Public Switched Network Security Assessment Guidelines

September 2000

PREPARED BY THE OFFICE OF THE MANAGER, NATIONAL
COMMUNICATIONS SYSTEM (OMNCS)
701 S. Court House Rd., Arlington, VA 22204-2198

Public Switched Network Security Assessment Guidelines

Table of Contents

EXECUTIVE SUMMARY......VII

1 INTRODUCTION......1

1.1 WHAT ARE THE SECURITY CONCERNS?......1
1.2 DOCUMENT SCOPE AND OVERVIEW......2

2 DEFINING THE SECURITY ENVIRONMENT: RISK ASSESSMENT......6

2.1 ASSET ANALYSIS......6
2.1.1 Assigning Business Value......6
2.1.2 Physical Assets......7
2.1.3 Service Assets......8
2.1.4 Information Assets......8
2.2 THREAT ANALYSIS......8
2.3 VULNERABILITY ANALYSIS......9
2.4 ASSIGNING RISK......10
2.5 FUNCTIONAL ISOLATION OF ASSETS......10

3 SECURITY POLICY AND PROCEDURES......11

3.1 POLICY SCOPE......11
3.2 PROCEDURES......11
3.3 GENERAL CONSIDERATIONS......12
3.4 INTRUSION RESPONSE POLICY......13
3.5 PERSONNEL POLICY......13
3.5.1 Employee Responsibility, Awareness, and Accountability......14
3.5.2 Corporate Responsibilities......15
3.5.3 Hiring......16
3.5.4 Termination Procedures......17
3.5.5 Employee Identification......17
3.5.6 Clearances......17
3.5.7 Former Employees' Responsibilities......17
3.6 INFORMATION PUBLISHING AND DISTRIBUTION POLICY......18
3.7 PHYSICAL SECURITY POLICY......20
3.8 NETWORK ELEMENT POLICY......21
3.9 OPERATION SUPPORT SYSTEM POLICY......22
3.10 NETWORK MANAGEMENT POLICY......22
3.11 TRANSPORT POLICY......22
3.12 ACCESS NETWORK POLICY......23
3.12.1 Architecture Policy Issues......24
3.12.2 Access Policies......24
3.12.3 Software Policies......24
3.12.4 Security Administration Policies......25
3.13 SECURITY AWARENESS......25
3.13.1 Purpose of Security Awareness......25
3.13.2 Target Audiences......26
3.13.3 Components of a Security Awareness Program......27

4 PHYSICAL SECURITY......29

4.1 PHYSICAL PREMISES SECURITY 29
4.1.1 General Building Security 30
4.1.2 Guards, Locks, and Identification Badges 30
4.1.3 Physical and Logical Key Administration 31
4.1.4 Functional Separation of Facilities and Multi-Level Access Control 32
4.2 BUILDING SERVICES 33
4.2.1 Utilities (Power, Water, Telecommunications, Waste Disposal) 33
4.2.2 Emergency Facilities 34
4.2.3 Transport Redundancy and Physical Protection of Critical Facilities 34
4.3 ENVIRONMENTAL AND GEOGRAPHICAL THREATS 34
4.4 CO-LOCATION PROCEDURES 35

5 NETWORK ELEMENTS 36

5.1 ANALYSIS OF THE OPERATIONS INTERFACE SECURITY 36
5.1.1 Identification and Non-repudiation 37
5.1.2 Authentication 37
5.1.3 System Access Control 38
5.1.4 Authorization 38
5.1.5 Audit 39
5.1.6 Integrity 39
5.1.7 Confidentiality 39
5.1.8 Security Administration 40
5.1.8.1 Ascertaining the NE’s security features 40
5.1.8.2 Comparing against policy 40
5.1.8.3 Assessing the security configuration 41
5.1.9 Installation 41
5.2 SECURITY PROFILE FOR THE CALL-PROCESSING INTERFACE 41

6 OPERATIONS SUPPORT SYSTEMS 43

6.1 SECURITY FOR OSS INGRESS 43
6.2 SECURITY ISSUES FOR THE OSS/NE INTERFACE 44

7 NETWORK MANAGEMENT SYSTEMS 46

8 TRANSPORT 49

9 ACCESS NETWORKS 50

9.1 ARCHITECTURE REVIEW 51
9.2 ACCESS MECHANISM REVIEW 52
9.3 OPERATING SYSTEM REVIEW 53
9.4 SECURITY ADMINISTRATION REVIEW 53
9.5 MISCELLANEOUS CONCERNS 56
9.5.1 Business Partner, Reseller and Vendor Access 56
9.5.2 Customer Access 56
9.5.3 Law Enforcement Access 57

10 DOCUMENTATION AND PRESENTATION 58

10.1 CATEGORIZING FINDINGS 58
10.2 ADDRESSING THE FINDINGS 58
10.3 INFORMING MANAGEMENT 59

11 SUMMARY 60

BIBLIOGRAPHY 61

APPENDIX A: RISK ASSESSMENT METHODOLOGY 63

A.1 RISK ANALYSIS 63
A.2 ASSETS FOR REVIEW 64

APPENDIX B: POLICY AND PROCEDURES CHECKLISTS 65

B.1 GENERAL SECURITY POLICY 65
B.2 INTRUSION RESPONSE POLICY 66
B.3 PERSONNEL SECURITY POLICY 67
B.4 INFORMATION PUBLISHING AND DISTRIBUTION SECURITY POLICY 69
B.5 PHYSICAL SECURITY POLICY 71
B.6 NETWORK ELEMENT SECURITY POLICY 74
B.7 OPERATIONS SUPPORT SYSTEM SECURITY POLICY 76
B.8 NETWORK MANAGEMENT SYSTEM POLICY 77
B.9 TRANSPORT SECURITY POLICY 78
B.10 ACCESS NETWORK SECURITY POLICY 80
B.11 SECURITY AWARENESS PROGRAM 83

APPENDIX C: SECURITY REVIEW CHECKLISTS 84

C.1 PHYSICAL SECURITY 84
C.2 NETWORK ELEMENT 91
C.3 OPERATIONS SUPPORT SYSTEMS 96
C.4 NETWORK MANAGEMENT SYSTEM 97
C.5 ACCESS NETWORKS 98

APPENDIX D: AUTOMATED ATTACK TOOLS 104

D.1 WAR DIALING 104
D.1.1 Resisting War Dialing Attacks 105
D.1.2 Using War Dialing 105
D.2 AUTOMATED NETWORK AND SYSTEM ATTACKS TOOLS: INTRUSION TESTING 105
D.2.1 Detecting Automated Network Attacks 106
D.2.2 Using Automated Network Attack Tools 106
D.3 PUBLIC INFORMATION SOURCES 107

LIST OF ACRONYMS 110

SOURCES AND REFERENCES 112

EXECUTIVE SUMMARY

The Public Switched Network (PSN) of the United States has undergone significant changes over the past decade as a result of new technologies, regulatory changes, and network consolidation. These changes have resulted in benefits that derive mostly from expanded service offerings, lowered barriers to entry to the telecommunications market, and a resulting flood of new service providers. Along with the benefits, however, there has been an increasing concern over the overall security of the nation's telecommunications infrastructure. With the rash of new entrants, security measures applied to the infrastructure are more diverse and varied with respect to the technologies in use and the pervasiveness of their application. The result has been an uneven mix of partial defenses rather than a cohesive, complete security solution. Hence, there is an increasing likelihood that portions of the infrastructure may be inappropriately or inadequately secured.

Securing the PSN requires that service providers be aware of vulnerabilities and threats, and be able to assess the security of the network and mitigate any flaws. In December 1998, the Office of the Manager, National Communications System (OMNCS) produced a publication entitled *Public Switched Network Best Practices Security Primer* that outlined security threats and vulnerabilities, and provides a set of security guidelines and recommendations from a service provider's perspective. As a companion to that primer, this assessment guide offers guidelines and methodologies for conducting a *security assessment* for service providers. The purpose is to provide a common framework to enable better identification of security risks by new and existing carriers, and to evaluate and address those risks in an efficient and effective way. The guide focuses on security issues specific to the PSN. General computer and data network security issues are included only when they are relevant to PSN security, since other guides address those areas.

This guide describes a risk assessment procedure to identify high-value, high-risk components of a service provider's network and information assets. The risk assessment is designed to form the basis of a review of the service provider's overall security stature. Following the description of the risk assessment methodology are a series of descriptions of important security aspects of various components of the provider's network and operations. These include descriptions of security policy, physical security, network element and operations security, network access security, security training and awareness programs, and intrusion response procedures. The descriptions have been designed to drive a comprehensive review of these important pieces of a service provider's security program. The descriptions assume a detailed knowledge of the functional components of the networks and ancillary processes and procedures, but very little knowledge of best practices for protecting the company from internal or external malicious tampering.

Summary checklists of the important aspects of a security review are provided at the end of this guide to help carriers either conduct a comprehensive security review or design small, specialized security reviews of assets and network components critical to the protection of their business. The guide also includes a section on documenting and presenting the results of a security review.

The OMNCS and Telcordia Technologies created this publication in an effort to provide practical security measures for the protection of communications networks, which are one of the Critical Infrastructures upon which the United States is dependent for its national security, as identified in Presidential Decision Directive 63 (PDD 63).

1 INTRODUCTION

The Public Switched Network (PSN) of the US has undergone a momentous evolution in recent years as an outgrowth of regulatory changes, new technologies, and network consolidation (i.e., the merging of voice and data networks made possible by the evolution of new high-speed data networks such as ATM/SONET[1]). These changes are beneficial for having opened the door for innovative services, aggressive pricing, and increased competition. Much of the benefit derives from the lowering of barriers to entry to the telecommunications market, and the resultant flood of new service providers (commonly referred to as Competitive Local Exchange Carriers, or CLECs).

Along with the positive aspects of change, however, the disintegration of tightly held and controlled telephone networks has led to concern about the overall security of the nation's telecommunications infrastructure. In the past, the relatively few players used similar security policies, techniques, and methodologies to ensure that their networks were at least moderately protected from malicious attacks or exploits. With the rash of new entrants, security measures applied to the infrastructure are more diverse and varied with respect to the technologies used and the pervasiveness of their applications. Despite this, there is an increasing likelihood that portions of the telecommunications infrastructure may be inappropriately or inadequately secured. Coincident with this, the increase in technologies such as personal computers has opened the network to new and varied forms of attack from individuals (e.g., "hackers") and others not formerly considered a threat. This development has further amplified the concern that moderate protection is no longer acceptable.

Securing a telecommunications network requires that service providers be aware of security vulnerabilities and threats, be able to assess the security of their networks, and be able to mitigate any discovered flaws. In October 1998, the Office of the Manager, National Communications System produced an informational publication entitled *Public Switched Network Best Practices Security Primer* that outlined security threats and vulnerabilities from the perspective of new service providers. This assessment guide is intended as a companion document that provides general guidelines and methodologies for conducting a *Security Assessment* for providers. The purpose is to provide a common framework to enable better identification of external and internal security risks by new and existing carriers.

Since a basic understanding of the security concerns is important for appreciating and using the methodologies, the following section provides a brief summary.

1.1 What Are the Security Concerns?

In general, the changes taking place in the telecommunications industry are resulting in more potential vulnerabilities, as listed below:

[1] ATM stands for Asynchronous Transfer Mode.
SONET refers to the Synchronous Optical NETwork.

- The scope of the threat from insiders is increasing due to regulatory changes, technology drivers, and new business which, combined, result in more open access to equipment and devices such as Network Elements (NEs) and Operations Support Systems (OSSs). The number of people having access to various critical systems is therefore increasing. The insider threat manifests itself both as malicious actions and accidental misuse of network facilities.
- Outsiders include hackers (both amateur and professional), terrorists, foreign intelligence agencies, organized criminals, and industrial espionage agents. The threat from these sources has been recognized as increasingly dangerous, and is projected to grow in severity. The threat is compounded by the growing interconnection of systems, which increases the number of points of access to a network.
- Widespread access (e.g., through the Internet, TCP/IP[2]-based networks, inter-network communications, network management systems, dial-up links) increases the number of vulnerable points within a network. Further, the expanding complexity of the network engendered by its increasingly open architecture requires constant monitoring, thus demanding even more open access and a corresponding increase in new avenues of access.
- The PSN is now seen as a resource whose viability must be maintained if the nation is to function during peacetime, wartime, and national crises. This fact is not lost on foreign governments, terrorists, and others who may be hostile to US interests.

In the past, the owners of the PSN, who had a vested interest in its security, saw to its protection. Today’s network, though, is open to many new parties. While part of their responsibility is to provide protection for the network, this is a difficult task that may not be compelling from a business or operations viewpoint. The methodologies and guidelines described in this guide are intended to help facilitate the task of analyzing and securing a telecommunications network.

1.2 Document Scope and Overview

Conducting a security review of a telecommunications network is a complex process that can be resource intensive. For this reason, it is important that the organization involved in the review be committed to the security of its infrastructure and have a program of security and security management in place. Further, the overall security stature of the infrastructure must be a high priority for the organization’s management. This guide is predicated on the assumptions that some security policies, security management, and security resources are in place, since otherwise there is nothing to review. It is also important that the process of conducting a security review not be so onerous and cumbersome that it will not be undertaken.

It is important to realize that a modern telecommunications network is actually a collection of interconnected networks that serve different purposes and have different architectures. For example, in addition to the network of local access loops, switches, and transport networks that carry the content of individual calls, there are associated networks that

[2] TCP / IP stands for Transmission Control Protocol / Internet Protocol.

support operations, maintenance, signaling, and other functions. A security review will necessarily need to assess the security of these associated networks as well as the switched network itself, since disruptions of the associated networks can cause disruptions to, or loss of, the PSN's capability to complete calls. Figure 1 is a highly simplified diagram of the major components of a modern PSN that should be considered when conducting a security review.

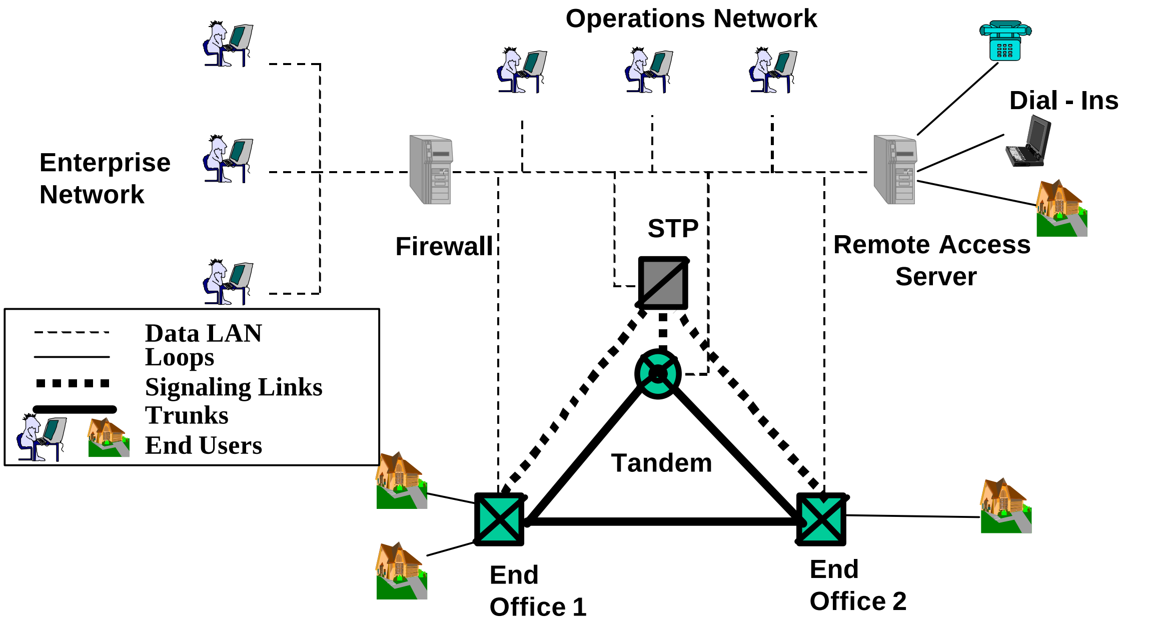

Figure 1: Simplified Telecommunications Network Diagram

Since many different organizations are involved in various aspects of running the components illustrated in Figure 1, ensuring an efficient and productive review requires that all phases of the business and operations of the network service provider be analyzed for the appropriateness of inclusion in the exercise. For this reason, the remainder of this guide is organized around various components of the service provider's business and network. Each of these components may be more or less appropriate for any given provider. The following sections address (in approximate order of precedence) the major components of the assessment and the purpose behind the assessment of those components. Appendices at the end of the guide provide checklists for the points discussed.

The guide addresses the following components of a security assessment:

1. **Security Environment Definition:** This is the discovery phase of the review and includes an identification and relative valuation of the critical business assets of the provider as well as identification of potential threats to those assets. This analysis, commonly known as a *Risk Assessment*, is used to direct later phases of the review to ensure that representative samples of critical assets are reviewed.

2. **Security Policies and Procedures Review:** A review of all existing security policies and procedures is essential to determining whether they exist in sufficient detail and breadth to protect the critical assets that have been identified.

Ideally, general security policies specify high-level organizational goals for protecting assets. Policies are then supplemented by specific procedures for securing different classes of assets. In practice, however, what comprises policy and what comprises procedure is often ambiguous. For this reason, policies and procedures are often combined in single documents that outline high-level security goals and prescribe procedures for implementing the goals. In this guide, policies and procedures are discussed together in Section 3. An attempt has been made to organize the material within these sections to cover high-level policies first and specific procedures for implementing the policies following the high-level discussion. Note, however, that even procedural elements of the review, as discussed here, are necessarily at a high level, since specific procedures depend on the security capabilities and configurations supported by the specific products deployed in the network. The important aspect of the review is to determine that security policies exist and are complete, and that sufficient documented procedures exist to provide guidance on implementing the policies.

Often, gaps in the policies and procedures will be identified in this early review phase. In addition to security policies and procedures specific to classes of assets, the policy review covers general security practices such as intrusion response procedures, security awareness training, and contingency planning.

3. **Physical Security Review:** This part of the review is designed to assess the security of physical premises housing critical assets, adequacy of building services from a security perspective (e.g., document disposal, utilities, custodial service), and protection against potential environmental or geographical threats to the physical infrastructure.

4. **Network Element Security Review**: This includes an analysis of the security features in place for critical NEs such as switches and routers. The NE review also includes an examination of selected special equipment that has been identified as critical, including, for example, Signaling Transfer Points (STPs), ATM switches, and SONET switches.

5. **Operations Support Systems:** Modern PSNs usually use *Access Networks* to support Operations, Administration, Maintenance, and Provisioning (OAM&P) functions on multiple NEs from a central location. These functions are performed by applications known broadly as Operations Support Systems (OSSs). OSS security, therefore, can be considered as an extension of NE security, so security features and mechanisms appropriate for the NEs should be deployed on the OSSs themselves. There are, however, aspects of the OSS/NE interface that should be considered separately.

6. **Network Management Review:** Network management refers to the controls that are used to manage nodes on a network (e.g., switches, cross-connects, multiplexers). A review of network management processes and procedures includes a review of the management system itself, the managed nodes, and the protocols (e.g., SNMP, CMIP) used by the management system. The review of the managed nodes is covered by the Network Element review (Section 5). Generally, the protocols will be fixed standards, and there is little to be done about the form of the protocols themselves. The network management review, then, will focus more on how the management system is implemented and configured, and the vulnerabilities that its use entails.

7. **Transport Network Review:** This includes an analysis of the security of the internal networks that connect PSN network components (e.g., trunks, signaling links). Transport facilities can be threatened either physically or logically.

8. **Access Network Security Review:** This is perhaps the most difficult part of the review, since Access Networks are usually widely distributed and large numbers of personnel are granted access. The review entails such things as authentication and authorization, interconnectivity, and firewall configuration. The details of the review depend on the composition of the specific Access Networks and systems under review (e.g., Windows® NT® or UNIX®-based, underlying protocols, types of access allowed, security features of operations system software packages). An important component of the Access Network review is an examination of access control procedures and devices. This analysis includes remote access servers, external scans of firewalls and Web servers, and war dialing exercises to identify modems. The review of remote access capabilities also includes an examination of the kinds of roles that are permitted to use remote access and the restrictions that are applied for each role. Of additional importance is a review of the breadth of access allowed to critical resources from within the corporation.

9. **Assessment Documentation and Presentation:** The final phase of any security review includes organization and prioritization of findings. The goal of review documentation and presentation is to assure that the resources available for addressing any review findings are spent in the most effective way.

Each of these components is covered in the remaining sections of this guide. Appendices containing supporting details are provided at the end of the guide, when appropriate.

Implicit in the above descriptions is the difference between reviews of security policy and procedure documents, and on-site inspections of facilities to ensure that the policies and procedures are applied. Some aspects of a corporation’s general security stature can be ascertained by reviewing the documentation of its security policy and procedure documents. However, verification of implementation of the policies and procedures will sometimes require on-site inspection of facilities. The organization of this guide reflects those differences. The section on Security Policies and Procedures (Section 3) covers document reviews for all aspects of security policy and procedures. Checklists for the document reviews are in Appendix B: Policy and Procedures Checklists. Sections 4 through 9 cover on-site reviews of facilities. Checklists for these reviews are in Appendix C: Security Review Checklists. Section 10 covers documentation and presentation of review results and has no associated checklist.

