White Paper

Information Security -- Network Assessment

For further details as to the process and the procedures followed, contact:

Computer Technology Associates, Inc.
INFOSEC Group
7150 Campus Drive, Suite 100
Colorado Springs, CO 80920
(719) 590-5100

NETWORK SECURITY ASSESSMENTS

1. SUMMARY.

Our assessment strategy rests on basic requirements for system and network security. There are certain characteristics that the network should possess:

- ✓ **Security Policy.** Networks should have an associated defined security policy that specifies information security requirements (e.g., confidentiality, integrity, availability, auditing, access control, etc.) as well as what users may and may not do on the network (e.g., what constitutes unauthorized and illegal activities).
- ✓ **Network Management.** Networks should be able to control access to and detect modifications of critical components. Networks must maintain control over their configuration (e.g., hardware, software, security, etc.) and connectivity.
- ✓ **Identification and Authentication.** Networks should provide and manage identification and authentication functions.
- ✓ **Resources Management.** Networks should provide and manage confidentiality, integrity, access control, and availability of network resources.
- ✓ **Account Management.** Networks should provide and manage security-related features of network accounts (e.g., user).

Our primary focus for the network security assessment is identifying network vulnerabilities that an active hostile human threat might exploit. Although our assessment identifies both technical and non-technical weaknesses (e.g. procedural deficiencies), our assessment is focused on an in-depth analysis of technical vulnerabilities.

Our offering includes --

- ♦ Identifying and reporting network security weaknesses,
- ♦ Providing the client information about the weakness,
- ♦ Helping validate that the weakness is a vulnerability the client wants to fix,
- ♦ Assisting in identifying measures to eliminate or mitigate the vulnerability, and
- ♦ Validating that the vulnerability is eliminated or mitigated.

Enterprise networks today operate in a high technology, open environment. Enterprises depend on their networks to enable them to successfully compete in domestic and international markets. The same worldwide connectivity that makes the enterprise competitive also exposes the enterprise to attack and financial loss. More and more enterprises are losing millions of dollars through high-tech crime and information technology misuses and abuses. The crimes include financial fraud, telecommunications fraud, theft of proprietary information, computer viruses, theft of computers and/or their components, and sabotage of data or networks. The threats to enterprise network assets are real.

We are concerned with both structured and unstructured threats. Examples of structured threats include industrial espionage and cyber terrorism. We all know of cases where a company discovers that one of its competitors or a hacker has penetrated its network. Structured threats have several common characteristics. The most important include goals, organization, planning, time, funding, technical expertise, and tools. Structured threats normally target assets or services of value. For example, structured threats may be designed to embezzle funds, acquire sensitive information, or disrupt critical services such as power generation, water management or law enforcement and safety operations. In many cases structured threats require detailed information about the network, its components, and the environment that they are attacking. This information includes network and system design and operations information that may be in the hands of employees and, in some cases, may be openly available on the Internet to outsiders. We are experiencing an increasing number of cases of employees (or former employees) who use their enterprise's connectivity not only to attack their own company's

computers and disrupt its network, but also to attack the computers and networks of other companies.

The best-known computer virus attacks so far, Code Red and NIMDA, both within the past year, were likely products of single individuals. They caused millions in damages and disruption. One can only imagine what an organized, well-funded and technically sophisticated group could do. Every organization keeping track of cyber related attacks agree that cyber attacks are increasing in volume, sophistication and coordination, and are attracted to high-value targets. The dynamic technological landscape (faster processors, higher bandwidth, new attack tools, etc.) frequently erodes the protective value of implemented security solutions, demanding continuous security updating, and proactive, adaptive network security assessments.

Unstructured threats are fleeting in nature. These threats are not organized, do not have funding, or may not involve the use of tools. A college student who tries to access a local area network out of curiosity, or an employee who enters erroneous data causing system failure are examples of unstructured threats. In addition to human activity, unstructured threats can emanate from natural (e.g., fire or flood) and structural (e.g., physical plant) sources.

Enterprises are rightfully concerned about Enterprise Network Security and what do to about it.

