating data that is sensitive with respect to disclosure or modification are supposed to make effective use of the automated access control mechanisms available on HGA computers to reduce risk of exposure to unauthorized individuals. (Appropriate training and education are in place to help users do this.) In general, access to disclosure-sensitive information is to be granted only to individuals whose jobs require it.

Users are not authorized to install software on PCs or the server. Only Administrators are authorized to install software packages, and only those approved by the Manager of the COG. (These stipulations are part of an HGA assurance strategy that relies on the quality of the engineering practices of vendors to provide software that is adequately robust and trustworthy.) Licensed copyrighted PC software applications are generally installed only on the server and protected to the extent practical from unauthorized copying. System administrators are supposed to regularly run virus detection and other security configuration validation utilities on the server and other applicable components.

---

[93] Readers are again cautioned that presentation of HGA's policies are not meant to imply that such policies are ideal.

COG is responsible for ensuring that all files on the server are backed up daily and stored in a secure off-site facility. COG personnel are also responsible for reviewing audit logs generated by the server, identifying audit records indicative of security violations and reporting such indications to the agency team for computer security incident handling. The COG Manager will assign these duties to specific members of the COG staff and, through appropriate management oversight, ensure that they are implemented as intended.

COG is responsible for maintaining the HGA computing hardware and software in a secure manner. No communication devices or network interfaces is authorized to be connected to HGA systems without written approval of the COG Manager. The COG staff is responsible for installing all known security-related software patches in a timely manner. Also, COG is responsible for maintaining spare or redundant PCs, servers, storage devices and LAN interfaces to assure that at least 100 persons can simultaneously perform word processing tasks at all times.

20.2.4.2 Training

COG is tasked to issue copies of all relevant security policies and procedures to new users. Before activating a system account for a new user, COG requires that the user:

- attend a security awareness and training course or complete an interactive computer-aided-instruction training session; and

- sign an acknowledgement form indicating that the user understands their security responsibilities.

20.2.4.3 T&A Application

The T&A application is an element of a larger automated payroll process. Consequently, it must play a role in protecting against payroll fraud.

The T&A application is designed to require that all T&A data submitted to the inter-agency mainframe be reviewed for accuracy by two distinct user *roles*: the *T&A Clerk* and the *T&A Supervisor*. The T&A application uses the LAN server's access control and identification and authentication (I&A) mechanisms to ensure that only authorized individuals can assume these roles. No individual is simultaneously authorized to act in both of these roles (i.e., have access to both sets of functions).

The T&A application ensures that only users with access to the T&A Clerk functions can enter T&A data and that only users with access to T&A Supervisor functions can approve and submit T&A data, or subsequent corrections thereof, to the mainframe.

Each T&A Supervisor is authorized to approve and submit T&A data for employees of specific departments. Supervisors are not authorized to approve their own T&A data.

The T&A application is supposed to be configured so that the Clerk and Supervisor functions can only be invoked from specific PCs attached to the LAN and only during normal working hours.

Administrators are not authorized to exercise functions of the T&A application apart from those concerned with configuring the accounts, passwords, and access permissions for Clerks and Supervisors. Administrators are expressly prohibited by policy from entering, modifying, or submitting T&A data via the T&A application or other mechanisms.[94]

20.2.4.4 Non-HGA Computer Systems

HGA relies on systems and components that it cannot control directly because they are owned by other organizations. HGA has developed policy to avoid undue risk in such situations. The policy states that system components controlled and operated by organizations other than HGA shall not be used to process, store, or transmit HGA information without explicit permission of the application owner and the COG Manager. Permission to use such system components is not be granted without written commitment from the controlling organization that HGA's information will be safeguarded commensurate with its value as designated by HGA. This policy is mitigated, somewhat, by the fact that HGA has issued an issue-specific policy on the use of Internet, which allows for its use for e-mail with outside organizations and access to other resources (but not for transmission of HGA non-public data).

20.3 Initiating the Risk Assessment

A recent change in the directorship of HGA has brought a new management team, including a *Chief Information Officer* (CIO), to HGA. Among the CIO's first actions was appointing a *Special Assistant For Computer Security* who immediately initiated a comprehensive risk analysis to assess the soundness of HGA's computer security program and its compliance with federal directives. This analysis drew upon prior risk assessments, threat studies, and applicable material internal control reports. The Special Assistant also established a time table for periodic reassessments.

The following three sections provide highlights from the assessment. This section examines the policies to which the system is subject. The next section addresses assets and threats. The assessment's analysis of vulnerabilities and safeguards is then discussed in section 6. For brevity, the details of the risk analysis are not included. The presentation focuses on the T&A application.

[94] Technically systems administrators may still have the ability to do so. This highlights the importance of adequate managerial reviews, auditing, and personnel background checks.

20.4 National and Agency General Policies

HGA has issued a *Computer Security Manual* that implements high level national policy. It synthesizes the requirements of many federal directives such as Appendix III to OMB Circular A-130, the Computer Security Act of 1987, and the Privacy Act. It also includes policy for automated financial systems, such as those based on OMB Circulars A-123 and A-127 as well as the Federal Managers' Financial Integrity Act.[95]

The HGA *Computer Security Manual* discusses many areas of policy and procedures to implement the various policies. Several examples of policy are discussed below. In addition, some of the policies that relate to the T&A application are included.

20.4.1 Payroll-related Policies

Since the T&A application is a component of a larger automated payroll process, many of its functional and security requirements have been derived from both governmentwide and HGA-specific policies related to payroll and leave. Elements of these policies include:

Validity of Inputs: Department supervisors are responsible for reviewing the correctness of the time sheets of the employees under their supervision and indicating their approval by initialing the time sheet. Supervisors are responsible for identifying and reporting significant irregularities and indications of fraud in such data prior to submission to the Payroll Office. In keeping with the principle of separation of duty, all data and corrections thereto that may affect pay, leave, retirement, or other benefits of an individual must be reviewed for validity by at least two authorized individuals (other than the affected individual).

Personnel Office Responsibilities: The Director of Personnel is responsible for ensuring that forms describing significant payroll-related personnel actions are provided to the Payroll Office at least one week prior to the payroll processing date for the first affected pay period; these actions include new hiring, terminations, transfers, leaves of absences and returns from such, and pay raises.