2 DEFINING THE SECURITY ENVIRONMENT: RISK ASSESSMENT

The first step in conducting a security review is to define the environment across which the review will apply. In general, this involves conducting a risk assessment of various business assets resident on the network. For large businesses this can be a difficult task, since many types of service and communication environments exist and are potentially at risk. A useful technique for deciding which elements of the environment are most at risk is to identify those assets of the business that are critical to its continued operation, profitability, and viability. This analysis, known as an *Asset Analysis*, directs later phases of the review by ensuring that representative samples of critical assets are reviewed.

Once the assets have been identified and evaluated, the second step is to conduct a *Threat Analysis* for the assets. *Threats* refer to the ways by which the asset may be compromised, and are important for determining the kind of security that should be applied to protect any particular asset. Finally, there should be an analysis of the level of exposure the asset has to exploitation. This is known as a *Vulnerability Analysis.* Taken together, these three analyses comprise a Risk Assessment.

2.1 Asset Analysis

For purposes of a security analysis, assets are placed into three broad classes.

- **Physical Assets** are the most familiar. They include building facilities and any equipment or supplies they house. Usually a security review will focus on protection of facilities (e.g., switches, data storage devices, computers) that are critical to the continued operation of the business. Security incidents involving theft or damage to physical assets can jeopardize the integrity of other types of assets. Normally, critical building facilities (e.g., central offices, data centers) are identified by an analysis of the equipment, systems, or data repositories residing there. For this reason, it is usually sufficient to identify critical network components and service and data assets (see below) and use their locations as the basis for performing physical reviews of building security.
- **Service Assets** fall into two classes: internal and external. Internal service assets (e.g., customer service systems, enterprise networks, operations support) are those that provide internal functions for increased productivity and efficiency. External services include those that provide service offerings or promote some other essential business function (e.g., Web servers for advertising, marketing, and customer relations).
- **Information Assets** are often the most valued assets of a business. They include such things as intellectual property, proprietary information, customer records, and operational and administrative information.

2.1.1 Assigning Business Value

An asset analysis determines the information and services that are valuable to the company and hence may be targeted by an attacker. Once identified, assets should be assigned a value based on their importance to the business. For the purposes of conducting a security review, it is usually sufficient to assign a value of High, Moderate, or Low to each asset:

- High – loss of the asset will impair operations to such an extent that customer services cannot be provided.
- Moderate – loss of the asset will impair productivity, but services can still be provided (though perhaps in a degraded manner).
- Low – loss of the asset will have no severe effect on business operations.

Some common attributes of high-value assets include:

- They are frequently referenced and required for business processes to continue
- Loss or unavailability affects customer service
- Loss or unavailability may affect the security of systems or networks.

Some common characteristics of moderate-value assets include:

- Loss or unavailability can be tolerated for a short time
- Loss or unavailability may affect some aspects of customer service, but will not cause a loss of basic function
- Loss or unavailability may impede operations, but not halt them
- Loss or unavailability may cause serious, but temporary slowdowns
- Loss or unavailability may have no immediate affect, but could have medium- to long-term consequences.

Some common characteristics of low-value assets include:

- Loss or unavailability will have no immediate affect on customer service or operations
- Loss or unavailability will have little consequence to network or system security.

2.1.2 Physical Assets

While the buildings and other physical facilities themselves are valuable, an assessment of measures in place to protect them from the most common threats (e.g., vandalism, bombing) is not a focus of this guide. Rather, the focus is on evaluating the ability of a facility to protect the infrastructure that supports the production, maintenance, use, and security of service and information assets. Evaluating the importance of any individual facility therefore depends on first identifying the critical network components and service and information assets that reside therein. Usually, the need to conduct a physical security review arises naturally out of the evaluation of service and information assets.

It is important to note that protection of physical assets is only a subset of *physical security*. Physical security refers to methods of protecting the buildings (i.e., external security) and the assets housed within the buildings (i.e., internal security). While this guide does not address the external aspects of building protection in detail, it does cover such internal physical security issues as protection of physical assets (e.g., equipment, labs), access to such assets, and policies regarding protection of such assets. These topics are addressed later.

2.1.3 Service Assets

At the highest level, service assets include management, operations, customer service systems, business-facing systems, and other important corporate functions. At a lower level, service assets are composed of a myriad of physical devices, systems, and networks that make the high-level functions possible. Traditional internal service assets within the PSN have included switching systems, operations support systems, business systems, and ancillary support systems. More recently, this list has grown to include signaling systems and their components, mediated access devices, intelligent network elements, element managers, support networks, and other internal features. Externally, it now includes off-premise intelligent maintenance and testing equipment, craft laptop devices, external network access on a large scale, and many other features.

The security of these devices must be considered in the context of their value, their criticality to the network at large, their exposure or access by outsiders, and their usefulness as an "access portal" to other assets. Consequently, evaluating the importance of any individual service assets depends on first identifying the critical services and information assets that they support. The threat assessment of service assets is an important part of the assessment process, since service assets are the common features of both services and information.

2.1.4 Information Assets

In a very real sense, information assets are the key assets of a business. They include intellectual property, proprietary information, business and technology plans and goals, strategies, customer information, and the critical day-to-day business workings. An evaluation of the sensitivity, secrecy, and integrity of information assets is therefore paramount to establishing sensible protection methods. Information assets should be categorized by value, sensitivity, lifetime (i.e., the length of time the information is considered valuable), availability, criticality to continued operations from the short-term through the long-term, integrity, and reliability. Other factors may be important, depending on the nature (e.g., volatility) of the asset.

2.2 Threat Analysis

Once the assets have been identified, a determination must be made of the likelihood that they will be compromised via any of the following common threats.

- *Theft or Disclosure* occurs when, by accident or by intent, assets fall into the hands of a person not authorized to access them.

- *Unauthorized access* is a special case of theft or disclosure where an unauthorized individual obtains access to protected assets (e.g., computing resources or building interiors).

- *Loss of Integrity* occurs when assets are modified by a person or process not authorized to do so.

- *Denial of Service or Use* occurs when an authorized entity is unable to access resources to which it is entitled.

Service assets are typically subject to denial of service (i.e., loss of availability) and loss of integrity. Loss of availability can cause lost revenue, decreased productivity, and decreased customer confidence. Loss of service integrity can cause services to be misused, to be used by unauthorized users, or to become unavailable.

Information assets are usually subject to disclosure, loss of integrity, and denial of use.

Accurate, quantifiable threat analysis is difficult to achieve since it relies on knowledge of the capabilities and motivations of adversaries. Whether or not any of these threats are realized against an asset depends on several factors such as its perceived value, its intrinsic value, and the ease with which it can be accessed. A general idea of the likelihood that an asset will be targeted can be gained by considering whether:

1. Individuals or organizations can be identified that will benefit from acquisition of the asset, and if any benefits outweigh the risk of being caught
2. Resources and knowledge of how to compromise the asset are generally accessible to potential attackers
3. These or similar assets have a recent history of compromise.

If these are all true, or probably true, then the asset should be considered to be at high-threat potential. If an asset is high-value, and the threat potential is also high, then the asset requires the most stringent security measures and should be scrutinized closely in any review. Alternatively, low-value assets with a low threat potential may not require extraordinary attention.

2.3 Vulnerability Analysis

The final aspect to consider in evaluating the overall security stature of assets is an assessment of their inherent vulnerability to threats. Inherent vulnerabilities are aspects of assets that may allow or facilitate attacks. For information and service assets, they can be categorized into one of three types.

- The *operating environment* includes components such as computers and software supporting the asset, and the media used to transport information and connect systems (e.g., wire, fiber). Any of these components may provide additional security features, create new security exposures, or have no effect on security.

- The *connectivity* of an asset refers to the number of direct interfaces to the system containing the asset. Attacks may be directed against a system having limited assets in order to obtain access to the more valuable assets of other systems connected to it.

- The method and extent of *user access* can contribute to the inherent vulnerability of the asset. The more general (and open) the level of user accessibility, the greater the inherent vulnerability.

Note that inherent vulnerabilities are closely related to threat potential, since both accessibility and knowledge of attack methodologies increase as inherent vulnerabilities increase. In general, high-value assets should be segregated into environments that are low in inherent vulnerabilities. Thus, for example, proprietary information should be stored in secure low-vulnerability devices, and not on public access Web sites. The assignment of high, medium and low inherent vulnerability is a value judgment based on the three types enumerated above. As a rule of thumb, if an asset is high in two or more categories of inherent vulnerability, it should be categorized as High. If it is high on one type and low on the others, it has medium inherent vulnerability. Otherwise, a low rating may be appropriate.

2.4 Assigning Risk

The assignment of risk to various assets will drive all further aspects of the review. The review will focus on the asset itself as well as any security policies relevant for the asset, the physical security of facilities hosting the asset, and any ancillary systems or networks associated with the asset.

Clearly, any asset that is high in value, threat potential and inherent vulnerability should be included in the network environments selected for review. Similarly, any assets rated low in all areas probably would not benefit from a comprehensive review. High-value assets should be carefully considered for review if either other assessment (threat potential and inherent vulnerability) is high, unless it can reasonably be concluded that it is adequately protected without a comprehensive review. For example, a high-value asset implemented on a platform with high threat potential may not require review if it has very low connectivity and tightly controlled access (i.e., low inherent vulnerability).

Of course, risk is only one dimension of defining the scope of any security review. This simple risk assessment process is intended to identify candidate assets for consideration in determining the scope of the review. The decision to include an asset in a review will be based not only on risk, but also on input from subject matter experts on the assets, the judgment of the reviewers, strategies and priorities of the business, and the availability of resources for conducting the review. Nevertheless, it is a useful tool for understanding the security needs and requirements of the business.

2.5 Functional Isolation of Assets

Once all of the critical assets have been identified and prioritized with regard to the overall risk to the company, the functional separation of the assets needs to be considered. For network-resident assets, this involves an analysis of the network topology to ascertain whether the functional components of critical assets are, or can be, isolated from other general or non-critical functions. For example, the OSSs used for switch control and configuration should be examined to see if they are placed in the network in such a manner as to be easily isolated through firewalls or other means. The results of this analysis can contribute to recommendations for changes in the network topology or changes in the locations of assets within the existing topology. In addition, the analysis can help identify the perimeter of any networks to be selected for review or closer scrutiny.

Similarly, for physical assets, the extent to which critical assets are located in the same building, or floor of a building, can help to identify both the risks to those assets and the individual facilities that would benefit most from a comprehensive security review.

3 SECURITY POLICY AND PROCEDURES

A security policy is a set of directives that creates a security program, establishes its goals, and assigns responsibilities to organizations, groups, or individuals. The security policy defines the responsibilities of staff, technicians, administrators, and others who interact with the network or its components. Security procedures and practices are controls that are applied to protect the corporation’s network and information assets in accordance with the policy.

3.1 Policy Scope

The security policy serves as an important input for choosing technical solutions (i.e., procedures and controls) and is one of the most important steps in securing business assets. Although the policy does not tangibly protect against risks and vulnerabilities, its effectiveness is reflected in the relative effectiveness of the technical solutions or procedures applied to protect the corporation’s assets. Even the most rigorous security mechanisms will be ineffective without a strong policy to back them.

Policies are generally driven by business needs, not technical requirements. For that reason, effective policies require the endorsement of upper management. Since the policy may apply across the entire organization and may specify disciplinary action, a mechanism for communicating security awareness to the entire population of users and managers is essential.

The security policy also drives the security review process since it specifies the procedures and rules that determine what constitutes security, and conversely, what therefore constitutes a breach of security. The review processes described in Sections 4 through 9 depend in large part on the contents of the policies that pertain to those areas (e.g., physical security, NE security).

Policies alone, however, are not enough. The policies must be translated into procedures and technical solutions that can be applied to protect the assets. Further, these procedures must be adequately documented so that they can be uniformly applied across an organization.

3.2 Procedures

Security documentation should include the controls and procedures that are used to implement the policies for all of the critical assets identified in the asset analysis. Further, protective measures should be designed so that the level of security applied in protecting the asset is commensurate with the value of the asset to the organization. This means that the review should attempt to identify assets for which the policy either does not apply or for which implemented controls are too weak, given the assets’ value. Less obviously, the review should also identify areas where overly stringent security measures are being taken to protect low-value items. Security controls incur a cost in money, administration, and maintenance, so the policy review can help ensure that the company’s security resources are appropriately allocated.

From the perspective of a security review, the important thing is that sufficient documentation is available to describe the company's security policy and the uniform procedures that are to be applied to meet the policy. The policy and procedures review is an assessment of the completeness and appropriateness of documentation. For this reason, in the remainder of this guide policies and procedures will be treated identically, and policy will be used generally to refer to both high-level goals and specific procedures for implementing them. There has been an attempt, however, to outline general policy statements first and more specific procedural requirements second.

3.3 General Considerations

Security policies and procedures are intended for use by all individuals having responsibility for maintaining the integrity of the assets they cover. For this reason, they should include motivating and justifying background information on the types of threats and vulnerabilities they are designed to counter. Poorly justified policies will not—and often *cannot*—be followed.

The policies and procedures rely heavily on employees' behavior for their effectiveness. For this reason, they also usually include disciplinary actions that will be taken in the event of a violation. Additionally, the policy and procedures must be defined in terms of actions and behaviors that are concrete and observable. Otherwise, it will not be possible to enforce the policy consistently, if at all. Unenforceable policies will not be effective.

No matter how well written and conceived policies and procedures may be, there will always be situations where critical business functions require exceptions or changes. The policy should include a process for appealing its strictures or obtaining unusual privileges if they are required. Further, the appeal process should not be so onerous as to cause people with pressing needs to circumvent it in the interest of expediency. Similarly, every practice or procedure should include a method of obtaining further information or clarification.

A related issue is maintenance of policies and procedures. In addition to methods for appealing policy restrictions, there should be a process in place for periodically monitoring policies for appropriateness as conditions change. That process would include procedures for modifying security standards and policies, and procedures for administering security policies and assessing compliance.

The remainder of this section discusses important areas that should be covered by policies and procedures. To the extent possible, commonly accepted practices and procedures are described for each area.

The intent of the policy and procedures review is to determine whether or not the documentation, as it currently exists, provides adequate coverage of the areas. Later on, during the on-site security reviews of each of the other areas, the focus turns to whether or not appropriate security measures have been implemented to meet the requirements drawn from the policies and procedures. It is the policies that drive the review, so much of the content that will come under review for each of the other areas is mentioned in this section, albeit at a more general level.

3.4 Intrusion Response Policy

The corporate security policy should include requirements for a process to respond to security events. Note that many of the points elaborated below with respect to intrusion response actions will apply very broadly across a corporation. That is, there should be incident reporting criteria and paths for incidents involving, for example, Network Elements, Operations Support Systems, inappropriate disclosure of proprietary information, physical security breaches and the like. The policy should include at a minimum:

- Criteria for types of security incidents that should be reported
- Escalation paths for reporting incidents
- Identification of a single point of contact to respond to security incidents. The single point of contact must have the authority to deal with incidents as they occur, since it is impossible to prescribe responses to all types of incidents. The responsibilities of the single point of contact should be clearly delineated and should include:
  - → Identifying and authorizing resources for investigating incidents and mitigating vulnerabilities (i.e., deploying an Intrusion Response Team)
  - → Contacting law enforcement
  - → Dealing with media inquiries
  - → Conducting *post mortem* quality improvement reviews.
- Information dissemination paths to alert employees, in an effort to prevent similar incidents in other parts of the company
- Identification of resources responsible for monitoring new and existing vulnerabilities and ensuring that fixes or patches are applied.

3.5 Personnel Policy

Personnel policy is a type of policy that must be dealt with separately from others since it can apply to all employees, contractors, consultants, and others who have access to buildings and services. In most cases, personnel policy will apply across several domains while other policies are more restricted in their reach. Security aspects of personnel policy include such things as employee awareness of security and hiring practices for potential employees who will have access to critical or sensitive assets. Personnel policy issues are particularly important for outsourced services, which often include guard services, custodial services, and data management services.

Personnel policies that focus on security should include

- Corporate and employee responsibilities and accountability for securing and protecting corporate information and assets
- Hiring practices
- Codes of conduct and ethics as they pertain to rules and guidelines for protecting corporate property and information

- Employee awareness of the security implications of foreign business, proprietary information protection, and media contacts
- Disciplinary and termination policies for failing to follow security rules and guidelines
- Responsibilities and obligations of former employees to protect corporate assets and material
- Termination procedures and mechanisms for line managers, security administrators, and Human Resources departments to revoke all access to facilities and computer systems. These are procedural elements of the policies that may be included under separate documentation.

These topics are among those covered in this section.

3.5.1 Employee Responsibility, Awareness, and Accountability

Employee responsibilities vary among companies, depending on the company's services, its estimates of the value of its products and services (in terms of their sensitivity, intrinsic value, perceived value, criticality to company growth and success); its role in industry, the market, its clients, national interests; and other factors. The following list suggests some important employee responsibilities for protecting the corporation and its assets. Employees must:

- Be aware of and be in compliance with employee codes of conduct as they pertain to protection and security. Employees should know that they are accountable for violations of corporate conduct guidelines. Some companies require employees to acknowledge, by signature, their understanding and willingness to comply.
- Report misconduct of other employees to corporate security, management, or corporate bodies that oversee conduct. In circumstances in which they are unsure of how to proceed, employees must request further information from corporate security, management, or corporate bodies that oversee conduct.
- Safeguard corporate assets such as sensitive or proprietary information, intangibles (e.g., corporate strategies, new ideas), equipment, and other valuable commodities. Employees must be aware of the use and meanings of various proprietary markings, and be aware of the consequences of ignoring or misusing such markings.
- Obey corporate policies on use of corporate facilities such as computers, telecommunications equipment (e.g., telephones), and buildings and grounds, since abuse can lead to lapses in security.
- Be aware of the potential for espionage (corporate or other), and know how to react according to corporate policies and guidelines.
- Live up to their responsibilities and obligations to the corporation regarding proprietary information and sensitive assets when ending their employment (see Section 3.5.7, *Former Employees' Responsibilities*).

These points may be covered in corporate policies on personnel responsibilities, codes of ethics, security awareness guides, employment contracts, corporate rules, and other policies or procedures that deal with broader topics than security. Since employees are responsible for following all rules and guidelines, the corporation should work with them to make sure that all expectations and understandings (by both parties) are clear, accessible, and consistent (i.e., no rule, policy, or guideline contains information or expectations that contradicts others).

3.5.2 Corporate Responsibilities

Before it can expect responsible actions by its employees, a corporation must make sure that all employees are aware of and understand the rules and policies pertaining to conduct, ethics, and other corporate values. The corporation must provide programs, guidelines, points of contact, and awareness training to its employees to familiarize them with all rules and policies, and to instruct them on how to react to situations not covered. The corporation must also create a workplace environment in which its rules and policies can be followed. This includes emphasizing that corporate reprisals against employees who report unethical behavior are themselves unethical and inconsistent with corporate goals. The corporation should also maintain an internal body to oversee and review corporate initiatives, programs, and policies concerning workplace ethics.

Corporate responsibility should be documented and available to all employees. From a security perspective, it should clarify corporate views and policies on:

- Employee safety
- Protection (i.e., security and safeguarding) and integrity of assets, records, accounts, and intangibles
- Secure business dealings (e.g., corporate, Government, foreign) and fairness practices
- Employee responsibilities.

Established corporate perspectives on these issues are the necessary first step in any program that requires employees to understand the security expectations of the corporation and their responsibility for meeting those expectations.

The Human Resources (HR) department of an organization plays a critical role in both preventing and dealing with threats and issues arising from employees and other workers. The combined threat that arises from the work force is referred to as the *insider threat*. HR can help deter the insider threat by screening and interviewing potential candidates for employment. Once an employee has been hired, HR should be involved in training the employee about computer and resource usage, access policies, security policies, corporate asset protection policies, and others. Organizations should regularly reinforce these policies and require employees to acknowledge that they have read and understand these policies. In addition, if an employee does attack the organization, HR should be involved in the process of terminating that individual.