An enterprise's network includes computers and workstations, routers, bridges, modems, etc. as well as the operating, executive, communications, and application software that govern how these components operate. Most components have some built in automated (technical) security mechanisms. These mechanisms provide protection services for the information that the components process, store, or transmit. These services are usually referred to as *technical security controls*. The environment that surrounds the network also has protective mechanisms. Security controls within the environment (*non-technical security controls*) reinforce protection afforded by the component. Physical, procedural, and administrative security mechanisms like back-up power, door locks, badge systems, policies, operational procedures, location, trusted users, etc., are all examples of security mechanisms present in the network's environment. Although the component and environment offer security mechanisms to protect information, the protection is not absolute — both can have weaknesses. Unauthorized individuals use the weaknesses to gain access to critical or sensitive information stored, processed, or transmitted by the network. An authorized user may exploit a weakness to misuse the network. The security mechanisms that protect the network can fail, be improperly configured, or not be implemented at all.

We use the network security assessment process to identify technical and environmental weaknesses in a network. Network security assessment also identifies real and potential threats to the network. Real versus theoretical threats must be effectively addressed and over-protecting marginally valuable assets at the expense of under-protecting critical assets must be avoided.

We identify errors in the configuration and operation of the network. We assess the enterprise's capabilities to detect external and internal attacks on the network. We report identified threats and vulnerabilities to management with recommendations concerning their seriousness and possible impacts on the enterprise. We provide recommendations and ways, sometimes at added expense, to either mitigate or remove identified vulnerabilities. Management makes the final judgement on the cost-benefit trade-offs of added security expense against mitigating these risks to the Enterprise.

2. OFFERING OVERVIEW.

Depending on the client's needs, a network security assessment may be a snapshot of a network at a point in time or it may be a continuous process. We can provide a single assessment over a set time (e.g. a few weeks). We also provide a continuous service over months or years that includes intrusion-detection, monitoring, continuous assessments of network components (e.g., on a regular schedule), and periodic site assessments (e.g., quarterly or annually). A complete assessment using the all the processes below helps the client establish the "security baseline" for the network. Continuous assessment helps the client maintain and improve this "security baseline." The assessment process has four modular components, each of which performs a specific security assessment task.

We start the process by collecting data and identifying the components and boundaries of the client's network. No matter what the size of the assessment, we need to bound the network and find out what is

important to the client. Data collection includes an information exchange with the client. We base our assessment on the enterprise's security policies and procedures, the National Institute of Standards and Technology's (NIST) "Generally Accepted Principles and Practices for Securing Information Technology Systems," and other best practices. We use the technical assessment module to discover component vulnerabilities and assess component technical security. Another module performs on-site security assessment of the network's support structure. We can conduct site assessments and technical assessment in parallel. Data analysis and reporting is a final “step.” This module puts together information from the site assessment and technical assessment as well as threat information. We analyze information and determine the risks to the network. We provide recommendations on how to mitigate the risks. During most assessments, we also validate the countermeasures the client’s staff has implemented to correct a weakness on a component or at a site. So the assessment processes is really iterative. Finally, CTA provides assistance to management in determining the best course of action to improve security of the enterprise's network.

We generally tailor the breadth and depth of the network security assessment process to meet the enterprise's needs and funding profile. However the process framework is based on a repeatable, proven approach and reflects best “Business Practices” for information security. The process examines both hard (computers, routers, etc) and soft (personnel, physical, environmental, etc) architectural elements. Our modular approach gives us the flexibility to perform assessments from outside or from within the enterprise, at any level of the network, and can include the use of statistical sampling techniques for large systems. Sampling helps reduce a client's costs and while maintaining a level of confidence that the assessment provides an accurate picture of the network's security.

We can also focus our attention on specific components of an enterprise network of specific concern to our client due to the sensitivity or criticality of the asset involved. For example, the client may be interested in determining the technical vulnerabilities of and threats to the enterprise's electronic commerce servers that underpin the financial backbone of the business. In this case, we limit examination of information related to the specific servers and threats, and conduct a localized technical assessment, considering however, that networks are like chains in which the component with the weakest security creates a threat to all other components in the network.

We can also tailor the depth or “level” of assessment. We define assessment level in two ways: how far into the network's structure the security assessment will go, and whether the assessment will an external assessment, an internal assessment, or a combination of both. In an external assessment we conduct perimeter defense assessments of components through the firewalls, routers, public access web servers and other devices designed to protect the network from "outsiders". In an internal assessment we conduct assessments from behind the firewalls and other devices. We generally recommend that clients conduct both external and internal assessments. External assessments help the client judge the effectiveness of components that are in place and designed to limit access to the network and its segments; internal assessments help clients judge the effectiveness of mechanism that are designed to protect their network and its critical components from misuse and abuse from insiders -- employees, trading partners, customers, etc. The internal assessment is also important because it discloses those vulnerabilities that an attacker might exploit if and when the network's perimeter defenses fail. We can conduct these assessments remotely, from the client's site, or a combination of both.