Payroll Office Responsibilities: The Manager of the Payroll Office is responsible for establishing and maintaining controls adequate to assure that the amounts of pay, leave, and other benefits reported on pay stubs and recorded in permanent records and those distributed electronically are accurate and consistent with T&A data, and other information provided by the Personnel Department. In particular, paychecks must never be provided to any individual who is not a bona fide, active-status HGA employee. Moreover, the pay of any employee who terminates employment, transfers, or goes on leave without pay must be suspended as of the effective date of such action; that is, extra paychecks or excess pay must not be dispersed.

[95] These policies, and others, are discussed in the Handbook's Introduction.

The Manager of the Payroll Office is responsible for establishing and maintaining controls and equipment adequate to ensure that paychecks are issued in a timely manner at the conclusion of each pay period. This may require maintaining alternate or redundant ADP equipment sufficient to assure continuity in the face of equipment malfunctions, electrical outages, and natural disasters. It is critical that paychecks be issued even if T&A input or other related information is not available on a timely basis. In the absence of such input, pay, leave, and other benefits shall be temporarily calculated based on information estimated from prior pay periods.

Personnel Information: HGA must personal information in accordance with the Privacy Act. Depending on the specific type of information, it should normally be accessible only to the individual concerned, the individual's supervisors, and personnel and payroll departments. Such information should also be timely and accurate.

20.4.2 Other Related Policies

Continuity of Operations: HGA's policies regarding continuity of operations are derived from requirements stated in OMB Circular A-130. HGA requires various organizations within it to develop contingency plans (CPs) and establish appropriate administrative and operational procedures to support them. The CPs must identify the facilities, equipment, supplies, procedures, and personnel needed to provide reasonable continuity of operations under a broad range of adverse circumstances. Each CP must be tested annually.

COG Contingency Planning: COG is responsible for developing and maintaining a CP encompassing the hardware and software components it manages and administers; these include the HGA PCs, the LAN, LAN server, router, printers, WAN interface, and associated operating systems and utilities. In the event of an emergency that takes some or all of these components out of service, COG may temporarily "ration" whatever computer services it can provide according to application priorities designated by HGA's upper management; these are identified in the plan.

COG's manager has responsibility for assessing adverse circumstances and providing recommendations to the Director of HGA. Based on these and other sources of input, the Director of HGA will determine whether circumstances are dire enough to merit activating various sets of procedures called forth in the COG CP.

Division Contingency Planning: HGA divisions also must develop and maintain their own CPs. The head of each division is responsible for ensuring that the division's CP and associated support activities are adequate. The CP must identify critical business functions and the system resources and applications on which they depend. It must also identify the maximum acceptable periods of interruption that can be tolerated for these functions without significant reduction in HGA's ability to fulfill its mission.

For each major application used by multiple divisions, chief of a single division must be designated as the *application owner*. The designated official (supported by their staff) is responsible for addressing that application in their CP, and for coordinating with other divisions that use the application.

If a division relies exclusively on computer resources maintained by COG (e.g., the LAN), it need not duplicate COG's contingency planning, but is responsible for reviewing the adequacy of the COG CP. If COG's CP does not adequately address the division's needs, the division must contact the COG Director with its concerns. In either situation, the division must make known the criticality of its applications to the COG. If the division relies on computer resources or services that are *not* provided by COG, the division is responsible for: (1) developing its own CP, or (2) for ensuring that the CPs of other organizations (e.g., the WAN service provider) provide adequate protection from service disruptions.

Backups: HGA's policies also stipulate that accidental deletion must not result in permanent loss of data more than one day old. Moreover, these policies stipulate that every computer system or component containing significant data must be backed up on a regular and frequent basis.

20.5 Assets and Threats

After examining the basic policies (that HGA was aware of) and implementing national and agency policy, the risk assessment looked at assets and threats.

20.5.1 Assets

HGA information systems comprise and are intertwined with several different kinds of assets valuable enough to merit protection. HGA systems play a key role in transferring U.S. Government funds to individuals in the form of paychecks; hence financial resources are among the assets associated with HGA systems. A variety of other assets are also involved. These include personnel information, contracting and procurement documents, draft regulations, internal correspondence, and a variety of other day-to-day business documents, memos, and reports. The system components owned and operated by HGA are also assets. Since the WAN and mainframe are owned and operated by other organizations, they will not be treated as HGA assets. Their contribution to the threat and vulnerability picture for other HGA assets however, will be considered. HGA personnel, buildings, and facilities *are also assets*, but were considered outside the scope of this risk analysis.[96]

HGA's assets include intangible elements as well. The reputation of the agency is a highly valued asset, as is the confidence of its employees that personal information will be handled properly and that correct wages will be paid on time.

[96] Note that these may be essential assets, but are excluded from this limited review.

20.5.2 Threats

Different HGA assets are subject to different kinds of threats. Some threats are considered less likely than others, and the potential impact of different threats may vary greatly. Threat likelihoods are generally difficult to estimate accurately. Both HGA and the risk assessment's authors have attempted to the extent possible to base these estimates on historical data, but have also tried to anticipate new trends stimulated by emerging technologies (e.g., external networks).

As for most large organizations that control financial assets, attempts at fraud and embezzlement are likely to occur. In fact, HGA has a history of such attempts related to the payroll process. Although many of these attempts have been caught, and some involved relatively small sums of money, HGA considers preventing financial fraud to be a *critical* computer security priority, particularly in light of the potential for damage to its reputation with Congress, the public, and other federal agencies.

20.5.2.1 Payroll Fraud

Historically, attempts at fraud have almost always come from within HGA or the other agencies that operate systems on which HGA depends. There have been few attempts by individuals outside these organization, though the rapid growth of the Internet and improved connectivity from it to HGA's LAN may increase the likelihood of outsider attacks.

Attempts to defraud HGA have included the following:

- Submitting fraudulent time sheets for hours or days not worked, or for pay periods following termination or transfer of employment. The former may take the form of falsely reporting overtime hours, or failing to report vacation hours. Alternatively, attempts have been made to modify time sheet data after it has been entered and approved for submission to payroll.

- Falsifying or modifying dates or data on which one's "years of service" computations are based, thereby becoming eligible for retirement earlier than allowed, or increasing one's pension amount.

- Creating employee records and time sheets for fictitious personnel, and attempting to obtain their paychecks, particularly after arranging for direct deposit.

If successful, some of these threats could lead to financial losses and significant damage to HGA's reputation.