3.5.3 Hiring

Corporate requirements and policies on hiring differ (perhaps largely) from one corporation to the next, and place varying degrees of emphasis on education, former employment, and other aspects of the job applicant's background. From a security perspective, the corporation should establish hiring policies that define its position on:

- **Drug testing**: The use of some drugs (even legal ones) has been associated with reduced capabilities to carry out job functions, possibly including security-related responsibilities.
- **Background checks**: This is necessary for employees whose work may require access to sensitive corporate or personal information, or clearances to work in restricted areas (as required and carried out by the Government). Inquiries into convictions, drug abuse, or other behavior that may render the applicant at risk may need to be part of a background check.
- **Polygraph tests**: Although controversial, polygraph tests may be required for some employees, particularly those whose work is considered sensitive or a target for corporate espionage. Polygraph questions must be carefully constructed to be effective, and should be administered by a person certified in this area. Details are outside the scope of this discussion.
- **Previous employment**: Former employment associations may exclude an applicant from consideration. Also, an evaluation by a previous employer may be needed to verify the applicant's suitability (e.g., honesty, personal ethics) for employment or for some types of work within the corporation. Usually, legal guidelines and policies within the Human Resources department address these issues.
- **Convicted felons**: Due to the seriousness of felonious acts, some corporations make it a policy not to hire convicted felons while others have no qualms about doing so. In the area of computer security, for example, there is no consensus on whether convicted hackers can be trusted to put their skills to good use.
- **Conflicts of interest**: An applicant's participation in or association, even indirectly through friends, with another company, be it a competitor or not, may generate conflicts of interest that could lead the person to divulge corporate secrets, information, or ideas either deliberately or unwittingly, to members of that company. For this reason, some corporations count such associations as a violation of their corporate ethics policies. Hiring policies should reflect this concern and should include rules for handling potential conflicts of interest by job applicants.

When establishing hiring policies and practices, a corporation must be aware of potential clients' interests and restrictions (e.g., Government strictures) and their effects. While a client may not reject a corporation's bid for services on the basis of its hiring policies, it may place limits on the kinds of personnel it will accept based on its own unique restrictions. However, this is a legal or contractual issue, and will not be taken up here.

3.5.4 Termination Procedures

Upon termination (voluntary or involuntary), an individual should have his badge, keys and any other physical pass returned to Corporate or Building Security, as well as having all access to all computer systems revoked. There should be communications between security, management, and the Human Resources department to ensure that any log-on IDs and physical access codes have been accounted for and suspended, and that all authentication devices (i.e., token generators) have been returned. It is a good practice to give each employee a corporate-wide identifier that appears in every system database, so that it is easier to inventory an individual's access to systems when that access needs to be revoked. Also, the system administrator may want to restrict the individual's access to various systems between the time notice of resignation is given and the person's actual date of departure from the company.

3.5.5 Employee Identification

Security concerns over unauthorized access by persons intent on theft of equipment or information, corporate espionage, vandalism, revenge against employees, or other unwanted actions often demand that the corporation set up methods to identify its employees and others who need access to buildings and the corporate campus. This is usually done via a requirement for possession and display of an identification badge by employees *and* authorized visitors, as described in Section 3.7, *Physical Security Policy*, and Section 4.1.2, *Guards, Locks, and Identification Badges*.

It may also be necessary for the corporation to identify each employee's vehicle. Some policies require that a vehicle sticker be visible in a window of the vehicle, but the corporation should be aware that other people, including kidnappers, and terrorists can use that sticker to identify employees. Alternatively, the vehicle's license plate provides a unique identifier, although in this case a record that maps the vehicle to its owner must be kept. Whatever method is devised must provide adequate identification while minimizing the employees' exposure to personal risk.

3.5.6 Clearances

In addition to Government clearances, employees may need to obtain corporate clearances to access certain information, equipment, labs, offices, buildings, or campuses. Should the corporation require this, a system must be established to:

- Define clearance levels
- Determine the criteria for each level of clearance, both in terms of what each clearance will grant, and what an employee must do to obtain such clearance
- Enforce rules regarding use of clearances
- Establish a method of revoking clearances.

3.5.7 Former Employees' Responsibilities

Due to the nature of their business, the information they value, the ideas they may generate, and the advantage they may have in the market, many corporations need their secrets to remain so even after the people privy to them leave the company. While it may be difficult or impossible to ensure that former employees will not give away secrets, it is nonetheless important to establish personnel guidelines that emphasize the corporation's desire for continued secrecy. The policy should address the corporation's expectations that former employees will:

- Understand the concerns that motivate this type of policy
- Respect those motivations
- Uphold the same responsibilities and obligations concerning proprietary information and other secrets that they upheld as employees.

The policy should also:

- State any expectations the corporation may have that former employees will return any and all proprietary material they may have off site
- Clarify the corporate views on the return of all company-owned computers, laptops, palm units, and any other data storage equipment they may have off site
- State the corporate views on the removal of company-related proprietary material the employee may have stored on personal computers, laptops and the like (incidentally, corporate codes of conduct should address whether this is acceptable practice in the first place)
- Specify the types of information to be kept private (e.g., ideas, research, marketing strategies)
- Specify the time duration for which any or all sensitive material is to be considered secret
- Specify the corporate stand on former employees' use of proprietary information, ideas, and intelligence in connection with their future employment, business ventures, or consultations with others
- State clearly the corporation's legal recourse (if any) against employees who violate their responsibilities in this matter, and point out any punitive measures it is willing and able to use
- State that all physical and electronic access devices (e.g., keys, pass cards) to buildings and computer systems be returned.

3.6 Information Publishing and Distribution Policy

Information publishing and distribution policies are designed to ensure that intellectual property and proprietary information are adequately protected. Inappropriate distribution of proprietary information can lead to loss of competitive advantage, theft of information, loss of customers' confidence in the business, and loss of legal recourse if proprietary information is inadvertently or intentionally released to the outside world. Generally these policies apply to information assets regardless of the media on which they are available (e.g., written reports and memoranda, electronic documents, internal Web pages, verbal communications). Such policies should include:

- Criteria for what constitutes sensitive information
- Types of documents that fall under the policy (e.g., written material, drawings, photographs, models, microfilm, electronic files on tangible media such as tape or disc)
- Clear definitions of distribution categories and labeling standards (e.g., restricted, confidential), including criteria for applying the standards
- Identification of authorities responsible for applying category standards (e.g., author, manager, legal counsel)
- Criteria for categorizing information
- Document retention policies
- Branding, copyright, service mark, and trademark standards (i.e., definitions, usage guidelines).

In addition to these general policies, the documentation should include specific:

- Procedures for changing the distribution category of information (e.g., downgrading the sensitivity of information)
- Guidelines for secure distribution of restricted information
- Guidelines for disposing of proprietary information in a secure manner
- Processes for clearing information destined for public presentation (e.g., papers, talks, books).

Electronic publication via Web pages or other electronic information services may require special attention to control the breadth of availability of such things as corporate directories, research or project management information, personnel information, personal Web pages and the like. Electronic publishing policies may interact with access control policies applied to components of the company’s information infrastructure (e.g., Intranet vs. Extranet vs. Internet). In general, the categories and labels applied to non-electronic media such as paper apply to their electronic counterparts. But since the methods of distribution and disposal are different, the policy must cover those electronic media explicitly.

Since the proprietary nature of information can sometimes be questioned, the policy should include references to authorities who are cognizant of relevant laws governing intellectual property and are empowered to make determinations as to the proprietary status of any such information.

Tangential issues associated with information protection include:

- Handling of client information
- Hosting of clients on site and off site
- Protecting confidentiality in public settings (e.g., restaurants, convention halls)
- Maintaining a need-to-know focus during contract negotiations and sales.

These points are important because they address the protection of tangible resources in circumstances where distribution of sensitive material may occur without conscious intent or where employees' guard may be down. The policy must address them as appropriate for the needs of the business. Note that these points begin to overlap the more general areas of *customer interaction* and *personnel policies*, the latter of which is addressed in Section 3.5.

3.7 Physical Security Policy

Physical security policies are intended to ensure that the facilities (e.g., buildings, rooms in buildings, unstaffed locations) that house equipment and employees are protected from burglary, forced entry, damage, destruction, environmental threats, ill-intentioned insider threats, and a host of other threats. These threats may result in loss of information; loss of operation; harm to workers; and damage to the businesses' reputation, image, and ability to operate.

Adequate physical security of facilities containing assets critical to continuing the network and business functions of the company is one of the most important steps that can be undertaken by a company. All of the logical steps implemented to protect network components and intellectual property will be defeated if an intruder can gain easy access to physical facilities. Further, theft or vandalism of computers, specialized tools, supplies, documents, etc., can result in significant expense and loss of proprietary information. Items such as manuals, policies, or other written materials can be stolen and used by intruders to execute logical attacks at a later time.

The physical security policies and procedures should include coverage of:

- **Building access security**. This should include guidelines or requirements for locks, guards, employee identifiers (e.g., badges, proximity cards, biometrics), key inventory, and key auditing systems used to control initial access to a building.

- **Internal building security.** This includes policies for segregating critical corporate assets (e.g., switches, data centers, cable vaults) from more general-purpose areas of the facility. There should also be procedures to restrict access to critical facilities to those whose job functions require it.

- **Building services**. Guidelines for power sources, water sources, waste disposal (particularly disposal of sensitive or proprietary information), emergency response procedures, and fire protection services should be included as part of the physical premise policies and procedures. Contingency plans should be in place to ensure the fast restoration of functions and services critical to the viability of the organization.

- **Site security**. Any environmental or geographical threats peculiar to the location of the facility should be taken into account. There should be procedures for identifying any such risks and any measures that could be reasonably undertaken to protect against them. Standards and Best Practices that are referenced in the Bibliography should be considered when a facility is located in an area of risk.

- **Computer and data security**. Contingency plans for providing computing and data services in the event of a physical disaster (e.g., fire) must be in place. This plan must include:

  1. Schedules for backing up corporate and mission-critical data on a regular basis and its storage at a separate site
  2. The capability to switch operations to a temporary data center (this should be contracted in advance so the facilities will be there when needed) from which data processing can continue
  3. The capability to relocate critical functions to an alternate site
  4. The establishment of data communications and telecommunications into the temporary work site.

In addition, the policy should include procedures to cover any unusual circumstances, such as co-location procedures mandated by the Telecommunications Act of 1996, which may have resulted in recent changes in physical security. The policy and procedure review should identify any such new areas that are not adequately covered by existing policies and procedures.

3.8 Network Element Policy

Network Elements (NEs) are physical components of the network infrastructure that include devices such as switches, routers, cross connects, and special-purpose equipment (e.g., STPs). Since the NEs form the heart of the corporation’s network, their security is usually a high-priority item. Network Element security policies should address:

- Physical security requirements for housing NEs (These may be incorporated into the physical security policy.)
- Access control requirements, including:
  - User ID/password policies
  - Remote access policies
  - Policies on enterprise network interconnectivity
  - Policies for authorization hierarchies
- Auditing requirements
- Policies aimed at maintaining the integrity of NE systems and software (i.e., for prevention and detection of modifications to software and configurations)
- Policies for protecting the confidentiality of sensitive information that may be stored on the device
- Policies governing security administration of the device
- Requirements for security documentation and secure defaults during installation
- Policies for fraud detection and prevention.

3.9 Operation Support System Policy

Operations Support Systems (OSSs) are systems (e.g., workstations, personal computers, mainframes) that are designed to support the NEs. Generally, OSSs will reside on Local Area Networks with connectivity to the NEs. The OSS policies may, in all or part, be implicit in the policies designed to protect the NEs. Since these networked systems provide connectivity to potentially large numbers of NEs, however, it is desirable to have explicit policies for:

- Functionally separating OSSs from general enterprise networks for purposes of access control (i.e., firewalls)
- Restricting access to OSSs to individuals with a need
- Requiring all switch access to go through the OSS (i.e., a prohibition on modems and direct hook-ups) to enforce audit trails and authentication requirements
- Controlling deployment of software or devices on OSS LANs that are not necessary for supporting the NEs or the needs of the Operations Support staff.

3.10 Network Management Policy

Usually, policies and procedures that apply to network management systems are included in the policies for OSSs, NEs, and Access Networks. There may, however, be policies and procedures that apply specifically to management systems:

- Policy may dictate which elements and systems are to be managed by standard management software packages or specific protocols such as SNMP
- There may be specific policies on what job functions are allowed to access management systems
- There may be restrictions on connectivity of network management systems to other networks, since management systems offer enticing targets to intruders.

Note that Network Management Systems are a subset of OSSs, so any policies applying to OSSs should also apply here.

3.11 Transport Policy

Transport includes network communications paths that support network connectivity through physical links over which higher-layer protocols travel. The transport layer of a network includes the physical media plus the electronic or optical switches, amplifiers, multiplexers, and other equipment necessary for low-level communications. In general, policies and procedures concerning the protection of transport facilities are a combination of physical and NE security. The intent is to prevent loss of critical transport capacity or capability due to security incidents. Such policies and procedures will generally include:

- Guidelines that help establish a relative estimate of the risks of laying cable or fiber over a given path, and help eliminate unsafe routes
- Criteria for requiring redundant routing

- Requirements that redundant transport facilities be geographically separated, combined with criteria and procedures that help establish those routes
- Guidelines for protecting outside plant, including
  1. Rules that define ways of posting rights of way, to reduce digging accidents
  2. Rules that define ways of concealing the routes of critical transport
  3. Rules for resolving disputes that may arise between 1 and 2 above
- Policies requiring protection of physical premises where critical transport facilities are potentially exposed (e.g., cable vaults, distribution frames)
- Requirements that impose extra protection for sensitive transport facilities (e.g., military communications)
- Guidelines for determining the level of protection and types of security required for transport NEs
- Guidelines for establishing secure operations access to transport NEs.

Depending on the nature of the media, other requirements may be imposed (e.g., antiwiretapping strictures, restricted access to outside plant).

While it is clear from this list that the guidelines for transport are mainly subsets of the policies and procedures on NE security, Access Network security, and physical security, it is worthwhile to define transport policies as an assurance that this area is not left out of consideration when assessing overall security. A transport policy may range from a separate set of rules and guidelines to a simple reminder or pointer to policies in other areas.

3.12 Access Network Policy

Access Networks are data networks used to perform various administrative functions on NEs. This includes such things as NE configuration and update, performance monitoring, and the like. Often, these functions are performed from a centrally located data center comprised of a LAN with data connections to the devices for which the Access Network and its applications have been designed. Access to network components may be restricted to access from Access Networks, though direct craft access, remote access through other NEs, and dial-up communications are common practices as well (although direct access to NEs via dial-up lines is generally considered to be a security risk). Access Networks can be used to perform identification, authentication, authorization, and auditing functions.

Since the Access Networks are critical to the operation of those portions of the PSN that they oversee, there are usually security policies and procedures that apply to them, although those policies may be included in general data network security policies. Policies and procedures generally include security requirements for the Access Network’s:

- Architecture (particularly as it pertains to connectivity with other networks)
- Access mechanisms
- Software (i.e., operating systems and applications)

- Security administration.

3.12.1 Architecture Policy Issues

The Access Network security policy should include requirements for:

- Ensuring that the Access Network is sufficiently isolated from more general data network capabilities (e.g., through firewalls or network isolation)
- Ensuring that critical functions are implemented for high availability, and that auditing, backup, and recovery mechanisms are in place
- Declaring the types of services and protocols that are allowed on the network, and any restrictions that may apply to the use of allowed services
- Supporting security mechanisms, including security monitoring, auditing, and intrusion detection for the network and resident hosts
- Providing security administration, maintenance, documentation, and training specific to the Access Network (e.g., periodic review of audit logs, availability of security documentation).

3.12.2 Access Policies

Since Access Networks are critical to continued business functioning, special care should be taken to ensure that access to these networks is adequately controlled. The policies and procedures should specify:

- Who should be given access to the network, and from where access may be granted
- Authentication and Identification techniques that are to be used for different types of access (e.g., local access through consoles, remote access)
- Authorization level classifications that restrict individuals' access permissions to those needed for performing their jobs. This should include a policy for disabling user accounts when they are no longer needed.
- Whether direct modem or dial-up access is to be allowed. If such access is deemed necessary, strict policies regarding the security of such ingress should be established.

3.12.3 Software Policies

In general, only software necessary for day-to-day functioning of the Access Network should be resident on the network. In addition, software used on the network should have appropriate security features to protect the network. The software policies and procedures should include:

- Processes and procedures for approving software that is to be deployed on the network
- Policies for managing software changes, including software updates and application of fixes, and policies for new software to ensure that security configurations are appropriate

- Policies that ensure the software being loaded is verified to be unaltered from the vendor
- Policies defining minimum security requirements for software
- Prohibitions against installing unnecessary or unapproved software.

3.12.4 Security Administration Policies

The security policy for the Access Network should define security administration roles and responsibilities, including requirements for:

- Overseeing and maintaining the security features of the managed and managing devices, controlling access rights to these devices, and maintaining *secure* administrative capabilities
- Security administration of user accounts including establishing the parameters and settings that constrain them (e.g., password complexity and aging)
- Managing authorization levels of users and devices
- Maintaining adequate security audit trails and monitoring them on an ongoing basis.

3.13 Security Awareness

While it is important to develop consistent and comprehensive security policies and procedures, even the best policies will fail if employees are not aware of the risks entailed by security incidents and their individual responsibilities to ensure that the policies are enforced. Reviews of Security Awareness programs should focus on their completeness, appropriateness, and extent to which they are directed towards the various special personnel group characteristics.

3.13.1 Purpose of Security Awareness

Security Awareness programs are designed to inform employees of both the risks to their company's assets and their individual responsibility to mitigate the risks. Program reviews should ascertain the extent to which the programs accomplish these goals and are appropriate to corporate needs. Security Awareness programs should be aimed at:

- Protecting corporate assets
- Familiarizing employees with the corporate security policy and why security is needed
- Providing each employee with specific guidelines outlining his or her responsibilities
- Meeting the goals of corporate "due diligence."

In order to meet these goals, an awareness program must first provide employees with usable security guidelines appropriate to their job responsibilities and levels. This entails informing employees of the risks to the well being of the company if security is breached, as well as outlining specific behaviors and responsibilities that they can assume to help meet the company's security goals.

Second, an effective awareness program must be ongoing, providing periodic reminders and reinforcement of security risks and responsibilities. The aim is to keep the level of awareness high over time.

A corporate-wide security awareness program can contribute to these goals by providing guidance and training on general security risks and the policies designed to mitigate the risks. Additionally, more specific programs can help individual subsidiaries and business units meet their more specific security goals.

3.13.2 Target Audiences

Target audiences for awareness programs will typically span a broad range of employee groups, ranging from executives to developers, to marketing and sales, to information professionals, and so on. Each of these groups will have different security needs, and hence will need specific awareness materials and programs. Of course, some security policies and practices will also be generally applicable to all, or most, employees. Some potential target audiences include:

- **Corporate executives:** Corporate executives must participate in and support security initiatives if the initiatives are to be successful. A clear corporate mandate, funding for security programs, and access to management for timely decisions are essential to an effective security program.
- **Managers:** Managers must understand their role in bringing the corporate security goals into the work place by allocating resources, providing time and training, implementing effective processes, and providing accountability appropriate for their organizations. In addition, since they are knowledgeable in their local environments, managers can be instrumental in assessing their security awareness needs.
- **General employee population:** Some security policies are applicable to all employees regardless of their job responsibilities. Badge policies, physical security, personal use of company resources, and protection of proprietary information are some examples of security issues that span job responsibilities.
- **General computer and network user community:** Many security policies are generally applicable to all users of corporate computing facilities. Distribution of security materials and training for most employees is essential to prevent holes from developing in the network security fabric due to ignorance of policies and threats.
- **Network and system administrators:** Implementation of computer and network security policies is often left to local system administrators. It is important to recognize that system administrators' primary responsibilities have traditionally focused on ensuring the functionality and availability of computer and network resources. Security is sometimes perceived as anathema to these primary goals. It is therefore essential that administrators be (turned into) strong supporters of the concepts of security, be able to balance security with other factors (e.g., availability, performance), and be knowledgeable in risks and countermeasures.
- **Security specialists:** Security specialists of various types will have the most pressing need for access to corporate policies and procedures at fine levels of detail. This is

particularly true of network and system security administrators and information security specialists who are charged with protecting the corporation's logical and intellectual assets. These individuals will also be largely responsible for monitoring the security measures across organizations and developing new policies, practices, and solutions as the environment evolves.

- **Systems developers and integrators:** Developers and integrators are primarily responsible for ensuring that new systems have the requisite security features for compliance with corporate security policies.
- **Public facing organizations – Help desks, operators, etc.:** Personnel whose primary responsibility involves service to customers and corporate clients are usually trained to be as accommodating, cooperative, and helpful as possible. For this reason, they are particularly vulnerable to "social engineering" attempts and, in fact, are often targets of "hackers" and other miscreants seeking access to valuable company resources. The policies that cover these difficult aspects of customer interactions must be detailed and clear, and must take into account that it may be unrealistic to expect personnel to detect all social engineering attempts.
- **Contractors and business partners:** When non-employees are given access to corporate resources, it is important that they clearly understand their responsibilities with respect to corporate security. Often, specific agreements between the corporation and these external entities are necessary to protect the corporation's interests. For corporate business partners or external contracting organizations, large corporations often execute Data Connection Agreements (DCAs) that govern minimum security requirements for using the partners' network assets. DCAs may also include mutual auditing privileges, requirements for notification of security incidents, and penalties for non-compliance. DCA reviews are appropriate for organizations that have a large number of interconnections with business partners or that provide wide access capabilities to business partners.

  Equipment vendors and suppliers often request or require physical or remote access to network or computing equipment in order to facilitate upgrades or maintenance. The policies and procedures must define their methods and levels of access, declare the circumstances under which they may acquire access, and set guidelines that cover liability in case of accidental or deliberate actions that exceed the vendor's authority.
- **Manufacturers:** Manufacturing personnel may or may not have access to corporate computer and network facilities, but may nevertheless have access to information that lends a competitive advantage to the corporation.