The network security assessment process described herein is applicable to any type of business. CTA has applied the process to both large and small enterprise networks for public and private sector client facilities with equal success. We use a standard, highly disciplined methodology across all components of the architecture, seeking frequently unexpected vulnerabilities. The method is driven by the fact, as indicated above, that the enterprise’s connected assets are only protected to the strength of the weakest link in the enterprise and that hundreds of vulnerabilities have been proven to exist in spite the presence of security devices claimed to be “impenetrable” and “hacker-proof” by the manufacturer. The enterprise inherits the risks of all its organizations that share such resources.

2.1. Step 1 – Data Collection and Network Identification.

Before entering Step 1 of the assessment process, CTA will have

- Presented general assessment options to the client and established a contract that describes precisely what assessments we will accomplish under the agreement.

- ♦ Provided the client a checklist or questionnaire containing information that we will need to discuss at the pre-assessment briefing meeting with network administrators, network security administrator and functional area AIS managers.
- ♦ Secured technical and procedural information from the client such as network diagrams, security policies and procedures, and functional descriptions of data/applications.

The first component in the assessment process is Data Collection and Network Identification. During this step, we collect initial information about the network and exchange information with the client. We discuss the four overall assessment modules -- data collection and network identification, site assessment, technical assessment, and data analysis and reporting. We also discuss the risks (if any) the enterprise is assuming by conducting the assessment, what we have done to minimize risks, and any expected impacts on network operation. Before we conduct an assessment, the client must understand precisely the scope of the assignment, how we conduct the assessment, the time it will take, and the resources we need. Our experience and expertise, combined with our corporate culture of the importance of teamwork with our client's staff, will establish confidence with the client's technical team of the soundness and benefits of our approach during this early, critical stage. We scope the assessment by bounding the network, identify network users (some of whom may be unauthorized), identifying components and services, and establishing the assessment plan of attack (breadth and depth). We also develop a statistical sample, if one is required.

2.1.1. **Objectives**

Our job in this step is to identify and confirm network components and services, connectivity to the network (e.g., routers, modems, etc.), who is gaining access to critical sub-networks, and any unauthorized network services (e.g., employees running their own web sites). It sounds straightforward, but in our experience very few enterprises have a complete understanding of their network architecture, applications, information distribution and location, who has access to network resources, and how this access is achieved.

During this step we also help the client decide what combination of assessment components and strategies will best meet the enterprise's needs, reflecting the reality of his network situation.

2.1.2. **Process**

a. Client orientation and CTA familiarization

- Meet with client's staff (network administrators, network security administrator, functional area MIS managers) for a pre-assessment briefing and discussion.
- Determine client's main security concerns.
- Determine if the client has a security policy, and if so, how is that policy enforced.
- Determine client's most critical systems or information, where it is located, and who has access to these systems and/or information.
- Determine client's expectations from the assessment.
- Distribute data collection sheets.

b. Collect and analyze data.

- Collect security and network information from client staff interviews, either through site visits or via templates accessible through our secure website, and through available documentation such as network diagrams, security policy (if one exists), and functional descriptions of data/applications.
- Determine the system/network architecture (physical and logical configuration) and the network connectivity (e.g., router, modems, etc.)
- Collect IP addresses and subnet masks for the networks that will be part of the assessment.

c. Conduct initial probes and scan component services.

d. Identify network users. To help identify users we may install network-monitoring devices on critical subnets. Here are trying to determine who is accessing the network. Are there hostile or suspicious sites accessing or attempting to access the network?

e. Review and analyze the data collected and prepare the Network Survey Report.

f. Prepare a tailored, detailed technical security assessment plan with the customer.

2.1.3. **Deliverables**

a. Survey Report

- Lists Network users and suspicious users- subnet and host IP addresses
- Verifies known connectivity and lists unknown network connections that we have found.
- Lists host running unauthorized services.
- Macro security assessment
- Lists critical network components and subnets

b. Detailed Technical Assessment Plan

- Describes how we will proceed
- Tailors the approach
- Provides the assessment schedule
- Describes the boundaries of the network assessment

2.2. Step 2 - Technical Security Assessment

The technical assessment of network components is the heart of the Network Security Assessment. During the technical assessment, we conduct in-depth searches for security weaknesses in network components. Our external assessment is run from the CTA Security Assessment and Monitoring Center in Colorado Springs. As indicated above, this assessment concentrates on assessing the security of perimeter components of network segments. Our internal assessments can either remotely or at the client's site. If the client has firewalls, filtering routers, or other components that provide the network perimeter protection, the client must allow our workstations through this protection. When an internal assessment is performed at the client's site we use a combination of commercially available tools and our own proprietary tools and procedures loaded on our specifically configured assessment workstations.

