Defense-In-Depth Revisited: Qualitative Risk Analysis Methodology for Complex Network-Centric Operations

Tim Bass
Silk Road, LLC
Vienna, VA

Roger Robichaux
Federated Systems, Inc.
O'Fallon, IL

ABSTRACT

Defense-In-Depth [1] concepts for global information operations are physical boundary-centric. However, network-centric operations are multidimensional, layered and often virtual. The interconnection of defensive operational elements, including the fixed and deployed base, runways, fighter planes, bombers, bombs, tankers, tents and individuals are logically and virtually connected. For this reason, traditional physical boundaries are minimally effective and often constraining. This paper extends the *Defense-In-Depth* boundary protection construct to a uniform qualitative risk management perspective that is tightly coupled with network implementation, resources, mission criticality, security policies and network-centric mission operations. The suggested risk management framework is applied to an operational example.

1.   INTRODUCTION

Information superiority objectives require sustainable, interoperable, and virtual information assurance operations. Such operations are based on the principle that compact, robust, mobile, command, control, communications and computer systems are achievable through standardization. These objectives are based on well-conceived mature architectures optimized for vertical and horizontal compatibility and for cross-vendor interoperability. In order to reduce the long-term costs of training, certifying, and operating unique network systems, network-centric information assurance risk management operations must be implemented in accordance with well-conceived policy and guidance based on logical and virtual boundaries vis-à-vis traditional physical boundaries.

Gene Rochin's seminal book, *Trapped in the Net: The Unanticipated Consequences of Computerization* [2], discusses a few eye-opening military disasters that were directly attributed to unforeseen risks associated with the integration of complex network technology. Failures in one internetworked system are likely to cascade to other interconnected systems, effectively multiplying the effects of the failure. Having clearly identifiable processes and technology audit trails are fundamentally important in these and future mission-critical network systems.

This paper provides a framework for a repeatable qualitative risk management processes that may be used as the foundation for organizational policy, guidance and architecture. The framework may be useful when building virtual and logical network-defense tactics, techniques and procedures.

2. OVERVIEW OF INFORMATION ASSURANCE CONCEPTS

Assurance of information-centric network and computer systems is often divided into six different classes [3]: human introduced errors, user abuse of authority, power and policy, system probing or mapping, system probing with

malicious hardware and software; system penetration, and subversion of network and device security and control mechanisms. All of these information assurance (IA) domains have the following risk elements in common:

Vulnerability: A characteristic of the system (e.g. a flaw, bug, or feature) that provides a means of exploitation.

Threat: The possible existence of an entity – person or process – that could exploit the vulnerability.
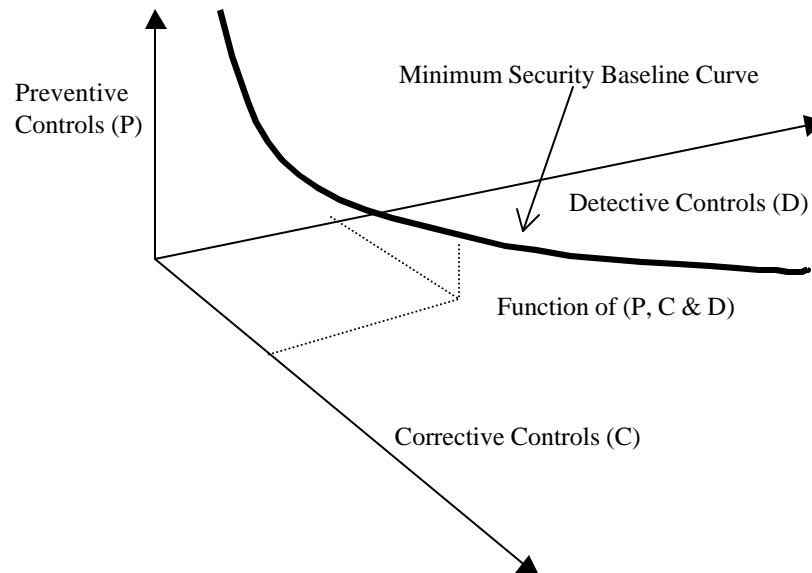

**Fig. 1**   Risk Mitigation Mechanisms and the Relationship to an Information Assurance Baseline

Furthermore, IA mechanisms may be subdivided into three categories: preventive, corrective and detective. Figure one illustrates the underlying risk management concept. For all complex systems, there are myriad combinations of protection, detection, and correction mechanisms that will provide similar qualitative levels of information assurance [4]. Every point on the heavy curve in the figure represents a similar qualitative IA posture achieved through varied combinations of protective, detective and corrective mechanisms and processes. The following standard risk management concepts apply:

- The overall cost of an IA security baseline is a function of the combined costs of prevention, detection and correction mechanisms.
- There are many combinations of preventive, detective, and corrective mechanism that will achieve comparable levels of information assurance.
- Given a fixed budget and a limited number of resources, intelligent combinations of preventive, corrective and detective mechanisms often result in highly cost effective IA architectures.

Risk management is the process of the identification, measurement, control and minimization of security risks in information systems to a level commensurate with the value of the assets protected. The analysis of criticality, vulnerability and threat are the underlying foundations for operational risk evaluation and identification. Risk is greatest where the vulnerability, threat and mission criticality intersect. The remainder of this paper illustrates that the risk management process an organization selects (in order to balance the three types of control mechanisms) is the key to building a successful and cost-effective *Defense-In-Depth* IA strategy.

2.1   RISK MANAGEMENT

As we just discussed, risk identification and management are the function of three variables: criticality, vulnerability and threat. These areas are illustrated in figure two. The first element is criticality – how important is this asset to the mission? The second element is vulnerability – in what ways can the asset be compromised, exploited, damaged or destroyed? The third element is threat – who or what can exploit a vulnerability and what capabilities does that threat have that might be exploited ?