20.5.2.2 Payroll Errors

Of greater likelihood, but of perhaps lesser potential impact on HGA, are errors in T&A data entry, or failure to enter information describing new employees, terminations, and transfers in a timely manner. Errors of these kinds can cause financial difficulties for employees and accounting problems for HGA. If an employee's vacation or sick leave balance became negative erroneously during the last pay period of the year, the employee's last paycheck would be automatically reduced. An individual who transfers between HGA and another agency may risk receiving duplicate paychecks or no paychecks for the pay periods immediately following the transfer. Errors of this sort that occur near the end of the year can lead to errors in W-2 forms and subsequent difficulties with the tax collection agencies.

20.5.2.3 Continuity of Operations

HGA's building facilities and physical plant are several decades old and are frequently under repair or renovation. As a result, power, air conditioning, and LAN or WAN connectivity for the server are typically interrupted several times a year for periods of up to one work day. For example, on several occasions, construction workers have inadvertently severed power or network cables. Such interruptions, depending upon when they occur, can prevent T&A data from getting processed and transferred to the mainframe before the payroll processing deadline. Another threat of small likelihood, but significant potential impact is that of a malicious or disgruntled employee seeking to disrupt time-critical processing (e.g., payroll) by deleting necessary inputs or system accounts, misconfiguring access controls, or sabotaging ADP-related equipment.

20.5.2.4 Information Disclosure / Brokering

Other kinds of threats may be stimulated by the growing market for information about an organization's employees or internal activities. Individuals who have legitimate work-related reasons for access to the master employee database, may attempt to sell such information to private investigators, employment recruiters, the press, or other organizations. HGA considers such threats to be moderately likely and of low to high potential impact depending on the type of information that is involved.

20.5.2.5 Other Threats

HGA's systems also are exposed to a number of other threats which, for reasons of space, cannot be completely enumerated here. Examples of threats and HGA's assessment of their probability and impact include the following:

- *Accidental Loss/Release of Disclosure-sensitive Information* - Overall, this threat was judged by HGA as medium probability, low impact.[97]

---

[97] Note that these are generalizations of judgements made by HGA. The consequences of the disclosure of some information are more severe than others.

- *Accidental Destruction of Information* - The threat of accidental deletion of day-to-day working papers and files kept on PC local hard disks is a high probability, low impact threat.

- *Loss of Information Due To Virus Contamination* - This threat is judged medium probability, medium impact.

- *Misappropriation of Systems* - Employees and contractors are not authorized to use HGA computers for non-Government business. There is a moderate probability that some individuals will abuse these privileges, for example by using HGA facilities to develop software or offer computing services (e.g., tax preparation) for sale. HGA considers this a low impact threat.

- *Unauthorized access to Telecommunications Resources* - HGA operates a PBX system, which may be vulnerable to hacking to 1) disrupt PBX availability agency operations, 2) gain access to outgoing phone lines for long-distance services, 3) gain access to stored voice mail messages and 4) gain surreptitious access to otherwise private conversations/data transmissions. HGA considers this a low probability, medium impact event.

20.6 Safeguards, Vulnerabilities, and Risk Mitigation

Section 4 described an early phase of a recent risk assessment. That phase identified HGA assets and a variety of potential threats against them. This section presents selected aspects of another part of the risk assessment, namely, the examination of *current* HGA safeguards and vulnerabilities, and recommendations for reducing risks. HGA management's responses to the risk assessment will also be described, including risk mitigation actions taken and their supporting rationale.

This section presents a collection of examples illustrating concepts described in more detail in earlier Handbook chapters. It is not a complete or comprehensive security analysis. Nor are the controls described intended to comprise a self-sufficient set of security solutions.

Five numbered subsections are presented. Each focuses on a primary HGA risk category (described previously). These subsections are:

1. Payroll Fraud;
2. Payroll Errors;
3. Continuity of Operations;
4. Information Disclosure; and
5. Network-Related Threats.

The discussion of each risk area includes three parts: a review of principal threat sources, risk assessment results, and HGA risk mitigation actions.

The discussions in these subsections were chosen to illustrate a *broad sampling*[98] of handbook topics. Risk Management and Security Program Management themes are integral throughout, with particular emphasis given to risk-driven safeguard selection. As illustrated below, many of the risks to which HGA is exposed stem from: (1) the failure of individuals to comply with established policies and procedures, or (2) use of automated mechanisms whose assurance is questionable because of the ways they have been developed, tested, implemented, used, or maintained.

20.6.1 Payroll Fraud

As described previously, payroll-related fraud is regarded by HGA as a principal source of risks to its financial assets, reputation, and employee confidence. Specific threats include:

- *Falsified Time Sheets* - When submitting time sheets, individuals might intentionally underreport their own leave or over-report "compensatory" time or overtime. Alternatively, an individual might attempt to submit bogus time sheets for pay periods that follow termination or transfer.

- *Unauthorized Execution of the T&A Application* - An unauthorized individual may attempt to execute the T&A application from an HGA PC for the purpose of entering, approving, or submitting fraudulent T&A data, or corrections thereof, to the mainframe. Means of attacks may include impersonating a Clerk or Supervisor by defeating I&A mechanisms or defeating the server's access controls which are supposed to prevent users from gaining access to Clerk or Supervisor functions (and executing the T&A program).

- *Execution of a Bogus T&A Application* - An individual could develop and execute a program on a PC or the server that imitates the T&A program, but sends bogus T&A data to the mainframe.

- *Unauthorized Modification of T&A Data* - An HGA PC user might be able to intercept T&A data and modify it enroute to the payroll application on the mainframe. Opportunities include tampering with incomplete T&A input files while stored on the server, interception and tampering during WAN transit, or tampering on arrival to the mainframe prior to processing by the payroll application.

A number of similar threats might also originate from outsiders who attempt to access the HGA server and LAN via the Internet or WAN. Network-based threats are treated briefly in a later section.

---

[98] Some of the controls, such as auditing and access controls, play an important role in many areas. The limited nature of this example, however, prevents a broader discussion.

20.6.1.1 Current Safeguards and Vulnerabilities

HGA has incorporated a variety of safeguards to reduce payroll fraud risks. These are discussed below.

Falsified Time Sheets - The primary safeguard against falsified time sheets is review and approval by supervisory personnel, who are not permitted to approve their own T&A data. The risk assessment has concluded that this safeguard, while imperfect, is adequate. The related requirement that two different individuals (a Clerk and a Supervisor) must cooperate closely in creation and submission of T&A data to the mainframe also safeguards against other kinds of illicit manipulation of T&A data by Clerks or Supervisors acting independently.