3.13.3 Components of a Security Awareness Program

Depending on the target audience, one or more methods of instilling and fostering security awareness may be appropriate. For some users, in-depth security training on various topics may be periodically required. For others, a general awareness program, bolstered with periodic supplementary materials or reminders, will be all that is required.

The review should identify the minimum components of the program that are necessary for the particular company under review. These may include:

- Introductory security awareness materials (e.g., new employee training and awareness packages, security awareness videos). These can be provided to help define the goals of the program and the corporate commitment to the program, and to outline each employee's responsibility toward reaching the security goals. Such introductory material can be prescribed for new employees, contractors, and employees moving to new assignments. Periodic refresher courses may be appropriate for all employees having specific responsibilities in areas where risk levels are high.
- Security awareness training (e.g., System Administrators, Security Administrators, Firewall administrators). Training modules can be designed to meet the specific security needs of particular jobs and organizations, as well as those of the general population of employees.
- On-line security awareness information. These may be needed to bring all the elements of security initiatives into a readily available central site. Such sites are useful both as reference sources for security-related materials, policies and procedures, and as tools for providing security awareness training via interactive, self-paced training scripts.
- Continuing reminders and ongoing training programs. These can be designed to maintain a high level of visibility for security issues across the employee body. Such reminders may be targeted at specific security issues (e.g., computer security, theft of materials) or may be of a more general nature. They are extremely important since even the best security policy will tend to drift out of peoples' minds unless its existence and value are reinforced regularly.

All of these components may or may not be appropriate for all employees, depending, for example, on job function and access to the facilities necessary to deploy specific aspects of the program. An analysis of the security needs and functional capabilities of different areas of the company is required for a realistic development and deployment plan.

4 PHYSICAL SECURITY

Generally when assessing security vulnerabilities, physical security is important since it represents an attacker's most serious obstacle to a successful break-in. An attacker having physical access to NEs, OSSs, or computers has taken a large step towards completely compromising those devices, for even if physical access does not lead to an intrusion into the device itself, the alternative of destroying the device could hardly be easier.

The goal of a physical security plan is to protect the organization's assets from the attacker whose goal is a physical break-in. The assessment of the physical security plan is aimed at finding any vulnerabilities that might allow an attacker physical access to the premises and the equipment it houses, and giving planners the information they need to add or enhance the building's protective mechanisms.

An attacker may elect not to compromise the physical perimeter of an organization, choosing instead to disrupt or destroy an organization's capability to operate. An attacker's goal may be either the compromise or destruction of the buildings and enclosures themselves, or the compromise of the contents of the buildings; i.e., the staff or equipment, or both. An assessment must address both of these possibilities, since in some cases, mere destruction or damage to the building may lead to a desired outage or loss of business to the victim, while in other cases, the primary target must be the building's contents, operations, or staff (perhaps even one person on the staff). The physical security assessment should evaluate the organization's:

- Need to protect against each kind of attack
- Susceptibility to each kind of attack
- Preparations for each kind of attack
- Resilience to each kind of attack
- Contingency plans for emergency restoration of equipment, facilities and operations.

The remainder of this section addresses important aspects of physical security.

4.1 Physical Premises Security

Generally organizations will implement various levels of building access controls in accordance with the importance of the assets resident in the facility. Often, large corporations will build separate high-security facilities for critical network components such as switches or data centers.

The first aspect of building security that must be assessed is the importance of the assets resident there. This is usually determined during the discovery phase and asset assessment of the review. For completeness, the following sections include assessment items that would normally be evaluated for a facility housing high-value or critical assets. Less strenuous reviews would be undertaken for less sensitive facilities. The overall physical security assessment must determine the level of needed protection, and the relative quality of the protective mechanisms in place.

4.1.1 General Building Security

Although a building’s doors and windows are usually considered to be its primary access points, other points, such as air vents; entry points for water, gas, communications, and electricity; and drainage conduits must be given consideration, depending on the kinds of threats. Additional entry points such as Central Office cable vaults need to be considered, as do other places where a destructive potential exists. Furthermore, the buffer space between the public and the building itself must be given careful consideration. Certain complexes and buildings consider lawns, landscaping, lighting, and fences to be the first layer of perimeter defense because they slow an intruder or prevent a covert approach to the building. Outside cameras and other surveillance equipment further enhance or enlarge this buffer space.

4.1.2 Guards, Locks, and Identification Badges

Building guards can protect the external perimeter of the building and sometimes protect internal areas. For critical facilities the review should be aimed at ensuring that:

- All doors providing access to the facility are either locked or guarded at all times
- Any doors not normally in use, such as emergency exits, are alarmed. The review should ensure that alarms function properly and procedures exist to respond to alarms.
- Doors are properly installed so that they cannot be removed from the outside (e.g., hinges and bolts are protected from tampering on the outside)
- During peak periods of ingress and egress, entrances and exits have a guard present. During off-peak times, the door should be monitored and there should be some other form of access control (e.g., swipe cards, proximity cards, keys).
- Access through unguarded doors uses a method requiring identification of each entrant
- Unguarded doors that provide access via keys or other means have mechanisms to prevent “tailgating[3].” Mantraps, revolving doors, and detectors can be used to prevent tailgating or send an alarm that it has occurred.
- The recruitment qualifications (possibly including criminal or other applicable background checks and testing), training, and retention methods used for employing guards are adequate and appropriate. This is particularly important for contracted guard services, which are common.
- Employees, on-site vendors, contractors, and other authorized individuals possess and display a badge at all times while in the building. The badge should clearly indicate their affiliation (e.g., employee, contractor, escorted visitor, unescorted visitor).

[3] Tailgating refers to an unauthorized person’s act of following through a door opened by an authorized person.

- Non-employee visitors are given a temporary identifier such as a visitor's pass, and are required to wear it visibly at all times. The pass must clearly display the dates for which it is valid.
- Procedures and conditions exist under which visitors can enter and work unescorted, and the conditions under which they must be escorted
- Employee badges display a color photograph. The photograph should be big enough that the employee need not have to hand the badge to a guard in order for the guard to see it. The photograph should be clear enough that the face of its wearer can be compared with it. It should be constructed so that the photograph cannot be altered or replaced.
- The badge displays the employee's name and any other identifying information (e.g., number, bar code) clearly
- The badge is durable and resistant to wear, damage, or alteration as much as possible
- The badge contains any electronic or magnetic information that may be needed by card readers
- The badge provides a capability to limit access to some areas of the corporate campus, as opposed to full access, when appropriate
- The badge has an address to which it can be mailed without postage, if lost, should a non-employee find it
- Corporate or building security can disable or invalidate a badge that has been lost or whose wearer is no longer permitted to enter the building or corporate campus
- When the wearer terminates employment, someone (a manager, building guard, corporate security) will appropriate and destroy the badge so that it cannot be re-used.

The guards are not the only personnel responsible for preserving the internal security of a building. The authorized occupants often enhance the security of a building by vigilance and passive monitoring. The assessment should determine whether the staff has been empowered to challenge unauthorized personnel in controlled areas. A penetration test can be valuable for ascertaining the degree to which guards and employees are appropriately trained in the importance of physical security. Reviewers may attempt to evade or talk their way past guards, or entice employees to provide admittance through unguarded entrances.

4.1.3 Physical and Logical Key Administration

Traditional physical keys are rarely used in sensitive facilities because they are difficult to inventory and recover, and they do not provide an audit trail of the user. Often, use of physical keys is restricted to access to internal portions of the building such as storerooms, custodial rooms, and wire closets. It is still common, however, to find businesses and installations that use keylocks as their primary means for ingress to buildings or access to critical areas within buildings. When that is true, it is important that:

- Procedures exist for authorizing distribution of keys to individuals

- Keys be individually numbered
- A complete inventory of keys and their owners be maintained and audited
- Criteria be in place for replacing locks when keys are lost
- Periodic audits of the key inventory be enforced and procedures for reconciling discrepancies be in place
- Procedures be in place for recovering keys when access is no longer needed or authorizations change.

Logical key (e.g., proximity cards) procedures must, of course, be evaluated against the same criteria. Key recovery, ingress and egress recording, and authorization procedures are simplified with logical keys since such systems provide central facilities for monitoring use, assigning authorization, and disabling of keys. Still, there must be procedures in place to ensure that those responsible for maintaining the key inventory and authorization database are notified when individuals leave or their access requirements change.

Combination locks, a special case of logical locks, should be assessed to ensure that combinations are not discernible from wear patterns or from combinations written down. Combinations should be changed if entry authorizations are changed.

4.1.4 Functional Separation of Facilities and Multi-Level Access Control

Physical security applies to internal portions of a building as well as the external perimeter. Access to internal areas that are considered sensitive or operationally critical should be controlled when access to their contents is limited for any reason (e.g., they contain sensitive data, experiments, or equipment). In general:

- Critical computer and network facilities should be contained in areas having separate physical access control mechanisms. Access should be granted only to those having a need.
- Procedures should be in place to ensure that proprietary information is kept in secure facilities when not in use. Offices and file rooms where such material is routinely kept should be locked. The cabinets in which they are kept should also be locked.
- All potential access points to critical computer and network facilities (e.g., consoles, operations centers) should be controlled in a manner commensurate with the control enforced over the facility itself. (This is covered in more detail in NE and OSS security.)
- A record of access to all such controlled spaces should be maintained.
- Storage media holding critical information should be encrypted or housed in locked, limited-access areas.
- A critical system’s physical address should not be disclosed to those not having a need to know.

Controlling the internal areas of a building can be enhanced through the use of segregated roles and responsibilities. For example, administrative staff generally do not require access to an organization's computer rooms. Likewise, engineers do not generally require access into the document control room. The review should assess whether existing functional segregation is appropriate.

4.2 Building Services

The operations of an organization are critically dependent on the availability of services such as water, power, telecommunications and waste disposal, among others.

4.2.1 Utilities (Power, Water, Telecommunications, Waste Disposal)

In general, without power, water, telecommunications, and waste disposal services an organization cannot operate effectively, if at all. It is often the case that the dependency upon these services is undervalued. The assessment should evaluate the organization's planned reactions to service interruptions. For services critical to the continuing function of the business, the following steps are essential:

- Both commercial and local emergency power feeds should be duplicated and geographically separated to prevent accidental loss of power.
- Emergency power should be available to allow continued operation for greater than the average duration of power outages. Generating capacity should be available for deployment before emergency supplies are exhausted. (Mobile generators may be owned or contracted.)
- Sufficient emergency generator fuel should be stored on premises to run uninterrupted for a site-defined time interval. There should be sufficient capacity to satisfy the site's estimates of its needs (based on fuel consumption rates and expected outage duration). Fuel should be changed at intervals to account for the build-up of moisture in the tanks and aging of the fuel and the tanks.
- Sufficient on-site water storage (or delivery services) should be available to support continued operation of people and critical components of the facility. Water quantities should be sufficient for equipment cooling and for drinking and meal preparation.
- Outside communications must either have active-standby backups, or must be robust enough to operate in a crisis, as must internal communications. Capacity should be sufficient to handle crisis-level traffic. Provisions for alternate networks such as wireless networks or satellite services may need to be included, depending on corporate needs.
- Restroom and sewerage facilities must function through crises, or temporary arrangements must be in place (at least contractually) for quick activation.
- Air conditioning for computer rooms and other areas that require controlled environments must be backed up to prevent machine failure or damage from overheating.
- Locked containers for disposal and destruction of proprietary information should be readily available wherever such material is used. The review should trace the disposal path of such material to ensure that it is closed.

Of interest for the assessment is the distribution of these services within the buildings. The assessment should evaluate the overall resistance of the facility to service interruption from the origination of the service at the utility provider to the distribution paths inside the building.

4.2.2 Emergency Facilities

The review should assess the adequacy of emergency facilities such as fire detection and suppression, power conditioning (i.e., the capability to support constant voltage, power, and cycles), air conditioning, ventilation, and other environment protection systems necessary for continued operation of critical systems. These systems must react in ways that allow:

- People to evacuate the premises
- Equipment to be protected (at least long enough for fire companies or others to arrive)
- Facilities to retain structural integrity
- The building's contents to be protected from the outside environment, as much as possible.

Emergency facilities are important as much for the aftermath of a security breach as they are for accidents and natural disasters, as suggested in the previous section.

4.2.3 Transport Redundancy and Physical Protection of Critical Facilities

In general, critical computer and communications systems facilities should be geographically dispersed to the extent possible without unduly affecting operational costs, performance, and security. In addition, routing of critical communications links (e.g., important interoffice trunks, signaling links) should be redundant and geographically dispersed both inside and outside the facility so that communications may be immediately rerouted over physically diverse backup routes when necessary. The communications networks required for maintaining service should be designed in such a way that no single point of failure will result in a widespread or serious outage.

4.3 Environmental and Geographical Threats

Critical sites should be reviewed to identify any risks due to their location in areas likely to experience natural disasters[4], serious accidents (e.g., chemical spills, gas line explosions), power interruptions, and related problems. The review should also consider the effects of simple environmental factors such as extreme heat or cold, damage from salts and pollution, and harsh climate conditions. Documents such as Telcordia's *Network Equipment Building System (NEBS)* requirements cover these factors.

Geographical issues include the reactions of the local populace, including acts of hostility, responsiveness of local emergency services, and the general level of safety afforded

[4] This includes earthquakes, volcano eruptions, hurricanes, flooding, tornadoes lightning strikes, dust storms, snow, extreme tides and other environmental conditions.

to staff, both on site and en route to the facility. Since human activities and motivations change over time due to unrest, political problems, religious views, or other factors, reviews should be repeated periodically according to a predetermined schedule.

While it is often impractical to abandon facilities where such risks exist, it may be appropriate to plan for such an occurrence by duplicating or relocating critical systems and resources that are housed at high-risk locations to safer locations. Contingency plans to resume operations in such alternative locations should be in place and tested at intervals (so that the emergency situation itself is not the first test).

4.4 Co-location Procedures

The Telecommunications Act of 1996 (also known as the Telecommunications Reform Act, or TRA) mandated that Incumbent Local Exchange Carriers (ILECs) offer various components of their networks to competitors in an unbundled and non-discriminatory manner. Co-location, a logical result of the mandate, refers to the situation that prevails when equipment belonging to different providers is present in the same physical location. Of particular concern for the purposes of physical security reviews is that providing such access often means that competitors (sometimes multiple competitors) will require access to physical components and facilities.

For example, physical co-location is the predominant way that the ILECs provide the facilities for unbundled loops under the TRA. Co-location for the purpose of providing unbundled loops can expose other functional components to misuse or abuse to the extent that their facilities are housed on the same premises. With this in mind, extra care must be taken when performing a physical security review of facilities with co-located providers. The review should check that:

- Critical equipment is isolated by physical barriers to restrict access.
- Key distribution, accounting, and auditing procedures are in place. Processes should be in place to ensure that personnel changes can be monitored across co-located companies.
- Adequate distances between incompatible equipment types (e.g., to reduce the chance of disruptive electromagnetic interactions between their electronics), and building services (e.g., water lines) are maintained to avoid equipment failure or disruption
- Critical equipment and facilities do not draw attention to themselves. The traditional method of clearly marking crucial equipment and transport facilities (so-called “red blocking”) becomes a potential hazard in an open environment, and this should be recognized. The intention of red blocking is to alert support personnel that the circuit is especially important, and that care must be taken not to disturb it accidentally. These red blocks, however, may also serve as targets.
- Should there be interconnection or access to an OSS or a customer records system, adequate security measures must be established to partition and restrict the access to only those records of the co-located company. All co-located equipment and access points should be adequately secured from outside ingress and vulnerabilities.

5 NETWORK ELEMENTS

Network Element (NE) is a generic term that encompasses telecommunications devices such as switches, transmission elements, and routers. Typically, these devices have embedded software and databases that are configurable via their operations interfaces.

NE security analysis consists of assessing the status of three different types of security:

- **Physical security of the NE installations.** Issues related to physical security are described in Section 4, *Physical Security*. The task of physical security analysis consists of addressing and resolving these issues so that an objective assessment can be made of the level of physical security (or lack of it) in the NE environment.
- **Security associated with the Operations Interface.** The operations interface is accessed primarily by users such as craftspersons, administrators, and various OSSs for performing operations functions such as provisioning, maintenance, testing, and billing. This interface needs to be secured to protect the switch software and database from unauthorized modification, destruction, or disclosure. In order to ensure the availability, reliability, integrity, and correct billability of service, it is essential that the operations interface be secured against unauthorized use and modification or destruction of its embedded processes, software and databases. A security analysis consists of testing whether all operations interfaces of the NE are adequately protected from outside intruders as well as from insiders who may commit a security breach maliciously or inadvertently.
- **Security associated with the Call-Processing Interface.** The call-processing interface deals with traffic input and traffic output generated by subscribers to the services associated with the NE. This interface needs to be secured to reduce the occurrence of fraudulent use of the service. Security analysis consists of accessing whether adequate steps have been taken to mitigate fraud.

5.1 Analysis of the Operations Interface Security

An NE may have one or several operations interfaces, depending on its type. Also, with the proliferation of network protocols (e.g., TCP, UDP, IP) and distributed architectures, it is becoming commonplace for NEs to function as nodes in an elaborate Access Network that can provide multiple connections to the NE (see Section 9, Access Networks).

The Access Network hosts the OSSs used to access the NEs for various administrative and maintenance functions. Consequently, operations security also is becoming a distributed phenomenon. That is, operations security features of an NE may no longer be confined within the NE. For example, a mediation device such as a firewall or a security server may protect a *trusted* network from intruders, and the NE, being a node in that trusted network, may be partially protected by that mediation device. Thus the security analysis of an operations interface of the NE needs to be addressed in terms of whether security-related functional requirements (of that interface) are being satisfied within the environment, either by the NE itself or by mediation devices external to the NE. These functional requirements can be mapped directly to real functions such as Identification, Non-repudiation, Authentication, System Access Control, Authorization, Audit, Integrity, Confidentiality, Security Administration, and Packaging and Delivery. NE security analysis consists of testing whether these functional requirements are being satisfied within the NE environment.

5.1.1 Identification and Non-repudiation

Identification is the process of recognizing a user's[5] unambiguous and auditable identity with the help of an *identifier* (e.g., user-ID, digital signature) by which the user can be held accountable for the actions and events he initiates. In general, the user-ID need not be confidential, but it must be unambiguous. Hence security analysis consists of testing the following:

- Does the NE prevent an administrator from creating a user-ID that already exists?
- In a situation where there are more users than the number of user-IDs that the NE can accommodate, has a peripheral mediation device[6] been deployed external to the NE to distinguish among users sharing the same user-ID?

If answers to these questions are *No*, it may not be possible to hold users accountable for their actions on an individual basis.

5.1.2 Authentication

Authentication is the process of verifying the *claimed* identity of a user. The NE environment must offer features to verify the claimed identity of a user before giving that user operations access. Depending on the NE and the applications, there could be different kinds of authenticators. For example:

- The user can be associated with confidential information that only the user is supposed to possess such as: password, private key, or randomly time-varying PIN (such as those provided by single-use password tokens).
- The user can be associated with a distinctive physical or logical address. (e.g., user's authorized directory number, network address)
- The user can be authenticated by certain attributes that others are not expected to possess such as: voice or speech pattern, handwriting style, palm print, or retina scan.

Security analysis consists of conducting tests to determine how the system ensures that the authenticator (e.g., password, PIN number, token, smart card) of one user is protected from being used by any other user or intruder.

[5] A user may be a person, a process, or a system that requests a session with the NE to perform an operations-related task such as administration, maintenance, provisioning, or testing.

[6] The mediation device is a device having the capability to unambiguously identify individual users who share the same user-ID in the NE. For example, it could be a security server that a user has to log on to before accessing the NE. Another example is a card reader that allows physical access to the console of the NE, which is located within a perimeter protected by a physical barrier. (It is assumed that users sharing the same user-ID for the switch have individualized ID cards for the card reader, and that at any one time only one user is allowed inside the perimeter.)

5.1.3 System Access Control

System Access Control authorizes establishment of a session (i.e., login) and continuation of a session until logoff. Thus, the security analysis consists of performing tests to answer questions such as:

- Before allowing a session, does the NE environment demand the user's identifier as well as the authenticator? Are all operations interfaces except the Emergency Access Interface[7] (EAI) equipped with this feature?
- If several incorrect login attempts are made consecutively, (e.g., a password cracking attempt), does the NE environment generate an alarm on a near real-time basis or lock the channel?
- At the time of login, is a warning banner[8] presented?
- Does the NE environment provide features such as "time-out" and keyboard locking?
- How are remote logins protected against intrusion[9]? (This is a critical question because for remote logins over untrusted paths the passwords become susceptible to eavesdropping.)
- If there is direct access to the NE over a Data Communications Channel (DCC), as in the case of a SONET, does the NE protect itself from an intrusion from another NE over the DCC?
- If the NE is a broadband switch (e.g., an ATM switch), how does the NE protect itself from surreptitious access over a protocol such as Simple Network Management Packet (SNMP), which may not require a login?
- If the NE is a switch with a requirement to provide court-ordered *switch-based* surveillance in conformance with the Communications Assistance for Law Enforcement Act (CALEA), how does the NE environment ensure the confidentiality surrounding the surveillance activity?