Vulnerability assessments determine if someone can remotely exploit vulnerabilities in the target network and its components by using the target's external connectivity. These assessment tools are not resident on the target and are run remotely. The tools that we use detect well-known vulnerabilities that attackers might be able to exploit. We use checklists and manual methods to supplement these tools. We also use checklists and manual methods to cover new vulnerabilities available from a variety of information sources that we continuously monitor that are not yet covered by the automated toolset. This provides the client with an assessment against the most recently experienced threats and vulnerabilities in the industry.

During the technical assessments, we conduct policy enforcement assessments as well as vulnerability assessments. Policy enforcement assessments detect internal policy violations and vulnerabilities that vulnerability detection scans don't detect. Normally these violations are related to component configuration errors. For example, a policy requiring that user passwords should be a minimum of eight characters is not supported by a system configured to accept three character passwords. Or the tool may identify users with inappropriate supervisor or administrator privileges in violation of policy. The policy enforcement assessment process also checks for weaknesses in the internal security of a component. The security policy includes file system security, configuration, user privileges, integrity, and similar functions. In many cases these internal assessments require assessment software resident on the target as an agent or manager. In some cases, such assessment software cannot reside on the target component requiring the use of checklists and manual methods to supplement the policy enforcement tools. We also use checklists and manual methods to cover components such as router and switches not

covered by typical policy tools.

2.2.1. **Objectives**

The objective of this step is to identify and report technical vulnerabilities.

2.2.2. **Process**

The process below is incremental-- we assess one subnet's or site's components, complete its report, and then move to the next subnet or site.

a. Select components to assess. In some cases the client wants to limit the assessment or focus on critical components. We work with the client to identify and select critical components for further assessment.

b. Run vulnerability detection tools against subnets and the critical components.

c. Run policy enforcement assessments of components. We install and run policy enforcement tools against the component. In cases were there are no policy enforcement tools or the tools don't provide full coverage, we use CTA developed checklists. Policy enforcement assessments may be conducted during site assessments.

d. Review tool generated reports and run supplemental procedures to detect vulnerabilities that the tool does not detect.

e. Produce and provide overall Technical Assessment and supplemental reports to client.

2.2.3. **Deliverables**

The deliverables are a Technical Vulnerability Assessment and reports generated by assessment tools. The report describes vulnerabilities and how to address them.

Technical Vulnerability Assessment Report
1 TECHNICAL ASSESSMENTS/COMPONENT ASSESSMENTS
1.1 Location of Internal and External Assessments
1.2 Technical Security Assessment
2. NETWORK SERVERS POLICY ENFORCEMENT
2.1 Introduction.
2.1.1 Tools
2.1.2 Approach
2.2 Policy Enforcement Summary/Recommended Actions
2.2.1 Account Restrictions
2.2.2 Password Control
2.2.3 Access Control
2.2.4 System Monitoring and Auditing
2.3.5 Data Confidentiality
2.3.6 Data Integrity
2.3.7 Availability
2.3 Recommended Actions

Technical Vulnerability Assessment Report

Technical Vulnerability Assessment Report
8 ROUTERS
8.1 Introduction
8.1.1 Tools
8.1.2 Approach
8.2 Internal IS Vulnerability Scan Summary
8.3 External IS Vulnerability Scan Summary
8.4 Traffic Management
8.5 Router Management
8.6 Recommended Actions
Appendix 1 -- Internal IS Vulnerability Scans
Appendix 2 -- External IS Vulnerability Scans

2.3. Step 3 - Site Assessment

The next step in the assessment is the site assessment. During site assessment, we conduct on-site assessments of the network's operational environment, security environment, security management, and network operations. Site assessments assess the security of the network's support systems at each site by examination and measurement of an organization's security management, organization, and structure. Site assessments also include an examination of safeguards, processes, and procedures applied within the facility to its network support systems and to the network's components to ensure availability, protection from compromise, and integrity for the network's components or the network's processes, data, and products.

We can collect information about the site and perform the site assessment on a single visit to the site although we prefer to conduct an initial fact finding visit followed by a second visit to perform the site assessment. This allows us to review site documents and procedures and tailor our assessment checklists and processes for the site.