Unauthorized Execution - Protection against unauthorized execution of the T&A application depends on I&A and access controls. While the T&A application is accessible from any PC, unlike most programs run by PC users, it does not execute directly on the PC's processor. Instead, it executes on the server while the PC behaves as a terminal, relaying the user's keystrokes to the server and displaying text and graphics sent from the server.

The reason for this approach is that common PC operating systems do not provide authentication and access controls, and therefore cannot protect against unauthorized T&A program execution. *Any* individual who has access to the PC could potentially run any program stored there. Another possible approach is for the T&A program to perform I&A and access control on its own by requesting and validating a password before beginning each T&A session. This approach, however, can be defeated easily by a moderately skilled programming attack, and was judged inadequate by HGA during the application's early design phase.

Recall that the server is a more powerful computer equipped with a multi-user operating system that includes password-based I&A and access controls. Designing the T&A application program so that it executes on the server under the control of the server's operating system provides a more effective safeguard against unauthorized execution than executing it on the user's PC.

Nevertheless, vulnerabilities still remain. The risk assessment pointed out that when a PC user enters a password to the server during I&A, the password is sent to the server by broadcasting it over the LAN "in the clear." This allows the password to be intercepted easily by any other PC connected to the LAN. In fact, so-called "password sniffer" programs that capture passwords in this way are widely available. The risk assessment similarly pointed out that a malicious program planted on a PC could also intercept passwords before transmitting them to the server. An unauthorized individual who obtained the captured passwords could then run the T&A application in place of a Clerk or Supervisor. Users might also store passwords in a logon script file.

To remove these vulnerabilities, the risk assessment recommended[99] the use of stronger authentication mechanisms based on smart tokens to generate one-time passwords. Such passwords cannot be used by an interloper for subsequent sessions.

Bogus T&A Applications - Protection against bogus T&A applications that run on the server is provided by the server's access controls. The server's controls have been configured so that the WAN interface device used to communicate with the mainframe is (theoretically, of course, since there may be other bypass mechanisms) only accessible to programs that possess a special access control privilege; only the system administrator has been granted access to assign this privilege to server programs. As a result, the server's operating system is designed to prevent a bogus T&A application created by any other user from communicating with the WAN and, hence, with the mainframe.

The risk assessment revealed that the server's access controls are probably adequate for this purpose, but cautioned that the server's operating system and access controls are relatively immature; they have only been in wide-spread use for a few years, and have been found to contain a number of security-related bugs during that time. The risk assessment cautioned that the server's access controls are ineffective unless properly configured and that the administration of the server's security features in the past has been notably lax. The assessment recommended improving the server administrative procedures and the speed with which security-related bug fixes distributed by the vendor are installed on the server.

Unauthorized Modification - Protection against unauthorized modification of T&A data requires a variety of safeguards because each system component on which the data is stored or transmitted is a potential source of vulnerabilities.

First, T&A data is entered on the server by a Clerk. On occasion, the Clerk might begin data entry late in the afternoon, and complete it the following morning, storing it in a temporary file between the two sessions. One way to avoid unauthorized modification is to store the data on a diskette and lock it up overnight. After the data has been entered, it will be stored in another temporary file until it has been reviewed and approved by a Supervisor. These files, now stored on the system, must be protected against tampering. As before, the server's access controls, if reliable and properly configured, can provide such protection (as can digital signatures, as discussed later) in conjunction with proper auditing.

Second, when the Supervisor approves a batch of T&A data, the T&A application sends it over the WAN to the mainframe. The WAN is a collection of communications equipment and special purpose computers called switches that act as relays, routing information through the network from source to destination. Each switch is a potential site at which the T&A data might be fraudulently modified.

---

[99] Note that, for the sake of brevity, the process of evaluating the cost-effectiveness of various security controls is not specifically discussed.

Third, on arrival at the mainframe, the T&A data is held in temporary file on the mainframe until the payroll application is run. Consequently, the mainframe's I&A and access controls must provide a critical element of protection against unauthorized modification of T&A data.

According to the risk assessment, the server's access controls, with prior caveats, probably provide acceptable protection against unauthorized modification of data stored on the server. The assessment concluded that a WAN-based attack involving collusion between an HGA employee and an employee of the WAN service provider, although unlikely, should not be dismissed entirely, especially since HGA has only cursory information about the service provider's personnel security practices and no contractual authority over the manner in which it operates the WAN.

The greatest source of vulnerabilities, however, is the mainframe. Although its operating system's access controls are mature and powerful, it uses password-based I&A. This is of particular concern because it serves a large number of federal agencies via WAN connections. A number of these agencies are known to have poor security programs. As a result, one such agency's systems could be penetrated (e.g., from the Internet) and then used in attacks on the mainframe via the WAN. In fact, to such an attack, T&A data awaiting processing on the mainframe would probably not be as attractive a target as other kinds of data or, indeed, disabling the system, rendering it unavailable. For example, if an attacker could modify the employee data base, it might be possible to cause paychecks or pensions checks to be disbursed to fictitious employees. Disclosure-sensitive law enforcement databases might also be attractive targets.

The access control on the mainframe is strong and provides good protection against an intruder breaking into a second application after they have broken into a first. However, previous audits have shown that the difficulties of system administration may present some opportunities for intruders to defeat access controls.

The risk assessment authors strongly advocated that the mainframe site begin requiring authentication via one-time password tokens for all WAN-based accesses. Such authentication techniques would make it very difficult for outsiders (e.g., from the Internet) who penetrate systems on the WAN to use them to attack the mainframe. The authors noted, however, that the mainframe serves many different agencies. Thus, the cost and procedural difficulty of implementing such controls would be substantial. They also noted that HGA has no authority over the way the mainframe is configured and operated.

20.6.1.2 Risk Mitigation

After input from COG security specialists and application owners, HGA's management accepted most of the risk assessment's recommendations. HGA management decided that residual risks due to falsification of time sheets were acceptably low; no changes in procedures were deemed necessary. The risks of payroll fraud due to the interceptability of LAN server passwords, however, were judged unacceptable, and COG was directed to investigate costs and procedures associated with using one time passwords for T&A Clerks and Supervisor sessions on the server. Other users performing less sensitive tasks on the LAN would continue to use password-based authentication.

While the immaturity of the LAN server's access controls was judged a significant source of risk, COG was only able to identify one other PC LAN product that would be significantly better in this respect. Unfortunately, this product was considerably less friendly to users and application developers, and incompatible with other applications used by HGA. The negative impact of changing PC LAN products was judged too high for the potential increment in security benefits. Consequently, HGA decided to accept the risks accompanying use of the current product, but directed the COG to improve its monitoring of the server's access control configuration and its responsiveness to vendor security reports and bug fixes.