5.1.4 Authorization

Authorization is the permission to access the NE resources (e.g., software, commands, data). The NE environment must have the capability to deny access to a resource of the NE unless there is proper authorization (e.g., user privilege, channel privilege, terminal privilege) for such access. Thus, the security analysis consists of performing tests to answer questions such as:

- Does the NE environment have the capability to deploy several levels of authorization (read only, read and write, create, retrieve, update, delete)?

[7] An NE may be equipped with an EAI which allows a session without requiring a login so that in the case of an emergency when the regular login feature does not function, the NE can be restored via the EAI. There are ways to protect the EAI against intrusion, and an alarm needs to be activated when the EAI is in use.

[8] An explicit display of a warning banner may be a legal prerequisite to prosecuting a suspected intruder. The warning banners should include information sufficient to meet US Department of Justice guidelines for allowing monitoring and successful prosecution of intruders.

[9] Several types of "strong authentication" can be deployed to protect remote logins.

- Does the NE environment prevent a user from accessing a resource of the NE unless the user is specifically authorized to do so?
- Does the NE environment offer adequate granularity such that, for a given resource, it becomes possible to grant or deny access to any given user and any given port?
- Does the NE environment have the capability to lock away potentially damaging commands (e.g., delete all translations, issue bogus SS7 messages to bring down the CCS network) from users who do not need to execute such commands?

With the introduction of the Telecommunications Act of 1996, competing service providers must be given nondiscriminatory access to NE resources. The security analysis should be extended to resolve how the confidentiality and integrity of one party's resources are protected from other parties.

5.1.5 Audit

The NE environment needs to have tools to generate an audit trail so that, if a security breach is suspected, an investigation can be made to establish whether or how the breach occurred. The security analysis consists of performing tests to answer questions such as:

- Does the NE environment maintain a history file (also called an *audit log*) that records all security-related events that are pertinent to establishing an audit trail for a *post mortem* analysis of a suspected security breech?
- Does the NE environment adequately protect the integrity of the audit log?
- Does the NE environment have the capability to generate customized audit reports, as required for establishing an audit trail?

5.1.6 Integrity

This feature deals with consistency and reliability issues associated with the NE data and software resources. It also includes maintaining an acceptable level of service if a security breach should occur. As such, the security analysis consists of performing tests to explore whether the NE environment can perform functions such as:

- Running integrity checks for system functions
- Verifying the integrity of data received from remote locations
- Retaining the security parameters after the occurrence of events such as a system restart or a disaster
- Providing the back-up capability to restore the system whenever necessary.

5.1.7 Confidentiality

Confidentiality is the assurance that sensitive information is communicated and stored in a way that protects it from unauthorized access. Examples of confidential information are passwords, files containing confidential data, and billing information. To preserve confidentiality, several cryptographic techniques are available, such as symmetric encryption, asymmetric encryption, and one-way encryption. Their deployment depends on the specifics of the application. Accordingly, the security analysis consists of performing tests to explore whether the NE environment supports acceptable and intended cryptographic techniques.

5.1.8 Security Administration

This feature entails proper activation, maintenance, and usage of the security features of the NE, to be conducted by a highly privileged and authorized security administrator. The administrator needs to perform functions such as overriding vendor-supplied defaults, keeping the security parameters up to date, monitoring suspected activities, and generating security audits when needed.

In order to facilitate the task of security administration, it is necessary that the administrator be able to perform these functions. In addition, the NE environment needs to generate alarms adequate to alert the administrator as to the actions to be taken. Security analysis consists of performing tests to explore whether the NE environment fulfills these requirements.

A security assessment at the level of security administration involves three steps:

1. Ascertaining the security features that are available on the NE, and determining their usage, value, and effectiveness
2. Comparing the NE’s security capabilities against the needs established by the NE security policy
3. Assessing the current security configuration.

5.1.8.1 Ascertaining the NE’s security features

Most NEs support some security features, though few, if any, support the complete suite described in the previous sections. The assessment should determine:

- Which security features are available on a given device
- The robustness of each feature
- The amount of control an administrator has over those features.

At the completion of this step, the assessors should know how each feature works, what its controls and parameter settings do, and how it can be used most effectively. This step may be necessary only during the installation and activation of the NE, although there may be instances where software updates necessitate repeating it.

5.1.8.2 Comparing against policy

This step compares the capabilities of the security features against the security requirements defined in the NE security policy, as follows:

1. All areas of compliance should be noted.
2. All areas of non-compliance should be noted. Two reasons for non-compliance exist:
   - The NE’s security features cannot satisfy the needs of the policy
   - The NE’s security features can satisfy the needs of the policy, but they are not in use or are not configured correctly.
3. The areas of non-compliance should be addressed.

The areas of non-compliance should be examined carefully to determine what types of vulnerabilities are left unmitigated by the deficiencies, what threats might arise because of them, and what alternatives are available to resolve these problems. This step is required whenever step 2 is performed. A feedback loop should be used to allow findings discovered during a review to alter or update the security policy.

5.1.8.3 Assessing the security configuration

This step should ascertain that:

- The security features are initialized to settings commensurate with the policy
- The features are maintained at a level of effectiveness that matches the security needs
- Access to the security features and their controls is highly protected and available only to authorized personnel
- Alterations in feature settings cause an audit record to be written to the security log, and, if required by the site, trigger an alarm to the security administrator.

This step should be repeated regularly since in the course of day-to-day operations the features can be turned off; settings can be altered due to real-time necessities, software upgrades, accidents, or malice; or security needs may change, necessitating updates of the security features.

5.1.9 Installation

Unless proper precautions are taken, an NE may be particularly vulnerable just after it is installed and put into service. The security analysis should determine that the NE environment offers adequate protection of the NE during installation time. For example, the following questions should be answered during a security analysis:

- During installation, are test procedures available to determine whether the delivered software is exactly as specified in the purchase contract and the master copy?
- Are there tools and procedures for verifying that a newly installed release contains the appropriate versions and levels of its component modules?
- Are all software changes documented and reviewed to ascertain that security has not been compromised?
- At the time of delivery and installation, is the NE environment configured with secure installation defaults?

5.2 Security Profile for the Call-Processing Interface

As stated earlier, if the call-processing interface is not adequately secured, it may be possible for an interloper to make fraudulent use of the telecommunications service provided. For example, it may be possible to complete a telephone call without creating a valid billable record. NEs such as the PBX, Voice Mail, and Automated attendant are vulnerable to such fraud. With the advent of Voice over Packet (VoP), potential opportunities may proliferate for the commission of such fraud. Security analysis consists of testing whether precautionary measures (such as those listed below) have been implemented for mitigating fraud:

- Does the interface maintain the confidentiality of information for which the caller is not authorized (for example, the PIN of an authorized caller)?
- Is the caller prevented from bypassing the service restrictions imposed on the user interface? (For example, if the interface is not entitled to a second dial tone, the caller should be denied use of that service.)
- Is the caller prevented from spoofing as another caller? (This is especially pertinent for calls generated over VoP.)
- Is there adequate protection against black box fraud[10]?

[10] Black Box fraud is committed when Customer Premises Equipment (CPE) is altered (i.e., tampered with) in such a way that it becomes possible to place a call to that CPE without the caller being billable.

6 OPERATIONS SUPPORT SYSTEMS

An Operations Support System (OSS) is a central computing environment that performs operations functions for one or more NEs that are remotely connected to it. OSSs are usually deployed on an Access Network (see Section 9). Examples of OSS functions include maintenance, testing, provisioning, and automatic message accounting (i.e., billing). To perform these functions, the OSS needs to establish a session with the NE and communicate with it to transmit appropriate messages and receive responses (including automated messages, such as alarms).

OSS security has two components: (1) security at the points of access to the OSS, and (2) security issues related to the OSS/NE interface.

6.1 Security for OSS Ingress

Typically an OSS allows three kinds of access

- Local access at the OSS console
- Remote dial-up access to the OSS
- Networked access over an Access Network.

To secure these access methods, the OSS needs to deploy the same security functions as those described in Section 5.1 above (i.e., identification, non-repudiation, authentication, etc.). Hence the corresponding methodology for security analysis is also very similar. To avoid duplication, these are omitted from this section. However, it should be stated that the Access Network on which any OSS is typically deployed is increasingly a TCP/IP network rather than an X.25 or other type of network. Hence the analysis should include tests to explore how the Access Network is protected from the typical vulnerabilities associated with the Internet. For example:

- Is the Access Network physically and logically isolated from other neighboring networks such as the Corporate Intranet and the public Internet?
- How is an Access Network based on TCP/IP protected from vulnerabilities such as Session Hijacking, Source Address Spoofing, Source Routing, Falsifying ICMP[11] Redirect messages, TCP Connection Spoofing, and UDP[12] spoofing?
- Have cryptographic techniques (e.g., IPsec, SSL3[13], TLS[14]) been deployed, and if so, are they providing adequate protection to the parties communicating across the Access Network? This is important if the Access Network serves several technologies (e.g., SONET, ATM, frame relay) simultaneously, and each is administered by different and possibly competitive staff. This is particularly germane if the Access Network has Internet connections.

[11] Internet Control Message Protocol.

[12] User Datagram Protocol.

[13] Secure Socket Layer, version 3

[14] Transport Layer Security

Depending on the extent of the Access Network, it may be appropriate to conduct a Network Access Review or Penetration Test against the Access Network to determine its resistance to attacks of this sort. Access Network security reviews are covered in more detail in Section 9.

6.2 Security Issues for the OSS/NE Interface

The OSS/NE interface refers to the communications link between the OSS and the NE and the protocols in place to support the communications. There are many types of OSSs performing a wide range of operations functions for numerous types of NEs. Consequently, there are numerous OSS/NE interfaces. These interfaces are logical extensions of the NE's operations interface and are subject to the same security controls used in the NE. The OSS/NE interface can be considered a subset of the larger set of communications required when an NE is controlled or managed by any device such as an element manager, OSS, remote administrator, or third party (e.g., the equipment vendor). This topic is discussed in Section 9, Access Networks, which addresses issues such as trust, authenticated and authorized use, and secure administration. There are, however, some security aspects of the OSS/NE interface that are separate from those of either the OSS or the Access Network:

- The interface between managed and managing devices should constitute a *trusted path*. If it does not, some other mechanism should be deployed to prevent intruders from subverting the interface.
- The OSS/NE interface should require authenticated communications. That is, when the OSS attempts to access some NE resource, the NE should challenge the OSS for its identifier and authenticator. If it cannot challenge the OSS, then the NE challenges should be passed through to the OSS user.
- The OSS should have authorization levels that allow appropriately authorized execution of all commands needed to secure the NE. This is especially pertinent if the NE is a broadband switch (such as an ATM), which may require special security-related commands such as "Lock out *all* local access to the NE."
- For OSSs that perform NE maintenance, automatic messages (such as alarms) generated by the NE should be received at the OSS in near real-time.
- The OSS should provide a near real-time alarm that monitors the communications link to the NE for loss of signal.
- If the interface between the NE and OSS uses a middleware technology such as Common Object Request Broker Architecture (CORBA[15]), the security features associated with the middleware should be activated.

When an OSS is deployed for NE access, other methods of remote access, such as modems, need to be severely restricted or prohibited. Since controlling direct access via modems remains problematic for most service providers (whether their policies permit it or not), it is often advisable to conduct a war dialing exercise as part of a program to ensure

[15] At present TMN has standardized CORBA for the service layer of the X-interface. However, there are plans to standardize CORBA for the OS/NE interface also.

that there are no unsecured modem entry points either to the Access Network or the NEs it supports. A description of how to conduct a war dialing exercise is included in Appendix D, Automated Attack Tools. Similarly, if the Access Network is TCP/IP-based, it is advisable to run vulnerability checking tools or to conduct penetration testing against any hosts or firewalls that have network connectivity. Procedures for conducting these are also provided in Appendix D.

7 Network Management Systems

Network management refers to the controls used to manage the individual network nodes within a network. This may cover switches, SSPs and SCPs within the voice network; STPs within the signaling network; and routers, cross-connect switches, and other intelligent, configurable nodes within the various management and Access Networks that support the PSN. Network management controls give access to the network nodes at a low level. They also give direct access to the operating parameters of the network, including performance, quality of service, path control, and many others.

Network management harbors one of the primary vulnerabilities for many networks because it is often relatively open, particularly if it allows Internet connectivity, which is becoming common. Network management vulnerabilities are not new: Almost all networks in operation today have network vulnerabilities that range from architectural to procedural. Furthermore, the management network's job has grown as multi-network control is consolidated, equipment becomes more intelligent, and the number of controllable nodes has increased. That is, a management network that used to access only PSN NEs may now provide access to SONET NEs, ATM switches, frame relay switches, and other network facilities. This *integrated network management* is a good way to control diverse networks and layered networks (e.g., ATM/SONET) by centralizing the management facilities and giving network managers a multi-layered view of the networks. However, it also offers a more significant target for intrusion since an attack on an integrated network management system can be widespread and can hit many networks.

There are three primary components of network management systems: the network manager, the managed objects, and the management protocol that conveys messages between the network manager and its managed nodes, and between the nodes themselves. All three must be given protection to prevent abuse through tampering at the management systems or the network nodes, or through the use of intelligent test equipment placed strategically along network paths.

Network manager: This is the most vital area for protection since an intruder who gains control of the network manager has control of the entire network. As stated earlier, this can be particularly serious if the management system gives access to many networks. The protection of the network management system is analogous to that of protecting operations support systems, which is covered in Section 6, Operations Support Systems.

Network nodes: The network nodes are the targets of an intrusion into the network management system, and should be protected as described in Section 5, Network Elements.

Management protocols: This term refers to protocols that define the format of the management messages and the nodes' capabilities to exchange and interpret those messages. Protocols can be arbitrarily divided into two types:

1. *Internal protocols* that allow the network nodes to communicate among themselves and between themselves and the network manager. Examples include SONET's TARP[16] and IP's ARP and RARP[17].
2. *External protocols* (for lack of a better term) that link the manager to the managed nodes, and which have broader scope than most internal protocols. The Simple Network Management Protocol (SNMP) and the Common Management Information Protocol (CMIP) are two examples of external protocols.

Current management protocols of both types often do not provide protection of management messages, which results in vulnerable messages that travel about the management network in clear text and are susceptible to attacks by intruders using protocol analyzers attached to the network.

If internal management protocols are in use, the analysis should examine their use, assess the ramifications of tampering, and determine whether the advantage of using them makes up for the risk of using them (value/risk ratio).

If network management is to be handled by existing protocols such as SNMP or CMIP, then the assessment should give them special attention, since these protocols provide little security, even in more recent versions. Rather, they seem to be based on a notion that all management messages can be trusted to come from authorized sources. The assessment should also evaluate their use, examine the ramifications of tampering, and determine a value/risk ratio.

From a protection standpoint, caution must be taken when building integrated network management systems because:

- Different network technologies have both overlapping and technology-specific controls, which can strain network managers' capabilities.
- Common controls may make unauthorized access easier.
- Competitors may co-manage networks, which may lead to conflicts of interest.
- Administrative boundaries may be more difficult to establish and maintain.
- Internet access for management of one layer may provide unintended access to others.
- A breakdown of the management facility or management network may affect all transport network layers.
- Unauthorized access to the management network increases the danger that all layers can be attacked.
- Weaknesses inherent in the management at one layer may open up other layers to mismanagement.

[16] *TARP* stands for *TID Address Resolution Protocol,* where *TID* itself is an acronym for *Target Identifier*.

[17] *ARP* and *RARP* stand for *Address Resolution Protocol* and *Reverse Address Resolution Protocol*, respectively.

An assessment of integrated network management systems must take these considerations into account. To do this, it should:

- Catalogue the various networks being managed, including the number of managed nodes and their geographic dispersal
- Determine whether the management community consists of trusted workers, competitive organizations, or outsourced personnel
- Determine strength of the network manager’s protective systems relative to the needs of the networks it manages, and using the security of OSSs as a model
- Assess the security measures in place on the managed nodes against security requirements in place for those nodes
- Take notice of the internal and external management protocols in use, and, at a minimum, raise awareness of their security strengths and weaknesses
- Examine any and all administrative boundaries for unintended openings and access into the management network
- Identify Internet access to any network layer or subset of the managed network, and determine whether such access can open unintended pathways to any other layers or subsets
- Assess the administrative policies that determine who can access the management network, ascertain that old or unused accounts are dealt with according to policy, and compare the access rights for each user with those necessary for that user’s job.

8 TRANSPORT

Transport refers to the internal (as opposed to external options such as the Internet) network communications paths connecting network components. Transport often refers to the physical layer media plus the low-level network technology (e.g., SONET) on which all other communications layers ride. The types of transport, and traffic they carry, include:

- Trunks – The subscriber call content transmission paths between switching systems. These are typically the telecommunications links between switches, as opposed to the links between switches and subscriber premises equipment (e.g., telephones).
- Signaling links – The signaling paths between and among switches, STPs, and SCPs
- Network Operations links – The command and control systems communication paths from the OSSs and their respective subscriber loop transmission systems, switches, signaling networks, and interoffice transmission facilities systems, such as multiplexing carrier systems.

Interoffice facilities are used to interconnect switches regardless of how many switching systems are in a wire center or the distance between the wire centers. In a multi-switch wire center, each switch is interconnected using trunks as if they were in separate wire centers.

Transport facilities can be threatened either logically or physically. Logical attacks, however, will usually be based on access to an NE or OSS, as described elsewhere in this guide. Physical attacks will involve access to specific transport media such as cables, cross connects, or fibers.

There are two ways of protecting against physical attacks:

1. Securing the premises where critical transport facilities are housed (e.g., cable vaults, conduit, distribution frames)
2. Providing redundant transport facilities for critical resources such a signaling links and interoffice trunks.

Both of these security measures should be evaluated as part of the physical security review of critical facilities (Section 4). It is particularly important to ensure that redundant transport facilities are geographically separated so that, for example, severing a fiber conduit does not eliminate connectivity on both of the redundant links.

The signaling links require special attention, since these links carry control information that can be attacked to cause widespread disruption of services carried over content transport networks such as the PSN. Access to signaling links either physically or logically (through an STP, for example) can allow an intruder to interject spurious messages that could be disruptive to the signaling network, the trunking network, or both.

9 ACCESS NETWORKS

Access Networks are data networks used to perform Operations, Administration, Maintenance, and Provisioning (OAM&P) functions on network elements. These functions include NE software updates, NE configuration for new service orders, performance monitoring, and the like. Usually, these functions are performed from a centrally located data center comprised of a LAN with data connections to the devices for which the Access Network and its applications have been designed. Often, access to network components is restricted to the Access Networks, although direct craft access, remote access through other NEs, and dial-up communications are common practices as well. Direct access to NEs via dial-up lines is generally considered to be bad practice, and is often a violation of company policies. Instead, there is dial-up access to the Access Network, which performs identification, authentication, authorization and auditing functions. Some service providers, however, may still use direct dial-up to NEs for some functions.

Access Networks include operations networks, management networks, remote access networks, and other networks that facilitate the operation of the associated transport networks. In Figure 1, the Access Network comprises the operations network and any other remote connectivity allowed through remote access servers for various other protocols. The enterprise network may also be used for access, as can any other networks that may be connected to it. Though these various networks may have different topologies, uses, and value, they have common security needs, which are covered in this section. The term *Access Networks* will be used in the remainder of this guide to refer to the various types of networks that provide OAM&P functions.

Increasingly, these networks are TCP/IP-based, since it simplifies maintenance and administration of the Access Network and leverages TCP/IP resources that companies have deployed to meet their other data communications need. Nevertheless, there are still legacy Access Networks based on protocols and technologies such as X.25 and Datakit®. Access Networks and the data that support them are often housed in facilities known as *data centers*. Examples of such data centers and networks include Network Signaling Control Centers, local Switch Control Centers (SCCs), Emergency Switch Assistance Centers (ESACs), and Network Operations Centers (NOCs)[18].

Since the Access Networks are critical to the operation of the portion of the PSN that they oversee, the security assessment should review:

- The architecture of the Access Network
- Access mechanisms
- Operating systems and applications
- Security administration.

[18] A Network Operations Center is a centralized location from which the overall health of portions of the network can be monitored and remedies applied for any emergent problems of performance, congestion, traffic loading, or equipment malfunction.

Each of these areas is important since together they comprise the network management body. A compromise of the Access Network is tantamount to compromise or takeover of the subtending PSN components.

In addition to these general concerns, there may be a need to review other access mechanisms that protect specific functions. These miscellaneous concerns are covered at the end of the section.

Note that reviewing an Access Network is no different than reviewing any data communications network, except that the security requirements may be more rigorous due to the nature of the assets being protected.