The operational control portion of the assessment addresses those areas that may directly affect the day-to-day operation of the network and its components. Network operational controls include security training and awareness, vulnerability and incident reporting, personnel and users, network support and operations, contingency and disaster planning, access, physical controls, and public access. The assessment includes network support and operations such as help desk functions, software and hardware configuration controls, backups, and media controls. The security environment establishes the security-related conditions or circumstances surrounding the operation of the network. The security environment assessment includes the security organization, asset protection requirements, network boundaries, and interconnections.

The site assessment may also be conducted at various levels depending on the client's needs. For example we can conduct an assessment that focuses on physical and operational security. We don't normally recommend attempted break-ins or social engineering attacks without client concurrence and approval. However under the appropriate conditions, we can test physical protections (cipher locks, physical access control procedures, etc.) and conduct "social engineering" attacks where we attempt to gain passwords or other sensitive information from users. These tests frequently disclose overall physical and procedural vulnerabilities that must be addressed.

Major Site Assessment Areas	
1.	**Personnel and User Control**
2.	**Contingency Planning**
3.	**Vulnerability and Incident Reporting and Response**
4.	**Security and Awareness Training**
5.	**Physical Security**
6.	**Network Support and Operations**

2.3.1. **Objectives**

The objective of this step is to identify and report site level environmental and operational vulnerabilities.

2.3.2. **Process**

The process below is incremental-- we assess sites, complete its report, and then move to the next site.

a. Arrange site visit with the client and perform an initial site data collection. Tailor checklists and procedures for the client's environment.

b. Conduct assessment and prepare draft findings.

c. Debrief site personnel.

d. Analyze results and complete final report.

2.3.3. **Deliverables**

The deliverable is a Site Assessment Report that lists vulnerabilities and recommendations on how to address them.

Site Assessment Report
1. INTRODUCTION
1.1 Objective
1.2 Scope and Methodology
1.3 Sites Visited
2. ASSESSMENT RESULTS AND RECOMMENDED ACTIONS
2.1 Documentation
2.2 Security Environment
2.2.1 Information Protection Categories
2.2.2 Interconnections
2.2.3 Security Organization
2.2.4 Network Environment
2.3 Management Controls
2.3.1 Risk Management
2.3.2 Security Management
2.3.4 Security Rules.

2.3.5 Life Cycle Management

2.4 Operational Controls

2.4.1 Training and Awareness

2.4.2 Vulnerability and Incident Reporting

2.4.3 Personnel and User Controls

2.4.4 Network Support and Operations

2.4.5 Contingency and Disaster Planning

2.4.6 Access

2.4.7 Physical and Environmental Controls

2.4.8 Public Access

2.5 Operational Environment

2.5.1 Operational Organization

2.5.2 Operational Functions

2.4. Step 4 - Network Security Assessment and Findings.

This step reports the consolidated security assessment findings. CTA creates a Security Assessment Report for the enterprise by facility, subnet, or both. In addition to the findings, the Security Assessment Report will identify alternative corrective solutions (countermeasures/safeguards) that might be applied to mitigate or minimize risks. Findings for all segments will be briefed at the macro level in the Security Assessment Briefing.

2.4.1. Objectives

The objective of this step is to provide a view of the network's security posture that includes recommendations to mitigate and minimize risks

2.4.2. Process

a. Review assessment results from site assessments and technical assessments.

b. Determine major findings and generate a summary briefing of major findings (good and bad)

c. Generate a list of recommendations (further analyses, actions they should take, etc.) and supporting rationale

d. Protect the report and findings as agreed upon with client

2.4.3. Deliverables

The deliverables are --

a. Network Security Assessment Report.

b. Network Security Assessment Briefing.

Network Security Assessment Report
1. INTRODUCTION
1.1 Tools.
1.2 Boundaries
1.3 Approach
2 NETWORK SECURITY SERVICES
2.1 Identification and Authentication
2.2 Access Control
2.3 Integrity
2.4 Confidentiality
2.5 Security Audit, Intrusion Detection, and Monitoring
2.6 Availability
3 MAJOR FINDINGS AND RECOMMENDATIONS
3.1 Threats
3.2 Intrusion-Detection
3.3 Auditing and Monitoring
3.4 Network Management
3.5 Network Server
3.6 Infrastructure
3.7 Routers
3.8 Firewalls
3.9 Public Access Servers
3.10 Connectivity
3.11 Documentation
3.12 Security Environment
3.13 Management Controls
2.14 Operational Controls
3.1.5 Operational Environment