HGA concurred that risks of fraud due to unauthorized modification of T&A data at or in transit to the mainframe should not be accepted unless no practical solutions could be identified. After discussions with the mainframe's owning agency, HGA concluded that the owning agency was unlikely to adopt the advanced authentication techniques advocated in the risk assessment. COG, however, proposed an alternative approach that did not require a major resource commitment on the part of the mainframe owner.

The alternative approach would employ digital signatures based on public key cryptographic techniques to detect unauthorized modification of T&A data. The data would be *digitally signed* by the Supervisor using a private key prior to transmission to the mainframe. When the payroll application program was run on the mainframe, it would use the corresponding public key to validate the correspondence between the T&A data and the signature. Any modification of the data during transmission over the WAN or while in temporary storage at the mainframe would result in a mismatch between the signature and the data. If the payroll application detected a mismatch, it would reject the data; HGA personnel would then be notified and asked to review, sign, and send the data again. If the data and signature matched, the payroll application would process the T&A data normally.

HGA's decision to use advanced authentication for T&A Clerks and Supervisors can be combined with digital signatures by using smart tokens. Smart tokens are programmable devices so they can be loaded with private keys and instructions for computing digital signatures without burdening the user. When a Supervisor approves a batch of T&A data, the T&A application on the server would instruct the Supervisor to insert their token in the token reader/writer device attached to the Supervisor's PC. The application would then send a special "hash" (summary) of the T&A data to the token via the PC. The token would generate a digital signature using its embedded secret key, and then transfer the signature back to the server, again via the PC. The T&A application running on the server would append the signature to the data before sending the data to the mainframe, and ultimately, the payroll application.

Although this approach did not address the broader problems posed by the mainframe's I&A

vulnerabilities, it does provide a reliable means of detecting T&A data tampering. In addition, it protects against bogus T&A submissions from systems connected to the WAN because individuals who lack a T&A Supervisor's smart token will be unable to generate valid signatures. (Note, however, that the use of digital signatures does require increased administration, particularly in the area of key management.) In summary, digital signatures mitigate risks from a number of different kinds of threats.

HGA's management concluded that digitally signing T&A data was a practical, cost-effective way of mitigating risks, and directed COG to pursue its implementation. (They also noted that it would be useful as the agency moved to use of digital signatures in other applications.) This is an example of developing and providing a solution in an environment over which not single entity has authority.

20.6.2 Payroll Errors

The previous section discussed some of the vulnerabilities, safeguards, and risk mitigation decisions associated with preventing payroll fraud. This section considers prevention of errors in T&A data, another important source of risks to HGA financial assets, its reputation, and employee confidence, as described in Section 4.2.2.

Sources of payroll errors include the following:

- T&A data entry errors;
- Failure to submit or process personnel status changes, e.g., initiation or termination of employment, in a timely manner;
- Inter-agency coordination errors in processing personnel transfers; and
- Accidental corruption or loss of T&A data.

20.6.2.1 Current Safeguards and Vulnerabilities

To protect against these sources of errors, HGA uses a combination of human procedures and automated mechanisms.

Data Entry Errors - Data entry errors in previous T&A applications have long plagued HGA. The frequency of data entry errors is reduced by having T&A Clerks enter each time sheet into the T&A application twice. The two copies are then compared. If they are identical, both are considered error free, and the first copy is accepted for subsequent review and approval by a Supervisor. If the copies are not identical, the discrepancies are displayed and for each discrepancy, the Clerk determines which copy is correct. Corrections are then incorporated into one of the copies, which is then accepted for further processing. If the Clerk makes the same data entry error twice, then the two copies will match and one will be accepted as correct even though it is erroneous. To reduce this risk, the T&A application could have been configured to require that the two copies be entered by different Clerks.

The T&A application further reduces opportunities for data entry errors by forcing a Supervisor to approve the data before it is sent to the mainframe. In addition, the data is subjected to a collection of "sanity checks" to detect entries whose values are outside expected ranges. Potential anomalies are displayed to the Supervisor prior to allowing approval; if errors are identified, the data is returned to a Clerk for additional examination and corrections.

After reviewing the risk assessment, management concluded that these safeguards provide satisfactory protection against data entry errors.

Paperwork Submission and Coordination - Ensuring timely submission and inter-agency coordination of paperwork associated with personnel status changes requires appropriate personnel department procedures. Although HGA management has established procedures for this purpose, an unacceptably large number of troublesome payroll errors during the past several years has been traced to late submission of personnel paperwork. The risk assessment reviewed HGA's procedures and found them adequate, but criticized HGA management for not providing sufficient incentives for compliance. The assessment recommended establishing compliance audits and appropriate penalties for non-compliance.

Accidental Corruption - Protection against accidental corruption of T&A data is provided by the same mechanisms used to protect against fraudulent modification, namely the access control features of the server and mainframe operating systems.

Protection against loss of T&A data is provided by COG's nightly backups of the server's disks. To a limited extent, HGA also relies on mainframe administrative personnel to back up T&A data while it is stored on the mainframe, even though it has no direct control over these individuals. As additional protection against loss of data at the mainframe, HGA retains copies of all T&A data on-line on the server for at least one year, at which time the data is archived and kept for three years. The server's access controls for the on-line files are automatically set to read-only access by the T&A application at the time of submission to the mainframe. Protection of the integrity of T&A data will be provided by digital signatures as they are implemented.

The WAN's communications protocols also provide protection against loss of data during transmission from the server to the mainframe (e.g., error checking). In addition, the mainframe payroll application includes a program that is automatically run 24 hours before paychecks and pay stubs are printed. This program produces a report identifying agencies from whom T&A data for the current pay period was expected, but has not been received. Payroll department staff are responsible for reviewing the reports and immediately notifying agencies that need to submit or resubmit T&A data.

The risk assessment concluded that HGA's safeguards (with the stipulated improvements) against accidental corruption and loss of T&A data were adequate.

20.6.2.2 Risk Mitigation

HGA's management concurred with the risk assessment, and tasked the Director of Personnel to ensure greater compliance with paperwork handling procedures and provide quarterly compliance audit reports. HGA's management noted that the digital signature mechanism it plans to use for fraud protection can also provide protection against payroll errors due to accidental corruption.

20.6.3 Continuity of Operations

This section considers some of the safeguards and vulnerabilities associated with assuring continuity of HGA operations.