9.1 Architecture Review

An Access Network security assessment should begin at the highest and most abstract levels in order to determine whether basic security needs have been incorporated into the network design, and whether security features are considered both necessary and sufficient. It must also verify that the network design is capable of supporting needed security features (a detail that is overlooked surprisingly often). The actual network architecture and topology are considered the best representation of the plan upon which the network is based. Furthermore, the architecture is a useful reference both before and after the network design is completed and implemented, since it provides insights into the key decisions made at network inception. A network architecture assessment must include:

- Identifying potential vulnerabilities in the architecture design or network topology. The review should identify whether the Access Network is sufficiently isolated from more general data network capabilities such as the corporate enterprise network and the Internet[19].
- Identifying single points of failure as part of an assessment of the overall reliability and redundancy of the Access Network
- Assessing audit and notification capabilities of the network and hosts residing on it
- Assessing data storage security measures. For example, critical data should be stored off site in a secure facility as well as at the data center in the event of need.
- Assessing backup and recovery mechanisms. For example, switch images should be “reload tested” to ensure that switch configurations can be restored in the event of a catastrophic failure.
- Evaluating the appropriateness of protocols and services running on the network. That is, unnecessary protocols and services (e.g., ICMP echo, ping, ftp) should be disabled or severely restricted.

[19] Although companies are planning Internet connections for operations purposes, and some may be using them today, security experts may be hard-pressed to endorse such a move, particularly in light of the sometimes serious and highly visible attacks suffered by online businesses.

- Checking (and possibly correcting) the configuration of the protocols and services (e.g., SMTP[20], HTTP[21]) that are required for day-to-day functioning of the network and staff who use them
- Examining the configuration of the security mechanisms, including security monitoring, auditing, and intrusion detection on both the network itself and hosts resident on the network
- Evaluating security administration, maintenance, documentation, and training. For example, checking that audit logs are periodically reviewed and ensuring that security documentation is up to date, complete, and readily available in data centers.
- Analyzing security mechanisms and policies in place for the network (e.g., use of modems, adequacy of firewalls). Much of this pertains to the review of access mechanisms discussed below.

9.2 Access Mechanism Review

On a day-to-day basis, most access to the Access Network may be through consoles located at the data center. Thus, there will be the additional security afforded by physical security mechanisms in place on the premises. Even then, however, access policies such as requiring unique login IDs and tables of authorities for different kinds of access (e.g., administrative authority, read-only capability) should be checked.

In addition to local access procedures, however, it will often be necessary for personnel to access the Access Networks from remote locations. Examples include craft access from the field and vendor access for software upgrades and diagnostic testing in the event of a fault. For remote access to the Access Network:

- Authentication and Identification techniques should be assessed for adequacy. Generally, strong authentication techniques such as token identifiers or Secure Socket Layer (SSL) should be used for external connections. For local access, a review of login and password requirements is usually performed.
- Authorization classifications should be reviewed. That is, there should be methods of authorization for individuals such that their actions are restricted to what they need to perform their jobs. Sometimes these authorizations will be effected through a centralized mechanism (e.g., Access Control Lists, RACF[22]), and sometimes they may be resident on the NEs themselves (e.g., Privilege Classes for switch accounts).
- Procedures should be in place for disabling user accounts when they are no longer needed.

[20] Simple Mail Transfer Program.

[21] Hypertext Transfer Protocol.

[22] Resource Access Control Facility (RACF) is one of IBM’s major access control mechanisms for mainframe computing platforms.

- Firewalls, or other perimeter defenses (e.g., one-time password devices) should be reviewed for appropriate configuration. This may include a penetration test in addition to a review of firewall policies.
- Warning banners should be displayed for all access.

9.3 Operating System Review

Operating systems (e.g., Windows NT, UNIX, MVS) supporting the Access Network (i.e., within the OSSs, NEs, element managers) should be reviewed for vulnerabilities. It may not be necessary to analyze each system if a sample of systems can be assessed. This assessment usually provides a baseline for the level of security, which can be cautiously extrapolated to a larger set of systems if common management practices are in use, and if the larger set contains no anomalous nodes, specialized applications, or atypical operating systems.

The operating system security analysis must take the following items into account:

- Change management and procedures for installation of the most recent security patches
- File and directory permissions
- Default settings of security features
- Configuration files (e.g., shell, network, default)
- Password robustness
- The use of guest and anonymous accounts
- Privileged accounts (e.g., administrator and root)
- Remote trust accounts
- Use of protocols having minimal or no security.

In addition, a full security assessment must take into account applications resident on the Access Network machines, particularly those applications having known vulnerabilities or a history of abuse by attackers. Applications supporting services such as electronic mail, DNS[23], network management, and file transfer should be examined for vulnerability to known attacks, correct installation of “fixes” to security problems, and appropriate use of security features, defaults, and settings. Application assessments are highly system-dependent and are more appropriately covered in computer security assessment guides or textbooks devoted to the topic than here.

9.4 Security Administration Review

Security administration refers to that aspect of administration concerned with overseeing and maintaining the security features of the managing and managed devices. Examples

[23] Domain Name Services

include controlling access rights to these devices, granting access rights to personnel, removing and modifying those rights according to procedures and policies, and maintaining *secure* administrative capabilities.

Security administration should, at a minimum, perform these functions:

- It should control the identification and authentication (I&A) methods that govern access to NEs and OSSs. This includes establishing user[24] accounts, removing them, supporting them, and establishing parameters and settings that constrain them (such as password complexity rules and expiration intervals).
- It should manage access control rights to devices and the data and applications resident on them. Access control includes I&A processes as well as the resource permissions for files and applications (at a level of granularity commensurate with security requirements governing the protection of information and other resources).
- It should administer the security audit trails. This includes turning them on and off, setting the desired traps to catch data sufficient for investigation of problems, collating and analyzing them, storing and archiving them, protecting them in such a way that their validity cannot be called into question should they be needed as evidence in legal cases.
- It should generate security audits in response to intrusions, infractions of security policies and procedures, and requests from management or corporate security.
- It should manage and ensure appropriate back-up procedures, perhaps in coordination with personnel whose job functions include back-up and archive maintenance.
- It should manage the security database, which involves keeping security data up to date. Security data includes security parameters, such as audit trail settings, password timeout settings, and access control lists.
- It should reset all vendor-supplied defaults on new equipment to settings commensurate with site requirements.

An assessment of security administration should address the following questions:

- Do the managed devices support security administration functions, a capability to separate those functions from all other onboard functions, and the capacity to reserve those functions for administrators only?
- Is the security administration function reserved only for authorized administrators who have been identified and their authorization documented?
- Can the security administrator monitor the activities of all users logged on to any or all managed devices?

[24] In this context, the term *user* refers a person, a process, or a system that requests a session with the NE or OSS to perform an operations-related task such as administration, maintenance, provisioning, and testing. It does not refer to the end users of the NE’s services (e.g., telephone callers).

- Can the security administrator authorize and revoke users' access privileges, and is the administrator the only one allowed to do so?
- Can the security administrator manage all security-related features and parameters on the managed devices?
- Does the security administrator periodically validate the security features (e.g., audit logs, access control lists) of all managed devices? Are the results of these validation checks and any resultant actions recorded officially?
- Can the security administrator access all audit data needed to generate a security audit on one or many managed devices?
- Can all security administration functions be performed in a secure manner? That is, is the security administration function itself a secure function that does not leak information about security parameter settings, security-related user information, security-related information on managed devices, features in operation, and ongoing security audits?
- Are all management tools and protocols (e.g., SNMP, CMIP) configured for high security and operated securely? In cases where the management protocol may not meet local requirements for secure configuration and management, has additional security been put into place and is it used?
- Have all vendor-supplied default security parameters been reinitialized to more secure settings on all managed devices **and** on the security management platform (if it is vendor-supplied)?
- Is there an active procedure for backing up security settings for all managed devices and for the security management platform? In addition, does the security management platform itself have a warm back-up in place if it should fail?
- Is all security audit data archived in a manner sufficiently secure for it to be useful as evidence in legal proceedings? Is there an optional capability to encrypt security audit data?
- Does the security administration function provide the capability to remove an administrator from the security administrative position without having to reset all administrative passwords on all managed devices? How is this capability implemented?
- Are contingency plans in place if a system administrator is unexpectedly unavailable?
- Are the system administrators restricted from independently performing critical commands that may disable a critical operation or modify critical data? Are adequate controls, backups, and audit trails in place to track usage of critical commands?
- Does an independent group ensure that the system administrators are performing their responsibilities, as defined in the policies and procedures, through a periodic audit?

Ideally, removing an administrator's privileges should be as easy as deleting his user-ID and password. However, if the administrative function is not set up to allow for administrative staff changes, the consequences of such changes could be that all administrative passwords on all managed devices may need to changed. This could be costly, inconvenient, fraught with error—and done all over again in six months. If the administrative accounts on managed devices were accessible only from the security administration function, the problem would be simple in its resolution. However, that is rarely so. Most major devices (e.g., NEs) are equipped with maintenance ports, consoles, remote access facilities, and other means of ingress that permit direct communication, including administrative access for those who know the user-ID and password. Keeping a former security administrator from accessing managed devices directly or remotely may be difficult unless this contingency has been planned for and built into the security administration function. It is a critical point that (one may hope) was carefully weighed and addressed at the time the security architecture was implemented.

9.5 Miscellaneous Concerns

In addition to internal access required for day-to-day OAM&P functions, there may be business or regulatory reasons for opening up the Access Network to external parties. This includes access for other communications service providers or business partners who resell and manage communications services or facilities, vendors who perform remote diagnostics and software upgrades or configuration changes for network devices, customer access for customer configurable products and services, and law enforcement access for criminal investigations. Access by these third party interests will be governed by general policies and procedures on Access Networks, but should be inspected to ensure that there are adequate controls to prevent compromises of the core network.

9.5.1 Business Partner, Reseller and Vendor Access

When other companies (e.g., CLECs) offer services using the company’s facilities, they will often need administrative access to NEs or other devices and data. This raises the concern of administrative control across domain boundaries and the corresponding cooperation required by the parties involved. This sort of cooperation may involve connection of two or more management networks (the reasons being unimportant to this discussion) at a network boundary. Unless the corporations that support the networks always work together administratively, trust each other, and are respectful of the boundary, provisions need to be in place to control or restrict activity across it. The simplest solution (and the one most often used today) is to forbid communications at the boundary, but regulatory, legislative, and competitive pressure may someday rule that out as impractical or undesirable. Security administration needs to include a plan to address administrative control at domain boundaries, to adopt policies and guidelines that will aid in restricting such access as necessary, and to implement solutions that enforce those policies. These efforts may also be germane to some collocation issues.

Often, third party access of this sort is governed by mutually agreed upon Data Communications Agreements (DCAs) that enumerate mutual responsibilities and rights of inspection for the participating companies.

9.5.2 Customer Access

While most remote access to the operations network are by operations support personnel (either vendors or staff), in some cases customers may require access to selected data or

NEs for self provisioning of services or configuration changes. For remote customer access, it is important to assess the adequacy of security measure that are in place to prevent customer access to either restricted operations functions and facilities or to other customers' data. The nature of the assessment will depend on the kind of access provided.

9.5.3 Law Enforcement Access

In October 1994, the Communications Assistance for Law Enforcement Act (CALEA) was passed by Congress. The Act was designed to assist law enforcement personnel in conducting electronic surveillance. In the Act, electronic surveillance is defined as "both the interception of communications content (wiretapping) and the acquisition of call-identifying information (dialed-number information) through the use of pen register devices and through traps and traces." CALEA requires telecommunications carriers to modify and design their equipment, facilities, and services to allow authorized electronic surveillance.[25]

Congress passed CALEA to preserve law enforcement's capabilities to carry out authorized electronic surveillance despite technological advances in telecommunications that threaten their ability to intercept communications. CALEA requires the service providers "to modify and design their equipment, facilities, and services" to support this capability.

The predominant issue with CALEA is one of privacy, in terms of both authorized and unauthorized access to subscriber information and conversations. From the standpoint of authorized access, CALEA addresses protection of data through due process of law. For unauthorized access, the question is one of protecting the surveillance points on the switch, which can be handled by general network and device security mechanisms. Thus, while CALEA mandates access for law enforcement purposes, the security concerns that it introduces are not substantially different from those that providers should be considering for other purposes and which are covered elsewhere in this guide. Nevertheless, a review of CALEA-based mechanisms may be appropriate if there is reason to believe that their implementation may allow other forms of potentially damaging access.

[25] From the Notice Of Proposed Rulemaking, *In the Matter of: Communications Assistance for Law Enforcement Act* , CC Docket No. 97-213, adopted on October 2, 1997, and released on October 10, 1997.

10 DOCUMENTATION AND PRESENTATION

Once the security assessment is complete, it is important to document the findings in a concise and useful way. This includes detailed technical documentation that is meant to help security and system administrators and their immediate management understand the nature of the findings and establish appropriate strategies for fixing or mitigating any problems that were discovered. In addition, it is usually helpful to prepare a high-level abstraction of the findings that can be used to inform executives with security responsibility of the nature and relative severity of the findings. The aim in both types of documentation is to help the individuals responsible for security prioritize and address the findings quickly, effectively, and at lowest cost.

The detailed technical findings report should be provided in draft form to any Subject Matter Experts (SMEs) familiar with the day-to-day functions and operations of the entities reviewed. This allows the SMEs to contribute additional information or context for any of the findings, and to correct or elaborate on any errors, misconceptions, or mitigating circumstances that should be considered before the findings are finalized. This also gives the SMEs an opportunity to contribute to the overall conduct of the review, fosters cooperation, and helps validate that the review is meant to improve processes and procedures rather than allocate blame. With this in mind, it is important to remember at this point that the entire review should be framed as a learning exercise rather than a finger-pointing activity.

10.1 Categorizing Findings

Findings should be ranked with respect to the level of risk, threat, and inherent vulnerability that the reviewers believe they entail. A good practice is to use a categorization scheme such as the one outlined here:

- **Exposures** are the most critical findings, posing an immediate risk to the security of the company's assets, and should be addressed first. This is particularly true if the threat to the asset is perceived to be high and the asset is resident on domains with high inherent vulnerability.
- **Concerns** are findings that pose medium to low risk to assets, and need to be addressed in a timely manner.
- **Informational issues** are concerns that need to be noted and should be acted upon at a later date, but do not pose a clear and immediate risk to assets.

Categories such as these allow management to allocate resources appropriately to get the most benefit from available money and staffing.

10.2 Addressing the Findings

All findings should be addressed from both a technical and business perspective. The review results should foster an understanding of both the technical environment that contributes to any finding and the technical solution alternatives that can be applied to mitigate any flaws. Where possible, both preferred and alternative technical solutions should be presented to allow implementers to determine the most appropriate solution set for the company given the available resources, expertise, and any relevant current corporate plans or strategies.

10.3 Informing Management

Including information in the review about the potential repercussions to the business should any assets be compromised is important for “socializing” the results to management. The review is only useful if it is effective in getting management to allocate necessary resources to implement the security controls needed to protect their business objectives or to meet regulatory obligations. Any high-priority vulnerabilities or risks should be reported to appropriate management for immediate action.

Management can be informed either through an Executive Summary of the findings or a short presentation stressing the most important flaws and plausible business impacts that could result if they are not resolved. In either case, the management presentation must be short and concise, and must emphasize potential business impacts.

11 SUMMARY

The security assessment methodology presented here provides an overview of the security assessments that should be a pervasive part of any deployed Public Switched Network. The methodology derives from a variety of sources, including security standards, generic security requirements, generally accepted security practices, and knowledge of security vulnerabilities that have been exploited in the past.

It is difficult, at best, to exhaustively list everything that should be assessed across every different type of network and network-resident device. In practice, it will be necessary to apply additional network-specific knowledge to the assessment to gain a complete understanding of any network's security stature. This is particularly true for an assessment of vulnerabilities that are specific to any particular network technology (e.g., equipment from different vendors, varying network protocols, applications resident on the Access Networks). While the details will differ among networks, the methodology described here covers the types of security functions that will necessarily be a part of any implementation. Further, there are many aspects of the security environment that are common across implementations (e.g., authentication and authorization principles, physical security, policy formulations).

The methodology is intended to form a baseline for guiding development of a security assessment of a typical PSN, and will likely evolve and change with the capabilities and technologies of emerging networks.

Bibliography

The following list contains documents that provide basic or essential information on telecommunications network security or that define or include requirements, recommendations, and guidelines considered important for telecommunications network security. Except as indicated these documents are all non-proprietary and publicly available.

This list is not intended as an exhaustive catalog of security documents. Rather, it is intended as a representative sample of the available documents. Furthermore, it contains those documents deemed most comprehensive and relevant to the PSN, its operations, and its supporting Access Networks. The NIST Web site 'www.nist.gov' contains current and relevant sources on the subject of information systems security and Common Criteria. There are also numerous Security Associations that are a good source of information and training in the area of information security.

Information Security Forum (formerly European Security Forum)

Windows NT Security Checklist, Version 1
Available to Forum members only.
June 1997

Contact: www.securityforum.org
+44 (171) 213 1745

Federal Reserve Bank

Sound Practices Guidance on Information Security.
by Federal Reserve Bank of New York.
September 1997.

NCS

Public Switched Network Best Practices Security Primer
by the National Communication System
December 1998.

NCSC-TG-001, version 2

A Guide to Understanding Audit in Trusted Systems
by the National Computer Security Center
June 1988

NIST Internal Report 5153

Minimum Security Requirements for Multi-User Operating Systems.
By David Ferraiolo, Nickilyn Lynch, Patricia Toth, David Chizmadia, Michael Ressler, Roberta Medlock, and Sarah Weinberg.
March 1993

NIST Special Publication 800-7

Security in Open Systems
by R. Bagwell, J. Barkley, L. Carnahan, S. Chang, R. Kuhn, P. Markovitz, A. Nakassis, K. Olsen, M. Ransom, and J. Wack
July 1994

NIST Special Publication 800-11

The Impact of the FCC's Open Network Architecture on NS/EP Telecommunications Security
by Karen Olsen and John Tebbutt
February 1995

NIST Special Publication 800-13
Telecommunications Security Guidelines for Telecommunications Management Network
by John Kimmins, Charles Dinkel, and Dale Walters
October 1995

NIST Special Publication 800-14
Generally Accepted Principles and Practices for Securing Information Technology Systems
by Marianne Swanson and Barbara Guttman
September 1996

Bellcore[26]
GR-815-CORE
Generic Requirements for Network Element/Network System (NE/NS) Security
by Ranendra Bhattacharyya
December 1997

Bellcore[26]
GR-1253-CORE
Generic Requirements for Operations Interfaces Using OSI Tools: Telecommunications Management Network Security Administration
Moshe Rosenblit, contact
June 1995

Bellcore[26]
GR-1332-CORE
Generic Requirements for Data Communication Network Security
by John Kimmins and Thomas Meddaugh
April 1996

Bellcore[26]
GR-1469-CORE
Generic Requirements on Security for OSI-Based Telecommunications Management Network Interfaces
Moshe Rosenblit, contact
September 1994

Bellcore[26]
GR-1194
Bellcore Operations Systems Security Requirements
by John F. Kimmins
December 1998

Telcordia Technologies
FR-2063
Network Equipment-Building System (NEBS) Family of Requirements (NEBSFR)
Issue 000, March 2000

[26] Documents produced by Bellcore are now obtainable only from Telcordia Technologies, Inc. These documents were written before Bellcore was transformed into Telcordia Technologies. Once Telcordia updates or otherwise revises these documents, they will be referenced only by the Telcordia name and document numbers, and will no longer be obtainable under the Bellcore name or by the Bellcore document number.

Appendix A: RISK ASSESSMENT METHODOLOGY

The following form can be used as an aid for conducting the risk assessment described in Section 2. Each network service or information asset (including physical network components such as switches and databases) should be identified. The physical location of assets should be included where possible to provide input to the decision on which physical facilities should be reviewed. For each asset, a value, threat potential and inherent vulnerability ranking of high, medium or low should be assigned. These rankings are then used to assign similar rankings of risk. High-risk assets should be slated for review, as should any physical facility that houses a high-risk asset.

A.1 Risk Analysis

Asset	Location	Value	Threat Potential	Inherent Vulnerability	Risk

A.2 Assets for Review

Based on the risk analysis, list the assets that should be reviewed in descending order of importance. Include the asset, the physical location and logical environment of the asset (i.e., network domain where the asset is resident), and any ancillary systems needed to support the asset (e.g., systems or domains providing OAM&P functions for the asset). Network domains and physical facilities hosting high-risk assets should be reviewed along with the asset itself. In addition, any relevant corporate security policies that apply to the assets should be identified both for review of the policies and as reference materials for the asset review.

Asset	Physical Location	Network Domain	Ancillary Systems	Relevant Policies

Appendix B: POLICY AND PROCEDURES CHECKLISTS

Note that, in most cases, the policy and procedure reviews are intended to ascertain the existence of policies and procedures necessary for the business under review. The completeness, adequacy, and appropriateness of the security measures in place to implement the policies and procedures are addressed during later stages of the review. Reviewers should reference the policy and procedure documents later in the review process to assess adequacy and enforcement. The checklists below can be used to document the findings of the policy review. Any question that is answered "No" should include descriptions of what led the reviewer to make that judgment. Note that questions in these and subsequent checklists are phrased so that a "No" response indicates that remedial action may be required in that area.