Threats against continuity of operations include the following:

- Loss of power, air conditioning, or network connectivity caused by physical plant failures, or renovation/ construction activities;

- Fires, floods, storms, and other natural disasters;

- Equipment malfunctions;

- Malicious acts by a disgruntled employee, or contractor;

- Malicious acts by outsiders including the planting of computer viruses and attempts to penetrate HGA systems;

- Accidental corruption or loss of data; and

- Theft of equipment, media, peripherals, etc.

20.6.3.1 Current Safeguards and Vulnerabilities

HGA's protection against these threats relies on a combination of plans, procedures, redundant or alternative equipment and facilities, and automated mechanisms.

Physical Plant, Disasters, Malfunctions - The CP developed by the COG sets forth the procedures and facilities that are to be utilized in the event that physical plant failures, natural disasters, or major equipment malfunctions occur sufficient to prevent normal use of HGA's PCs, LAN, server, printers, and other associated equipment.

The plan prioritizes applications that rely on these resources, indicating those that should be suspended if available automated functions or capacities are temporarily degraded. In accordance with the plan, COG personnel have identified system software and hardware components that are compatible with those used by other nearby agencies so that these agencies could support essential HGA system-based operations for periods of a few days in an emergency. HGA has signed an agreement with two other agencies that commit each to reserving spare computational and storage capacities for the others for this purpose.

To prevent more limited computer equipment malfunctions from interrupting routine business operations, COG maintains an inventory of approximately ten fully equipped spare PC's, a spare LAN server, and several spare disk drives for the server. COG also keeps thousands of feet of LAN cable on hand. In the event that a segment of the LAN cable that runs through ceilings and walls of HGA's buildings fails or is accidentally severed, COG technicians will run temporary LAN cabling along the floors of hallways and offices, typically restoring service within a few hours for as long as needed until the cable failure is located and repaired.

The risk assessment commended HGA for many aspects of COG's CP, but pointed out that many COG personnel were completely unaware of the responsibilities assigned to them by it. The assessment recommended that the COG institute a program of periodic internal training and awareness sessions for COG personnel having CP responsibilities.

The assessment noted that although HGA policies require annual testing of CPs, the capability to resume HGA computer processing activities at another cooperating agency has never been verified, and might turn out to be illusory. The assessment urged that COG undertake a rehearsal during the next three months in which selected parts of the plan would be exercised. The rehearsal should include attempting to initiate some aspect of processing activities at one of the designated alternative sites.

The risk assessment reviewed a number of the (both T&A and non-T&A) application-oriented CPs developed by HGA divisions. Most were cursory and attempted to delegate nearly all CP responsibility to COG. The assessment criticized several of these for failing to address potential disruptions caused by lack of access to: (1) computer resources not managed by COG, and (2) non-system resources such as buildings, phones, and other facilities. In particular, the CP encompassing the T&A application was criticized for not addressing disruptions caused by WAN and mainframe outages.

Malicious Acts - HGA's protection against malicious acts by disgruntled employees relies on physical security (to prevent sabotage) and on many of the automated mechanisms used to prevent unauthorized or accidental modification of information.

HGA's protection against PC virus contamination is based on policy and procedures that prohibit PC users from installing software on their PCs or on the server. These state that only System Administrators are authorized to install software, and only the software on the

COG approved list. Only the Manager of COG has authority to add packages to the approved list. COG procedures also stipulate that administrative personnel should execute virus scanning programs on the server and, on a spot-check basis, on a number of PCs each month. If a virus is found, COG personnel are responsible for immediately notifying the team for Computer Incident Handling.

The risk assessment found HGA's virus prevention policy and procedures to be sound, but noted that there was little evidence that they were being followed. In particular, no COG personnel interviewed had ever run a virus scanner on a PC on a routine basis, though several had run them during publicized virus scares. The assessment cited this as a significant risk item.

Accidental Corruption - HGA's protection against accidental corruption or loss of data is based largely on making regular backup copies of on-line data and storing the copies in a secure storage facility at a sister agency. In compliance with HGA policy, COG personnel backup the LAN server's disks onto magnetic tape every night and transport the tapes to the sister agency weekly. HGA's policies also stipulate that all PC users are responsible for backing up any significant data stored on their PC's local hard disks daily. For the past several years, COG has issued a yearly memorandum reminding PC users of their responsibilities in this regard. It also strongly encourages them to store significant data on the LAN server instead of on their PC's hard disk so that such data will be backed up automatically during COG's LAN server backups.

The risk assessment concluded that HGA's safeguards against accidental corruption and loss of *T&A data* were adequate, but that safeguards for some other kinds of data were not. The assessment included an informal audit of a dozen randomly chosen PCs and PC users in the agency. It concluded that many PC users store significant data on their PC's hard disks, but do not back them up. Based on anecdotes, the assessment's authors stated that there appear to have been many past incidents of loss of information stored on PC hard disks and predicted that such losses would continue.

20.6.3.2 Risk Mitigation

HGA's management agreed that additional Contingency Plan training was needed for COG personnel and committed itself to its first plan rehearsal within three months. After a short investigation, the HGA divisions owning applications that depend on the WAN concluded that WAN outages, although inconvenient, would not have major impact on HGA. This is because the few time-sensitive applications that required WAN-based communication with the mainframe were originally designed to work with magnetic tape instead of the WAN, and could still operate in that mode; hence courier-delivered magnetic tapes could be used as an alternative input medium in case of a WAN outage. The divisions responsible for contingency planning for these applications agreed to incorporate into their CPs both descriptions of these procedures and other improvements.

With respect to mainframe outages, HGA determined that it could not easily make arrangements for a suitable alternative site. HGA also obtained and examined a copy of the mainframe facility's own contingency plan. After detailed study, including review by an outside consultant hired by HGA, HGA concluded that the plan had major deficiencies and posed significant risks for HGA because of HGA's reliance on it for payroll and other services. This was brought to the attention of the Director of HGA, who, in a formal memorandum to the head of the mainframe's owning agency, called for: (1) a high-level inter-agency review of the plan by all agencies that rely on the mainframe, and (2) corrective action to remedy any deficiencies found.

HGA's management agreed to improve adherence to its virus prevention procedures. It agreed (from the point of view of the entire agency) that accidental loss of information stored on PC hard disks occurs frequently. It estimated, however, that the labor hours lost as a result would amount to less than a person year -- which HGA management does *not* consider to be unacceptable. After reviewing options for reducing this risk, HGA concluded that it would be cheaper to accept the associated loss than to commit significant resources in an attempt to avoid it. COG volunteered, however, to set up an automated program on the LAN server that e-mails backup reminders to all PC users once each quarter. In addition, COG agreed to provide regular backup services for about 5% of HGA's PCs; these will be chosen by HGA management based on the information stored on their hard disks.

20.6.4 Information Disclosure / Brokering

This section discusses safeguards, vulnerabilities, and risk mitigation decisions concerning threats associated with information disclosure.

As noted in an earlier section, HGA is concerned about unauthorized disclosure of information. This includes both disclosure to insiders (employees and contractors) and to outsiders, such as information brokers. Elements of the T&A datafiles are protected by the Privacy Act. In addition, HGA takes a conservative approach toward protecting information about its employees. Since information brokerage is more likely to be a threat to large collections of data, the HGA risk assessment focused primarily, but not exclusively, upon protection of the mainframe.

20.6.4.1 Current Safeguards and Vulnerabilities

HGA's protection against information disclosure is based on a need to know policy, and personnel hiring and screening practices. The need to know policy states that T&A information should be made accessible only to HGA employees and contractors whose assigned professional responsibilities require it; T&A information must be protected against access from all other individuals, including other HGA employees. Appropriate hiring and screening practices can lessen the risk that an untrustworthy individual will be assigned such responsibilities.

The need to know policy is supported by a collection of physical, procedural, and automated safeguards, including the following:

- T&A paper documents are supposed to be stored securely when not in use, particularly during evenings and on weekends. Approved storage containers include locked file cabinets and desk drawers -- to which only the owner has the keys. While storage in a container is preferable, it is also permissible to leave T&A documents on top of a desk or other exposed surface in a locked office (with the realization that the guard force has keys to the office). (This is a judgement left to local discretion.) Similar rules apply to disclosure- sensitive information stored on floppy disks and other removable magnetic media.

- Every HGA PC is equipped with a key lock that, when locked, disables the PC. When information is stored on a PC's local hard disk, the user to whom that PC was assigned is expected to (1) lock the PC at the conclusion of each work day and (2) lock the office in which the PC is located.

- The LAN server operating system's access controls provide extensive features for controlling access to files. These include group oriented controls that allow teams of users to be assigned to named groups by the System Administrator. Group members are then allowed access to sensitive files not accessible to non-members. Each user can be assigned to several groups according to need to know. (The reliable functioning of these controls is assumed, perhaps incorrectly, by HGA.)

- All PC users undergo security awareness training when first provided accounts on the LAN server. Among other things, the training stresses the necessity of protecting passwords. It also instructs users to log off the server before going home at night or before leaving the PC unattended for periods exceeding an hour.

The risk assessment examined HGA's use of these and other safeguards and concluded that significant, avoidable information brokering vulnerabilities were present -- particularly due to HGA's lack of compliance with its own policies and procedures. It found that T&A documents were typically not stored securely after hours and that few PCs containing T&A information were routinely locked. Worse yet, few were routinely powered down, and many were left logged in to the LAN server overnight. These practices make it easy for an HGA employee wandering the halls after hours to browse or copy T&A information on another employee's desk, PC hard disk, or LAN server directories.

The assessment recommended that HGA improve its security awareness training (e.g., via mandatory refresher courses) and that it institute some form of compliance audits. The training should be sure to stress the penalties for non-compliance. It also suggested installing "screen lock" software on PCs. Such packages will automatically lock a PC after a specified period of idle time in which no keystrokes have been entered; unlocking the screen requires that the user enter a password or reboot the system.

The risk assessment pointed out that information sent to or retrieved from the server is subject to eavesdropping by other PCs on the LAN. The LAN hardware transmits information by broadcasting it to all connection points on the LAN cable. Moreover, information sent to or retrieved from the server is transmitted in the clear, that is, without encryption. Given the widespread availability of LAN sniffer programs, LAN eavesdropping is trivial for a prospective information broker, and hence likely to occur. The assessment recommended that HGA modify its information handling policies so that employees would be required to store some kinds of disclosure-sensitive information only on PC local hard disks (or floppies), but not on the server; this would eliminate or reduce risks of LAN eavesdropping. It was also recommended that and an activity be installed log on the server (and regularly reviewed). Moreover, it would avoid unnecessary reliance on the server's access control features which are of uncertain assurance. The assessment noted, however, that this strategy conflicts with the desire to store most information on the server's disks so that it is backed up routinely by COG personnel. (This could be offset by assigning responsible for some one other than the PC owner to make backup copies.) Since the security habits of HGA PC users have generally been poor, the assessment also recommended use of hard-disk encryption utilities to protect disclosure-sensitive information on unattended PCs from browsing by unauthorized individuals. Also, ways to encrypt information on the server's disks would be studied.

Last, the assessment noted that HGA's employee master database is stored on the mainframe where it might be a target for information brokering by employees of the agency that owns the mainframe. It might also be a target for information brokering, fraudulent modification, or other illicit acts by any outsider who penetrates the mainframe via another host on the WAN. The assessment recommended that HGA conduct a thorough review of the mainframe's safeguards in these respects, and that it regularly review the mainframe audit log, using a query package, with particular attention to records that describe user accesses to the HGA employee master database.

20.6.4.2 Risk Mitigation

HGA concurred with the risk assessment's conclusions about its information brokering risk exposure, and adopted most of the associated recommendations.

20.6.5 Network-Related Threats

Most of the human threats of concern to HGA originate from insiders. Nevertheless, HGA also recognizes the need to protect its assets from outsiders. This section provides a brief discussion of some of safeguards, vulnerabilities, and risk mitigation decisions concerning outsider attacks that originate from external networks.

Such attacks may serve many different purposes and pose a broad spectrum of risks, including unauthorized disclosure or modification of information, unauthorized use of services and assets, or unauthorized denial of services. As shown in Figure 1, HGA systems are connected to the three external networks: (a) the Internet, (b) the Inter-agency WAN, and (c) the public switched (telephone) network. Although these networks are a source of security risks, connectivity with them is essential to HGA's mission and the productivity of its employees; connectivity cannot be terminated simply because of security risks.

In each of the past few years prior to establishing its current set of network safeguards, HGA had detected several attempts by outsiders to penetrate its systems. Most, but not all of these, have come from the Internet, and those that succeeded did so by learning or guessing user account passwords. In two cases, the attacker deleted or corrupted significant amounts of data, most of which was later restored from backup files. In most cases, HGA could detect no ill effects of the attack, but concluded that the attacker may have browsed some files. HGA also conceded that its systems did not have audit logging capabilities sufficient to track an attacker's activities. Hence, for most of these attacks, HGA could not accurately gauge the extent of penetration.