B.1 General Security Policy

General Security Policy	Yes	No	Comments
Is there a security policy?			
Is there a justification or motivation for the policy?			
Has a responsible individual or organization been identified for maintaining and administering the policy?			
Are procedures in place for modifying the policy?			
Are there procedures for appealing policy restrictions?			
Does the policy include requirements that employees be made aware of their responsibilities under the policy? If so, is a responsible party identified for ensuring that policies are made available to employees?			
Are disciplinary measures defined for violations of the policies?			

B.2 Intrusion Response Policy

Intrusion Response Policy	Yes	No	Comments
Does an Intrusion Response policy exist? If so, complete the rest of this checklist.			
Is the justification or motivation for the policy clearly stated in its documentation?			
Is an intrusion response procedure in place for dealing with intrusions or other security incidents?			
Does the company monitor external information sources on vulnerabilities and incidents?			
Is there a single point of contact for reporting security incidents or obtaining incident response information?			
Is there a method for making appropriate system administrators aware of incidents or potential vulnerabilities?			
Is there a process for ensuring that recommendations developed as a result of a security incident are appropriately executed?			
Is there a method for making employees aware of potential vulnerabilities?			

B.3 Personnel Security Policy

Personnel Policy	Yes	No	Comments
Does a Personnel policy exist? If so, complete the rest of this checklist.			
Does the policy document include sufficient justification or motivation for the policy?			
Does the policy include requirements for a security awareness briefing to new employees on the implications of security breaches?			
Does the policy explicitly prohibit hiring of known criminals or “hackers” for sensitive positions?			
Are there background checks for personnel in critical or sensitive positions? If yes: • Is the “critical personnel” concept well defined? • Are the background checks sufficient to ensure that critical personnel are unlikely to have criminal backgrounds?			
Does the policy explicitly state that contracted services organizations provide assurances commensurate with corporate guidelines?			
Does the policy include descriptions of corporate and employee responsibilities for securing and protecting corporate assets?			

Personnel Policy	Yes	No	Comments
Does the policy include a code of conduct and ethics as it pertains to security?			
Does the policy include disciplinary practices for violations?			
Does the policy include obligations of former employees for protecting corporate assets? If so, does it include coverage of the specific types of assets for which it applies, the duration of any restrictions, and the corporation's legal recourse should a violation occur?			
Does the policy include requirements for reporting misconduct?			
Does the policy contain guidelines for personal use of corporate resources?			
Does the policy include requirements for cooperating with guards and other security personnel?			
If appropriate, does the policy include requirements for: • Drug testing • Conflicts of interest • Polygraph tests • Hiring of foreign nationals • Government security clearances?			

B.4 Information Publishing and Distribution Security Policy

Information Publishing and Distribution Policy	Yes	No	Comments
Does an information distribution and publishing policy exist? If so, complete the rest of this checklist.			
Does the policy document include sufficient justification or motivation for the policy?			
Are criteria for categorizing information as sensitive clearly defined?			
Are there clearly defined labeling standards for the information sensitivity categories?			
Are the types of information (e.g., documents, customer records) and media (e.g., electronic, written, photographs) that fall under the policy defined?			
Is responsibility for applying the categories and labeling conventions clearly and appropriately assigned?			
Is there a policy for restricting distribution of sensitive material on a need-to-know basis?			
Is there a procedure in place for changing the sensitivity category of information?			
Are there guidelines and appropriate technology (e.g., encryption standards, access control mechanisms) in place for secure distribution of restricted materials?			
Is there a document retention policy?			

Information Publishing and Distribution Policy	Yes	No	Comments
Is there a process for clearing information for public release?			
Are there standards for use of branded, copyrighted, trademarked, and service marked information?			
Are there policies for handling of third party information (e.g., client information, information covered by non-disclosure agreements, contract information)?			
Are there policies for protecting information from disclosure in public places (e.g., restaurants)?			
Are there policies for securing restricted information when not in use (e.g., storage in offices)?			
Are disciplinary measures for infringements described?			
Are there any additional policies related to information security? If so, describe them.			

B.5 Physical Security Policy

Physical Security Policy	Yes	No	Comments
Is there a physical security policy?			
Does the policy document include sufficient justification or motivation for the policy?			
Does the policy cover systems used to control initial access to a building, including guidelines or requirements for: • locks • guards • employee identifiers • key inventory and auditing • employee vehicle identification?			
Does the policy include requirements for segregation of critical corporate assets (e.g., switches, data centers, cable vaults) from more general-purpose areas of the facility?			
Does the policy define procedures to restrict access to critical facilities to persons whose job functions require it?			
Does the policy include guidelines for protection of building services, including: • power and water sources			

Physical Security Policy	Yes	No	Comments
- waste disposal (particularly disposal of sensitive or proprietary information) - emergency response procedures - fire protection?			
Does the policy define procedures for identifying any environmental or geographical threats peculiar to the location of the facility? If so, does the policy require measures to protect against these threats?			
Does the policy include requirements for contingency plans that provide computing and data services in the event of a disaster? If so, do the requirements include: - Schedules for regularly backing up critical data? - Provisions for off-site storage of back-ups? - Provisions for data and services continuity (i.e. switching operations to a temporary site)? - Procedures for permanent relocation of lost functionality?			
Does the policy include provisions for testing the contingency plans?			
Have there been any recent regulatory, business or technology changes that affect physical security (e.g., mergers, collocation)?			

Physical Security Policy	Yes	No	Comments
If so, does the policy include measures to address the new concerns?			
Are there any additional physical security policies? If so, describe them.			

B.6 Network Element Security Policy

Network Element Policy	Yes	No	Comments
Is there a network element policy? If so, complete the rest of this checklist.			
Does the policy document include sufficient justification or motivation for the policy?			
Does the policy include physical security requirements for facilities housing NEs? (These may be under physical security policy.)			
Does the NE policy include access control requirements, including: • User ID/password policies • Remote access policies • Policies on enterprise network interconnectivity • Policies for authorization hierarchies?			
Are there auditing requirements?			
Are there policies for preventing and detecting modifications to NE software and configurations?			
Are there policies for protecting information stored on the NE?			
Is there a security administration policy for NEs?			
Are there security documentation and installation policies?			

Network Element Policy	Yes	No	Comments
Are there policies for fraud detection and prevention?			
Are there any additional NE-related policies? If so, describe them.			

B.7 Operations Support System Security Policy

The important elements of an OSS security policy may be included in the NE policy, Access Network policy, or both, and may not exist as a separate policy statement.

Operations Support System (OSS) Policy	Yes	No	Comments
Does an OSS policy exist? If so, complete the rest of this checklist.			
Does the policy document include sufficient justification or motivation for the policy?			
Is there a policy requiring isolation of OSSs from general network resources?			
Is there a policy restricting access to OSSs on an as-needed basis?			
Is there a policy requiring all Network Element access to be mediated by an OSS?			
Are there policies prohibiting deployment of software not needed for OSS functions on the OSS LAN?			
Are there other OSS-related security policies? If so, describe them.			

B.8 Network Management System Policy

These policies may not exist separately from OSS, NE and Access Network policies. However, if the company uses network management tools and protocols, their use should be evaluated against existing policy statements for potential vulnerabilities or exposures they may introduce into the network.

Network Management System Policy	Yes	No	Comments
Does a Network Management System policy exist? If so, complete the rest of this checklist.			
Does the policy document include sufficient justification or motivation for the policy?			
Does the policy identify elements and systems for which network management tools are appropriate?			
Do the policies and procedures identify allowable network management products and protocols?			
Is there a policy requiring isolation of the network management system from general network resources?			
Is there a policy restricting access to network management systems on an as-needed basis?			
Is the network management system implemented in such a way as to enforce other general OSS and NE security policies and requirements?			
Are there other network management-related security policies? If so, describe them.			

B.9 Transport Security Policy

Transport security issues are special cases of physical, Access Network, and NE security and may not exist as a separate policy statement.

Transport Security Policy	Yes	No	Comments
Does a transport security policy exist? If so, complete the rest of this checklist.			
Does the policy document include sufficient justification or motivation for the policy?			
Does the policy include guidelines for ensuring safe transport routing?			
Are there criteria for redundant routing and a requirement that redundant routes be geographically separate?			
Are there requirements for protecting outside plant, including: • Rules that define ways of posting rights of way, to reduce digging accidents • Rules that define ways of concealing the routes of critical transport?			
Are there policies for protecting premises where transport facilities are potentially exposed (e.g., cable vaults, distribution frames)?			
Are there policies for protecting sensitive transport facilities (e.g., military communications)?			

Transport Security Policy	Yes	No	Comments
Are there criteria for determining the level of protection required for transport NEs?			
Are there policies for secure operations access to transport NEs?			
Are there other transport-related security policies? If so, describe them.			

B.10 Access Network Security Policy

Access Network Policy	Yes	No	Comments
Does an Access Network policy exist? If so, complete the rest of this checklist.			
Does the policy document include sufficient justification or motivation for the policy?			
Access Network Architecture			
Does the policy include requirements for isolating the Access Networks from other data networks in the organization?			
Does the policy require that critical functions be implemented for high availability?			
For critical functions, does the policy specify requirements for: • auditing • system and data backup procedures • recovery mechanisms?			
Does the policy restrict services and protocols on the network to those required for network functionality?			
Does the policy include requirements for: • security monitoring			

Access Network Policy	Yes	No	Comments
• auditing • intrusion detection?			
Does the policy include requirements for security: • administration • maintenance • documentation • training?			
Access Policies			
Does the policy specify: • who (in terms of roles and responsibilities) should be granted access to the network • restrictions on locations from which access is allowed • procedures for disabling unused accounts?			
Does the policy specify identification and authentication techniques used for the different types of access allowed?			
Does the policy require authorization restrictions based on job function?			
Does the policy specify whether or not direct access via dial-up lines or modems is allowed? If such access is allowed, does the policy require security measures for such access?			

Access Network Policy	Yes	No	Comments
Software Policies			
Does the policy restrict software on the Access Network to that required for day-to-day functionality?			
Does the policy specify minimum required security features for software on the network?			
Does the policy include processes and procedures for obtaining approval to deploy software?			
Does the policy include software change management procedures?			
Security Administration			
Does the policy define an independent role for a security administrator?			
Do the security administrator's roles and responsibilities include: • overseeing and maintaining security features of software and devices resident on the network • administrating the security of user accounts • managing authorization levels for users and devices • maintaining and monitoring audit logs?			

B.11 Security Awareness Program

There may or may not be an explicit policy for a Security Awareness Program. The important points of a program, however, should be covered somewhere in the policy statements.

Security Awareness Program	Yes	No	Comments
Is there a security awareness program for employees? If so, complete the rest of this checklist.			
Is the importance of security awareness explained and justified in program materials?			
Are there security awareness materials for new employees? If so, are there separate materials for different target groups (e.g., security administrators, programmers)?			
Does the corporation offer a spectrum of security-related courses to its employees? If so, are there requirements for ongoing security training?			
Is security awareness material generally available from a central location? In particular, are security policies and procedures accessible to those who need them?			
Is there an ongoing program that provides periodic reminders of general security issues? Are there programs in place to deal with specific security issues as they arise?			

Appendix C: Security Review Checklists

The checklists below have been designed to help ensure completeness of all aspects of the security review, other than the policy and procedure review, where an on-site inspection of implemented security practices and procedures can reasonably be conducted. The policy review can be used as reference to ensure that documented policies and procedures have been appropriately implemented. Conversely, the reviews can identify measures that have been deployed but that are not documented as part of the security policy. As with the policy checklists, any question answered "No" should include clarifying comments, and should be identified in the review report if they require corrective actions (some may not be relevant). As with the policy checklists, the questions in these checklists are phrased so that a "No" indicates that a feature, mechanism, or condition does not exist or is inappropriate and needs attention.

These checklists are necessarily general in nature. Specific security measures in place will depend on the systems or installations under review, and will require elaboration to reflect the security feature set available on any device or system.

Checklists are included for reviews of physical security, network element security, and access network security. There is no separate checklist for OSS security or transport security, since applicable assessment components are covered in other checklists.

C.1 Physical Security

The physical security review should be conducted on all facilities hosting high-risk assets. It is often advisable to prioritize the facilities according to the number or importance of the assets they contain and to begin the assessment with high-priority facilities. This will help to identify strengths and weaknesses of the security measures used for the most important facilities. These findings can be used to guide additional physical reviews, allowing the reviewers to focus on specific areas where weaknesses were observed, and reducing the time needed to review additional facilities.

Physical Security Review	Yes	No	Comments
Physical Premises Security: General			
Does the building have any perimeter defenses (e.g., fences, external monitoring devices)?			
Does the building have potential access points other than			

Physical Security Review	Yes	No	Comments
ground-level doors (e.g., ventilation systems, roof access)?			
Are doors installed so they cannot be removed from the outside?			
Physical Premises Security: Guards, Locks, and Badges			
Are all doors locked, guarded, or equipped with other access control mechanisms (e.g., proximity card access) at all times?			
Are main doors guarded during periods of peak access?			
Are guards adequately trained to challenge credentials of individuals attempting access?			
Are the recruitment, training, and retention methods for employing guards adequate and appropriate?			
Are main doors monitored and equipped with secondary access mechanisms during off-peak periods? If so, does the secondary access method provide a means for identifying and logging the entrant?			
Are unguarded doors equipped with a mechanism to prevent “tailgating?”			
Are secondary access points (e.g., fire doors, loading docks, and other ingress points) that are not used for primary access alarmed when unattended? If so: • do the alarms function properly and are they regularly tested and maintained? • are there clear procedures for responding to alarms?			

Physical Security Review	Yes	No	Comments
Are all personnel who are authorized to enter the facility required to possess and display an identification badge at all times? If so, is the requirement enforced?			
Do employee badges display a color photograph large enough to be easily discerned by the guards?			
Is the employee badge resistant to wear, damage, and alteration?			
Does the badge display the employee's name and any other identifying information (e.g., number, bar code) clearly?			
Does the badge contain any electronic or magnetic information that may be needed by card readers?			
Can the badge provide limited (vs. full) access to some areas of the corporate campus, when appropriate?			
Does the badge have an address to which it can be mailed, if lost, without postage should a non-employee find it?			
Are there procedures for retaining, destroying, or deactivating badges of employees who leave the company?			
Are non-employee visitors required to obtain and display a temporary identifier such as a visitor's pass?			
Are there procedures and conditions for escorting non-employees to and within the facility? If so, are they enforced?			
Physical Premises Security: Key Control			
Are any critical facilities accessible through the use of			

Physical Security Review physical keys alone?	Yes	No	Comments
Are there procedures for authorizing distribution of keys (logical and physical) to individuals?			
Are keys individually numbered?			
Is a complete inventory of keys and their owners maintained?			
Is the key inventory database maintained and audited on a regular basis? If so, are there procedures for reconciling discrepancies?			
Are there procedures for disabling logical keys and replacing locks for physical keys when keys are lost or stolen?			
Are combination lock combinations changed periodically?			
Is it impossible to discern or discover the combination of combination locks from wear patterns or records of combinations (e.g., insecure storage, combinations written or hidden near locks)?			
Physical Premises Security: Separation of Facilities			
Is access to critical areas within the facility governed by separate access control mechanisms?			
Is the access control afforded sensitive areas within the facility commensurate with the general access control provided for the building?			
Are external access points (e.g., consoles) to critical computer and network facilities physically protected in a manner			

Physical Security Review	Yes	No	Comments
commensurate with the facility itself?			
Is a record of access to controlled critical facilities logged and audited?			
Are storage media for critical information adequately protected (i.e., encrypted or locked in limited access areas)?			
Are the physical addresses of critical systems protected from widespread disclosure?			
Building Services: Utilities			
Are power feeds duplicated and geographically separated?			
Is sufficient emergency power available to run the site uninterrupted for a site-defined period of time?			
If fuel is stored on-site, are there provisions for changing the fuel regularly to prevent aging or moisture buildup in storage tanks?			
Are contingency plans in place for providing power during long-term outages?			
Is there on-site water storage or provisions for water deliveries sufficient to support continued operations?			
Are there backup external communications channels?			
Are there provisions for maintaining adequate sanitary facilities in the event of loss of services?			
Are there provisions for environmental regulation (heating and air conditioning) in the event of a loss of service?			

Physical Security Review	Yes	No	Comments
Are locked containers available where needed for disposal of sensitive information?			
Is there adequate protection of disposed sensitive information at all points along the disposal path?			
If such disposal is a contracted service, is the contractor bonded and rated as highly trustable?			
Building Services: Emergency Services			
Are adequate and effective evacuation processes in place?			
Is there fire detection and suppression in critical areas of the building?			
Are there safeguards to maximize the structural integrity of facilities housing critical assets?			
Building Services: Redundancy and Dispersion			
Are critical communications links redundant, geographically diverse, and instantly available?			
Are critical computer and network facilities redundant, geographically diverse, and immediately available?			
Have all single points of failure for critical systems and communications links been eliminated?			
Environmental and Geographical			
Are critical facilities located in areas unlikely to experience natural disasters, serious accidents (e.g., chemical spills), power interruptions, or related problems?			

Physical Security Review	Yes	No	Comments
Is the location of the facility conducive to the safety of staff both on site and en route to the facility?			
Collocation Procedures			
Is equipment in collocated facilities isolated by physical barriers?			
Are procedures in place to ensure that personnel changes can be monitored across collocated companies?			
Are adequate distances between incompatible equipment types maintained to prevent equipment failure or disruption through electromagnetic interactions?			
Are adequate distances maintained between building services (e.g., water lines) and equipment to avoid accidental damage to equipment in the event of a services failure?			
Is collocated critical equipment free of distinguishing labels or markings that might call unwanted attention to it?			

C.2 Network Element

Network Element (NE) reviews apply to telecommunications devices such as switches, routers, and transmission elements, that have embedded software or databases that are configurable via an operations interface. Compromise of the operations interface can affect all aspects of NE performance. Some voice NEs also have a call-processing interface that can potentially be compromised to obtain fraudulent usage of services it provides. These are covered in separate tables below.

Different equipment venders' NEs have different security capabilities and feature sets. It is important to conduct a preliminary analysis of the NE's feature set to determine what features are available. The feature set can then be analyzed to determine if it is adequate for the criticality of the NE's function. The second important aspect of the review is a determination of whether or not the security features have been activated on the NE, and if their configuration is sufficient to meet the requirements of the NE policy. The checklists below provide guidance on the minimum set of security capabilities that should be deployed. Depending on the NE and on the applications it supports, the appropriate configuration of other security features may also be assessed.

Network Element Review: Operations Interface	**Yes**	**No**	**Comments**
Identification and Non-repudiation			
Does the NE require every user to be uniquely identified?			
Does the NE prevent creation of a user-ID that already exists?			
If the number of users is higher than the number of user-IDs that the NE can accommodate, is there an external mediation device to distinguish among users of shared IDs?			
Authentication			
Does the NE require a password or other authentication mechanism to verify the claimed ID of the user?			
For multiple-use passwords, are there password complexity			

Network Element Review: Operations Interface	Yes	No	Comments
rules and aging capabilities?			
Access Control			
Does the NE require a user-ID/authenticator for every session on every operations interface (except the Emergency Access Interface, EAI)?			
Are logins via an EAI, if it exists, alarmed or recorded on an audit trail?			
Does the NE generate an alarm or lock out a user after multiple consecutive failed login attempts?			
Does the NE display an appropriate warning banner at the time of login?			
Do NE sessions automatically time out after a specified period of inactivity?			
Are remote logins mediated by an Operations Support System?			
Are remote login sessions to the NE protected from sniffing or hijacking attacks?			
Is modem-based access to the NE adequately controlled or prohibited where possible?			
Is the protection afforded for access via the Access Network comparable to that offered via consoles or other remote access?			
If an NE is controlled via a management protocol (e.g., SNMP), does that protocol provide sufficient protection			

Network Element Review: Operations Interface	Yes	No	Comments
from surreptitious or unauthorized logins?			
Authorization			
Does the NE support several levels of authorization (read only, read & write, create, retrieve, update, delete)?			
Does the NE configuration prevent a user from accessing a resource of the NE unless specifically authorized to do so?			
Does the NE support the capability to grant or deny access to any given user and any given port for specific resources?			
Does the NE support limiting potentially damaging commands (e.g., “delete all translations”) to users authorized to execute such commands?			
Audit			
Does the NE maintain an audit log of all security-related events?			
Does the NE adequately protect the integrity of the audit log?			
Does the NE have the capability to generate customized audit reports?			
Integrity			
Does the NE support integrity checks for system functions? If so, are integrity checks run periodically and frequently?			
Does the NE support verifying the integrity of data received from remote locations?			

Network Element Review: Operations Interface	Yes	No	Comments
Does the NE retain security parameters after events such as			
a system restart?			
Does the NE provide back-up capability to restore the system whenever necessary? If so, are reload-tested backups retained both on and off the premises and maintained according to a periodic and frequent schedule?			
Policy Implementation Assessment			
Does the NE support any confidentiality requirements for storage and transmission of data as required by policy?			
Are the security settings and configurations of the NE maintained in a manner consistent with the requirements specified in the policy?			
Are security administration activities executed in a manner that complies with the requirements and intent of the policy?			
Can all NE security policies be implemented by the existing capabilities of the NE? If not, are areas of non-compliance noted and addressed by some other means?			
Are scheduled activities conducted on the NE in a manner that complies with the requirements and intent of the policy?			
Installation			
During installation, are test procedures available to determine whether the delivered software is exactly as specified in the master copy?			
Are there tools and procedures for verifying that a newly			

Network Element Review: Operations Interface	**Yes**	**No**	**Comments**
generated release contains the appropriate versions and levels of its component modules?			
Are all software changes documented and reviewed to ascertain that security has not been compromised?			
At the time of delivery and installation, is the NE environment configured with secure installation defaults? If these defaults are inconsistent with corporate security policy, are they configured to conform to that policy?			
Network Element Review: Call Processing Interface	**Yes**	**No**	**Comments**
Does the interface maintain the confidentiality of information for which the caller is not authorized (e.g., the PIN of another authorized caller)?			
Is the caller prevented from bypassing the service restrictions imposed on the user interface?			
Is the caller prevented from masquerading as another caller?			
Is there adequate protection against black box fraud?			

C.3 Operations Support Systems

Operations Support Systems (OSSs) provide centralized access to the NEs they support, so they should include security capabilities and features similar to those required for the NEs (see checklists in Appendix C.2). This will help ensure that the interface between the OSS and NE does not compromise the NE. There are many types of OSSs performing a wide range of operations functions for numerous types of NEs. Consequently, there are numerous OSS/NE interfaces. The OSS/NE interface can be considered a subset of the larger set of communications required when an NE is controlled or managed by any device such as an element manager, OSS, remote administrator, or third party (e.g., the equipment vendor). These aspects of the review are covered in the checklists on Access Networks (Section C.5). However, some security aspects of the OSS/NE interface should be considered separately.

Operations Support System	**Yes**	**No**	**Comments**
OSS/NE Interface			
Are mechanisms in place to protect the integrity of the path between the managed and managing device?			
If the OSS/NE interface uses middleware technology (e.g., CORBA, SNMP), have the security features of the middleware been appropriately configured and deployed?			
Are all of the security features of the NE (e.g., authentication, authorization) projected into the OSS environment?			
Does the OSS provide an alarm when the communications link to the NE is lost?			
Does all remote access to NE require OSS mediation (e.g., no modem access)?			
Is the OSS/NE interface authenticated? If not, are NE authentication challenges propagated to the OSS?			

C.4 Network Management System

The network management system is a special case of an OSS with management oversight for NEs, and the review of the management system should include a review of all policies and procedures that are also relevant for OSSs. In addition, the review should be aimed at ensuring that security measures in place for the NE's are not inadvertently compromised by the use of the management system. Since network management systems and tools are powerful, extra care should be taken to assess the appropriateness of their use.

Network Management System	**Yes**	**No**	**Comments**
Are the numbers and locations of managed devices known and documented?			
Does the management system include protective features commensurate with the network and network nodes it manages?			
Are there restrictions on access to the management system to trusted personnel with a job-related need?			
Are personnel aware of potential vulnerabilities that may be introduced by management system protocols?			
Is access to the network management system appropriately constrained so that unintended access pathways are limited? (Including, for example, access from public networks such as the Internet.)			
Is the OSS/NE interface authenticated? If not, are NE authentication challenges propagated to the OSS?			

C.5 Access Networks

Access Network Review	Yes	No	Comments
Architecture			
Is the Access Network isolated (via firewall or other means) from more general data networks? (If so, an assessment of the adequacy of the firewall configuration may be necessary.)			
Are all critical Access Network components redundant (i.e., no single points of failure)?			
Does the Access Network provide auditing and notification capabilities?			
Is critical network data stored in a secure manner? (i.e., encrypted or locked, and off site as well as on site).			
Do adequate backup and recovery procedures exist?			
Are protocols and services used on the network restricted to those required for performing day-to-day functions? If so, are they appropriately configured?			
Are security mechanisms on the network appropriately configured? (Depending on the type of network, vulnerability scanning tools may be available to check for security feature configurations.)			
Is documentation describing network and host security features available on site?			
Are Access Network personnel aware of security require-			

Access Network Review	Yes	No	Comments
ments and policies for the network? If so, are the policies enforced?			
Access			
Are unique user-ID/password pairs required for all personnel having access to the network? If so, are password complexity and aging rules in place?			
Do access terminals on the network time out after a specified period of inactivity?			
Is an appropriate warning banner displayed at time of login at all access points?			
Are strong authentication mechanisms required for external access to the network?			
Are authorization levels for functions required by different job categories defined and consistently enforced?			
Are authorizations appropriate for defined job functions?			
Are procedures in place for disabling user accounts when they are no longer required?			
Are firewalls or other perimeter defenses regularly reviewed and maintained?			
OSS Operating System			
Are software change management procedures in place for monitoring and installing security updates or patches?			
Are file and directory access permissions defined and			

Access Network Review	**Yes**	**No**	**Comments**
enforced for different user authorization levels?			
Are default settings of security features set to the most restrictive mode? That is, does explicit action have to be taken to relax security features?			
Are host operating system configuration files protected from unauthorized access or modification?			
Does the host operating system enforce password complexity and aging requirements?			
Are procedures in place and enforced for authorizing and monitoring guest and anonymous accounts?			
Are privileged accounts adequately protected?			
Are trust relationships among hosts and external entities appropriately restricted?			
Are insecure protocols (e.g., UDP, *ftp*) disabled?			
Are security requirements and assessment procedures in place for applications running on the operating system?			
Administration			
Is there a defined role for a security administrator on the network? If so, are the security functions reserved for only authorized administrators?			
Are there procedures and processes in place for implementing access restriction requirements to NEs and OSSs? If so, are the restrictions enforced?			

Access Network Review	Yes	No	Comments
Are there procedures and processes in place for administering security audit trails?			
Are security audit logs maintained and periodically reviewed?			
Do the managed devices support security administration functions, a capability to separate those functions from all other onboard functions, and capability to reserve those functions for administrators only?			
Can the security administrator monitor the activities of all users logged on to any or all managed devices?			
Can the security administrator, and only the security administrator, authorize and revoke users' access privileges?			
Can the security administrator manage all security-related features and parameters on the managed devices?			
Are the system administrators prevented from independently performing critical commands that may disable a critical operation or modify critical data?			
Are there requirements for the security administrator to monitor and validate security features on the managed devices? If so, is there a process for recording and completing any actions required to remedy any non-compliance?			
Can the security administrator access all audit data needed to generate a security audit on one or many managed devices?			
Can all security administration functions be performed in a			

Access Network Review	Yes	No	Comments
secure manner?			
Are all management tools and protocols (e.g., SNMP, CMIP) configured for high security and operated securely?			
Have all vendor-supplied default security parameters been reinitialized to more secure settings on all managed devices and on the security management platform (if it is vendor-supplied)?			
Is there an active procedure for backing up security settings for all managed devices and for the security management platform?			
Does the security management platform itself have a warm backup in place if it should fail?			
Is all security audit data archived in a secure manner sufficient for it to be useful as evidence in legal proceedings?			
Does the security administration function provide the capability to remove an administrator from the security administrative position without having to reset all administrative passwords on all managed devices?			
Miscellaneous Considerations			
Are security mechanism in place for network and administrative connections by third party companies?			
Is there a Data Connection Agreement (DCA) governing mutual roles and responsibilities for connections to third party companies?			

Access Network Review	Yes	No	Comments
Are customer configurable services offered on the network? If so, is there access adequately constrained to prevent access to confidential information and network operations functions?			
Are CALEA access mechanisms appropriately administrated and controlled to prevent unintended unauthorized access?			

Appendix D: AUTOMATED ATTACK TOOLS

Commercial and public domain automated attack tools have been available for years. These tools, originally developed by perpetrators to attack systems, are used by security personnel to locate vulnerabilities in deployed networks, systems and services. These tools support two commonly used automated attack methodologies:

1. War dialing – the act of dialing sets of telephone numbers to locate active modems accepting connections.
2. Intrusion testing – the act of probing a system or network for vulnerabilities. These tools can be configured to exploit vulnerabilities (e.g., attempts to guess passwords and gain unauthorized use of services or data).

Automated attack tools are very powerful, and their use can lead to serious security breaches in a company's computer systems and communications networks (e.g., Intranets, LANs). For purposes of the security review, automated attack tools can be used to assess an Organization's plans for:

- Resisting and responding to automated attacks, particularly attempts to deny services to customers (Denial of Service attacks).
- Anticipating threats to network services by utilizing automated attack tools to locate vulnerabilities in their systems and networks and plan for corrective action.

Effective security management practice should include the use of such tools as part of an internal program to periodically assess the deployed network infrastructure. The next two sections discuss the tools that support the two methodologies mentioned above.

D.1 War Dialing

War dialing is a form of attack in which an intruder attempts to discover the telephone numbers of telephone links attached to Network Elements, computers, workstations, PCs, and other on-line devices, for the proposes of exploiting them remotely. A war dialing attack typically performs a systematic examination of a set of telephone numbers, usually by starting with the lowest number (say, 0000) in the exchange and incrementally collecting "candidate" numbers until it reaches the highest number (e.g., 9999). The candidate numbers are those that appear to be answered by a modem.

War dialing detects only modems that are turned on and connected to a telephone line at the time the attack is being mounted. Furthermore, a war dialer will not detect a modem in use because the telephone number will be busy. This means that war-dialing attacks are least effective when directed against an environment in which modems are switched off when not in use.

War dialing software is available only for analog connections, not digital, (though that may be changing). The public domain package *ToneLoc* is a commonly used war dialing package. When discovering an accessible device, the tool will log identification information for the device. Using available collections of common identifiers and passwords—or lists of all words in a dictionary—a tool can attempt to exhaustively try combinations to uncover accepted access authentication values.

D.1.1 Resisting War Dialing Attacks

It may be possible to trace the attacker if war dialing is detected while it is occurring. Therefore, personnel should be educated to recognize war dialing attacks against the company. Education is important since this type of attack has telltale signatures. These include:

- Abnormal telephone calls. A staff member who receives a call that is silent for 15 to 30 seconds (a standard configuration for *Toneloc*) should alert appropriate security personnel. If Caller ID is available, the calling number should be noted. If multiple calls are reported they should be traced to determine if a war dialing attack is occurring.
- Sequenced dialing. Since the attack software dials numbers in sequential order, the PBX can be configured to detect when a set of telephone numbers is dialed in sequence. When this occurs, an alarm should be activated and a trace put on the calls. Note, however, that some war dialers can be programmed to dial randomly through an exchange or PBX.

Dial-back modems, once believed to be secure, provide only minimal security against today's war dialing attacks. Strong identification and authentication techniques should be used instead of, or in addition to, dial-back modems to prevent unauthorized access. Currently, one-time password mechanisms are the generally accepted standard.

D.1.2 Using War Dialing

Security personnel can use war dialing as a detection tool to locate and test modem access. War dialing can identify vulnerabilities such as easily guessed or missing passwords, lack of warning banners, and entry points that might give inappropriate access to application or system information. War dialing can also determine if personnel detect the signatures of an attack and report observed occurrences. Lastly, it can be used to search for breaches in security policies[27] that forbid the use of modems. This type of search must be conducted at a variety of time intervals in order to locate modems that may be in use or turned off at the time a war dialing exercise was taking place.

D.2 Automated Network and System Attacks Tools: Intrusion Testing

Automated network and system attack tools take advantage of lax security, known security flaws, procedural inconsistencies or inadequacies, and other weaknesses to discover holes through which an intruder can invade or attack a machine. Attack tools focus on

[27] A strong policy addressing the use of modems on systems and on the network is important in controlling the placement of unsupervised access to network services through independent modems.

known weaknesses. The tools detect vulnerabilities based on a limited (though perhaps large) number of attack scenarios, most involving a sequence of steps. This means that the attack tools tend to leave an attack signature, which can be detected through examination of audit trails and other telltale "footprints." The notion forms the basis for the concept of *intrusion detection* as a defensive measure against automated attacks.

Many commercial attack tools can report suggested corrective actions to prevent uncovered vulnerabilities. The appropriate corrective action must take into account the broader security architecture for the network and services.

D.2.1 Detecting Automated Network Attacks

Intrusion detection systems (IDSs) are designed to detect automated network and system attacks. IDSs either look for attack signatures or for activity that does not conform to "normal" user activity. IDSs can potentially detect unauthorized access, Denial of Service (DoS) attacks, abuse of privileges, and misuse of systems.

Depending on their level of sophistication, IDSs can:

- Detect attacks and notify that they are occurring
- Terminate attacks
- Record and playback sessions
- Identify attackers (on occasion) or the attack source
- Strike back (though these features should be used with care)
- Update Access Control Lists in Firewalls or Routers (also to be used with care).

Certain automated attack tools can circumvent IDSs by using a number of techniques to avoid detection. For example, a Denial of Service attack can be launched against the IDS itself, leaving the network open to other attacks that will then go undetected. In another scenario, small attacks below the threshold of the IDS can be perpetrated over days or weeks to desensitize the IDS so that the ultimate attack does not trigger the IDS alarms.

An IDS with logging functions can provide a history of unusual network activity over time. The history supports effective evolution of security management as the network and supported services change.

D.2.2 Using Automated Network Attack Tools

Most communication networks employ configurable devices to control the flow of traffic in the network. As a result, the view of network elements, systems and services gained through attack tools will vary depending on the source of the attack (i.e., where the attacking system gains connectivity to the network). Automated network attack tools should be used to detect vulnerabilities at multiple access points:

- Access points from external networks such as the Internet or business partner connections. These tools can be used by system or security administrators to obtain a perpetrator's view of the network. To be effective, the tools should check all access points into the network (e.g., outside the firewall). All systems should be scanned for network and system vulnerabilities. When vulnerabilities are located immediate action should be taken to mitigate the exposure. Similarly, all network elements outside the network or on the perimeter should be tested. This includes firewalls, servers (e.g., DNS, e-mail, and WWW) and the network infrastructure (e.g., routers and switches).

Scans can also be used to determine whether employees are detecting and responding to test attacks, so that a measure of their reactions to real attacks can be estimated.

- The internal network. Internal Networks and systems can be scanned to locate internal vulnerabilities. It is important to minimize internal exposures in case the perimeter is compromised. By running such tests, administrators will be alerted to many kinds of attacks and will be better positioned to contain the attack to a small section of the network and to minimize the impact of insider exploits.

D.3 Public Information Sources

Security reviews of TCP/IP-based networks often overlook assessing the amount of information a potential intruder can gather about the network topology. Some of this public information can give an intruder insights into potential problems with the network. On the opposite side of the coin, public information gathering can help a company identify potential areas of vulnerability and may suggest some changes in network configuration that will help conceal information of potential value to intruders. Examples of sources of relevant information include:

- Domain Name Services (DNS). The company DNS server holds the domain names for all networked machines on the corporate network. These names can be useful to an attacker if they describe the services a given machine provides. For example, a domain name that includes the sequence “911” gives an attacker a pretty good idea of which machine supports emergency services and thus, where to attack. Similarly, a domain name that includes the string “Cisco” (for example) provides a good starting point for an attacker who wants to target routers.

  From the standpoint of a security analysis, then, examination of the DNS records can reveal information that might make an attacker’s job easier. This same information can therefore help an organization pinpoint areas that may need strengthening, if only by domain name changes or by denying external access to internal DNS Zone records.

- Internet Network Information Center (InterNIC). The InterNIC is a storehouse of information on a company’s Internet connections. It maintains records on the IP address ranges available to the company, company contacts who should be notified in case of an attack or potential attack, and other less critical data. The analysis should verify the validity of the information and determine that guarantees (e.g., authentication measures) are in place to protect this information from illicit modification.

- Web sites. A deeper security analysis often includes obtaining information available on bulletin boards, chat rooms, and other sites, including disreputable (e.g., hacker) sites. This type of information can be gathered on an ongoing basis so that a company may be alerted as soon as possible when information relevant to its network appears on these sites. Some useful sites include *www.10pht.com*, *www.antionline.com*, and *packetstorm.security.com*. Other sites provide access to tools for war-dialing and automated network attacks. A number of network computing publications maintain links to tool sites, such as *www.securityfocus.com*. The Web sites hosting specific tools tend to change frequently.

Careful use of these three sources can strengthen a security assessment by providing extra data that can be collated and factored into the other areas.

List of Acronyms

The following acronyms are used in this guide.

ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
CALEA	Communications Assistance for Law Enforcement Act
CCS	Common Channel Signaling
CLEC	Competitive Local Exchange Carrier
CMIP	Common Information Management Protocol
CORBA	Common Object Request Broker Architecture
CPE	Customer Premise Equipment
DCA	Data Connection Agreement
DCC	Data Communications Channel
DNS	Domain Name Services
DoS	Denial of Service
EAI	Emergency Access Interface
ESAC	Emergency Switch Assistance Center
HR	Human Resources
HTTP	Hypertext Transfer Protocol
I&A	Identification & Authentication
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
ILEC	Incumbent Local Exchange Carrier
IP	Internet Protocol
IPSec	Internet Protocol (IP) Security
LAN	Local Area Network
NE	Network Element
NOC	Network Operations Center
OAM&P	Operations, Administration, Maintenance, and Provisioning
OMNCS	Office of the Manager, National Communications System
OSS	Operations Support System
PBX	Private Branch Exchange

PSN	Public Switched Network
RACF	Resource Access Control Facility. A product of IBM
RARP	Reverse Address Resolution Protocol
SCC	Switch Control Center
SME	Subject Matter Expert
SMTP	Simple Mail Transfer Program
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical NETwork
SS7	Signaling System number 7
SSL	Secure Socket Layer
SSL3	Secure Socket Layer, version 3
SSP	Service Switching Point
STP	Signaling Transfer Point
TARP	TID (Target Identifier) Address Resolution Protocol
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TMN	Telecommunications Management Network
TRA	Telecom Reform Act. Alternate term for *Telecommunications Act of 1996*
UDP	User Datagram Protocol
VoP	Voice over Packet
WWW	World Wide Web

Sources and References

1. FED RES. *Sound Practices Guidance on Information Security*. Federal Reserve Bank of New York. September 1997.
2. Ferbache, David, and Gavin Shearer. 1993. *UNIX® Installation Security & Integrity*. PTR Prentice Hall, Englewood Cliffs, NJ.
3. FR-2063*, Network Equipment-Building System (NEBS) Family of Requirements,* Issue 99, (Telcordia, March 2000)
4. GR-815-CORE. *Generic Requirements for Network Element/Network System (NE/NS) Security*, Issue 1 (Bellcore[†], December 1997).
5. GR-1194. *Bellcore Operations Systems Security Requirements*, Issue 1. (Bellcore[†], December 1998).
6. GR-1253-CORE. *Generic Requirements for Operations Interfaces Using OSI TOOLS: Telecommunications Management Network Security Administration*, Issue 1. (Bellcore[†], June 1995).
7. GR-1332-CORE. *Generic Requirements for Data Communications Network Security*. Issue 2 (Bellcore[†], April 1996)
8. GR-1469-CORE. *Generic Requirements on Security for OSI-Based Telecommunications Management Network Interfaces*, Issue 1 (Bellcore[†], September 1994).
9. Gottola, Michael G. *The UNIX Audit: Using UNIX to Audit UNIX*. McGraw-Hill, Inc. New York. 1993.
10. Haimes, Yacov Y. *Risk Modeling, Assessment, and Management*. John Wiley & Sons, Inc. New York. 1998.
11. NCS. *The Insider Threat to Information Systems: A Framework for Understanding and Managing the Insider Threat in Today's Business Environment*. National Communications System. June 18,1998.
12. NCS. *Public Switched Network Best Practices Security Primer*. National Communications System. December 1998.
13. NCSC TG-001. *A Guide to Understanding Audit in Trusted Systems*. National Computer Security Center. June 1988.
14. NIST IR 5153. *Minimum Security Requirements for Multi-User Operating Systems*. National Institute of Standards and Technology. March 1993.
15. NIST SP 800-7. *Security in Open Systems*. National Institute of Standards and Technology. July 1994.

[†] Documents produced by Bellcore are now obtainable only from Telcordia Technologies, Inc. These documents were written before Bellcore was transformed into Telcordia Technologies. Once Telcordia updates or otherwise revises these documents, they will be referenced only by the Telcordia name and document numbers, and will no longer be obtainable under the Bellcore name or by the Bellcore document number.

16. NIST SP 800-14. *Generally Accepted Principles and Practices for Securing Information Technology Systems*. National Institute of Standards and Technology. September 1996.

17. Notice Of Proposed Rulemaking, *In the Matter of: Communications Assistance for Law Enforcement Act* , CC Docket No. 97-213, adopted on October 2, 1997, and released on October 10, 1997

18. Stallings, William. *SNMP, SNMPv2, and CMIP: The Practical Guide to Network Management Standards*. Addison-Wesley Publishing Company, Reading MA. 1993.