In one case, an attacker succeeded in acquiring System Administrator privileges on the server, a significant breach. HGA found no evidence that the attacker attempted to exploit these privileges before being discovered two days later. The attack made use of a bug in an e-mail utility. When the attack was detected, COG immediately contacted the Agency Incident Handling Team, and was told that a bug fix had been distributed by the server vendor several months earlier. To its embarrassment, COG discovered that it had already received the fix, which it then promptly installed. It now believes that no subsequent attacks of the same nature have succeeded.

Although HGA has no evidence that it has been significantly harmed to date by attacks via external networks, it believes that these attacks have great potential to inflict damage. HGA management considers itself lucky that such attacks have not harmed HGA's reputation and the confidence of the citizens its serves. It also believes the likelihood of such attacks via external networks will increase in the future.

20.6.5.1 Current Safeguards and Vulnerabilities

HGA's current set of network safeguards has only been in place for a few months. These safeguards have been specifically configured to reduce risks from the kinds of external network threats that HGA has detected in the past. The basic approach is to tightly restrict the kinds of external network interactions that can occur. This is accomplished by funneling all traffic to and from external networks through two interfaces that provide access control by filtering out unauthorized kinds of interactions. As indicated in Figure 1, the two interfaces are the network router and the LAN server. The only kinds of interactions that these interfaces allow are: (a) e-mail and (b) data transfers from the server to the mainframe controlled by a few special applications (e.g., the T&A application).

Figure 1 shows that the network router is the only direct interface between the LAN and the Internet. The router is a dedicated special purpose computer that translates between the protocols and addresses associated with the LAN and the Internet. Internet protocols, unlike those used on the WAN, specify that packets of information coming from or going to the Internet must carry an indicator of the kind of service that is being requested or used to process the information. This makes it possible for the router to distinguish e-mail packets from other kinds of packets, for example, those associated with a remote login request.[100] The router has been configured by COG to discard all packets coming from or going to the Internet except those associated with e-mail. COG personnel believe that the router effectively eliminates Internet based attacks on HGA user accounts because it disallows all remote login sessions, even those accompanied by a legitimate password.

The LAN server enforces a similar type of restriction for dial-in access via the public switched network. The access controls provided by the server's operating system have been configured so that during dial-in sessions, only the e-mail utility can be executed. (HGA policy, enforced by periodic checks, prohibits installation of modems on PCs, so that access must be through the LAN server.) In addition, the server's access controls have been configured so that its WAN interface device is accessible only to programs that possess a special access control privilege. Only the System Administrator has the capability to assign this privilege to server programs, and only a handful of special purpose applications, like the T&A application, have been assigned this privilege.

The risk assessment concurred with the general philosophy taken by HGA, but identified several vulnerabilities. It reiterated previous concerns about the lack of assurance associated with the server's access controls and pointed out that these play a critical role in HGA's approach. The assessment noted that the e-mail utility allows a user to include a copy of *any* otherwise accessible file in an outgoing mail message. If an attacker dialed in to the server and succeeded in logging in as an HGA employee, the attacker could use the mail utility to export copies of all the files accessible to that employee. In fact, copies could be mailed to any host on the Internet. The assessment recommended stronger I&A be required for dial-in access, or alternatively, that a restricted version of the mail utility be provided for dial-in; the restricted version would prevent a user from including files in outgoing mail messages.

The assessment also noted that the WAN service provider may rely on microwave stations or satellites as relay points, thereby exposing HGA information to eavesdropping. Similarly, any information, including passwords and mail messages, transmitted during a dial-in session is subject to eavesdropping. To reduce these risks, the assessment recommended that HGA replace its current modem pool with encrypting modems, and provide each dial-in user with such a modem. It also recommended that HGA work with the mainframe agency to install a similar encryption capability for server-to-mainframe communications over the WAN.

20.6.5.2 Risk Mitigation

As with previous risk assessment recommendations, HGA's management tasked COG to

[100] Although not discussed in this example, recognize that technical "spoofing" can occur.

analyze the cost, benefit, and impact of addressing the vulnerabilities identified in the risk assessment. HGA eventually adopted some of the recommendations based upon the risk assessment while declining others. In addition, HGA decided that its policy on handling T&A information needed to be clarified, strengthened, and elaborated, with the belief that implementing such a policy would help reduce risks of Internet and dial-in eavesdropping. A revised policy statement was developed and issued. It stated that users are individually responsible for ensuring that they do not transmit disclosure-sensitive information outside of HGA's facilities via e-mail or other means. It also prohibited them from examining or transmitting e-mail containing such information during dial-in sessions. Penalties for non-compliance were also developed and promulgated.

20.7 Summary

This chapter has illustrated how many of the concepts described in previous chapters might be applied in a federal agency. An integrated example concerning a Hypothetical Government Agency (HGA) has been discussed and used as the basis for examining a number of these concepts. HGA's distributed system architecture and its uses were described. The T&A application was considered in some detail.

For context, some national and agency-level policies were referenced. Detailed operational policies and procedures for computer systems were discussed and related to these high-level policies. HGA assets and threats were identified, and a detailed survey of selected safeguards, vulnerabilities, and risk mitigation actions were presented. The safeguards included a wide variety of procedural and automated techniques, and were used to illustrate issues of assurance, compliance, security program oversight, and inter-agency coordination.

As illustrated, effective computer security requires clear direction from upper management. Upper management must assign security responsibilities to organizational elements and individuals and must formulate or elaborate the security policies that become the foundation for the organization's security program. These policies must be based on an understanding of the organization's mission priorities and the assets and business operations necessary to fulfill them. They must also be based on a pragmatic assessment of the threats against these assets and operations. A critical element is assessment of threat likelihoods. These are most accurate when derived from historical data, but must also anticipate trends stimulated by emerging technologies.

A good security program relies on an integrated, cost-effective collection of physical, procedural, and automated controls. Cost-effectiveness requires targeting these controls at the threats that pose the highest risks while accepting other residual risks. The difficulty of applying controls properly and in a consistent manner over time has been the downfall of many security programs. This chapter has provided numerous examples in which major security vulnerabilities arose from a lack of assurance or compliance. Hence, periodic compliance audits, examinations of the effectiveness of controls, and reassessments of threats are essential to the success of any organization's security program.