Fig.2 Risk Identification Model
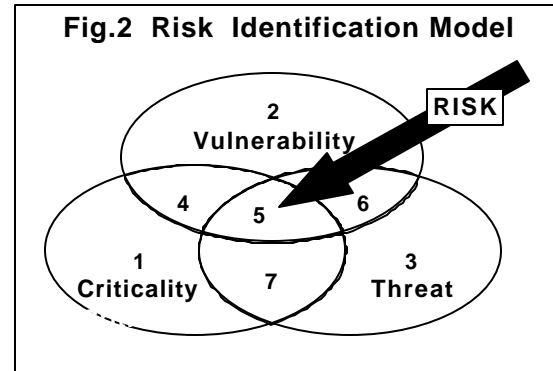
Qualified operational risk is the intersection of these areas: criticality, vulnerability and threat. Therefore, to identify and minimize risks to network-centric operations we must consider the operational context and the relationships among the various components in order to reduce the overall operational risk (illustrated as area five in figure two).

All network-centric information, systems, programs, people, equipment and facilities reside within the network domains circumscribed by the numbered sub-domains illustrated. The following list describes these sub-domains.

1.   Critical assets (information, systems, programs, people, equipment or facilities) for which there is no known vulnerability and no known threat.

2.   Vulnerabilities in systems, programs, people, equipment or facilities that are not associated with critical assets and for which there are no known threats.

3.   Threat environments that have no critical assets or vulnerabilities (or vulnerability information).

4.   Critical assets for which there are known vulnerabilities, but no known threat.

5.   Critical assets for which there are known vulnerabilities and threats. This is the most sensitive area.

6.   A threat or number of threats has acquired specific knowledge and/or capability to exploit a vulnerability although not to critical assets.

7.   Critical asset for which there are no known vulnerabilities, but there is exposure to a specific threat.

2.2   RISK MANAGEMENT REVISITED FOR DEFENSE-IN-DEPTH CONCEPTS

The premise of this discussion is that to minimize the impact of threats and vulnerabilities, and to minimize the potential damage to organizational information, organizations must cost-effectively manage risk and the security countermeasures to minimize exposure. This effort must be focused on mission-criticality and mission-impact. A wide range of choices are available to manage risk. Each mechanism brings with it an operational cost in terms of human, training and fiscal resources; and also in implementation and maintenance costs. Furthermore, such mechanisms may have operational impacts such as increased bandwidth requirements or decreased throughput speeds. For these reasons, risk control mechanisms are broadly clustered into seven defensive areas [5].

1. **Avoidance:** All risk is by-passed by deciding not to process, store or maintain the information.
2. **Transfer of Assets:** Assets at risk are moved outside the risk boundary.
3. **Reduction of Threat**: Mechanism(s) put in place to reduce threat.
4. **Reduction of Vulnerability**: Mechanism(s) put in place to reduce vulnerability
5. **Reduction of Criticality or Mission Impact**: Alter process(es) to minimize risk.
6. **Detection:** Analysis of logs, audit trails, intrusion detection systems, etc.
7. **Recovery**: Appropriate level of backup and recovery processes and mechanisms.

A number of different approaches, methodologies and tools may be employed to manage operational risk in a *Defense-In-Depth* construct. The mechanisms are collectively known in the financial industry as compensating controls. The risk management model in this paper provides a cost-effective way to analyze and apply compensating controls. These controls will be commensurate with the criticality of assets, exploitable vulnerabilities and specific threats. In addition, they will also be commensurate with the resources available and urgency to solve the problem.

The elements below summarize the established information assurance sub-processes used as building blocks of an overall risk management process or program, mapped to standard risk control mechanisms:

Establish Criticality And Mission Impact. Determine what assets are critical to the mission; declare what must be protected and to what extent; (information and information systems) based on an analysis and assessment of what is required to accomplish the mission and the level of information assurance required. [*preventive mechanism*]

Establish Trustworthiness. Work to reduce the threat by establishing a high level of assurance in the trustworthiness of people, practices, systems and programs by identifying existing and future processes, policy, and other trust mechanisms. *[preventive mechanism]*

Strengthen Personnel Security And Management Practices. Develop and support a motivated, skilled and security-responsive workforce. *[preventive mechanisms]*

Protect Information Assets. Control asset sharing, isolate information and capabilities based on need-to-know; create robust backup and recovery plans; identify and reduce known information system vulnerabilities; and employ state-of-practice and new technology to enforce and support security policy. *[preventive mechanism]*

Detect Problems. Actively seek potential threats or problems (accountability for actions through reliable (non-refutable) records of actions and review of recorded action), whether isolated or correlated, that may result in anomalous or malicious activity (detection of unauthorized activity and deterrence). *[detective mechanism]*

React/Respond. Correct suspected and actual unacceptable activity using sound personnel, personnel security and system management practices (mitigation of unauthorized activity), and failing that, seek legal or other appropriate management remedies. *[corrective mechanism]*

In addition to these strategies, an organization must also refine and update policies, procedures and practices to account for changes in operations related to changes in the organizational mission, evolving security environments and advances in technology. These strategies extend beyond boundary protection models.

2.3   RISK IDENTIFICATION AND QUALIFICATION

Risk identification in combination with compensating control identification is the essence of our *Defense-In-Depth* risk management model, not physical boundary protection. In this section we describe a simple 4x4 risk-qualifying model, assuming (in order to simplify the process) that threats exists and are uniform for all connected systems. The figure below illustrates the qualifying model that could be used for the majority of IA risk management operations.
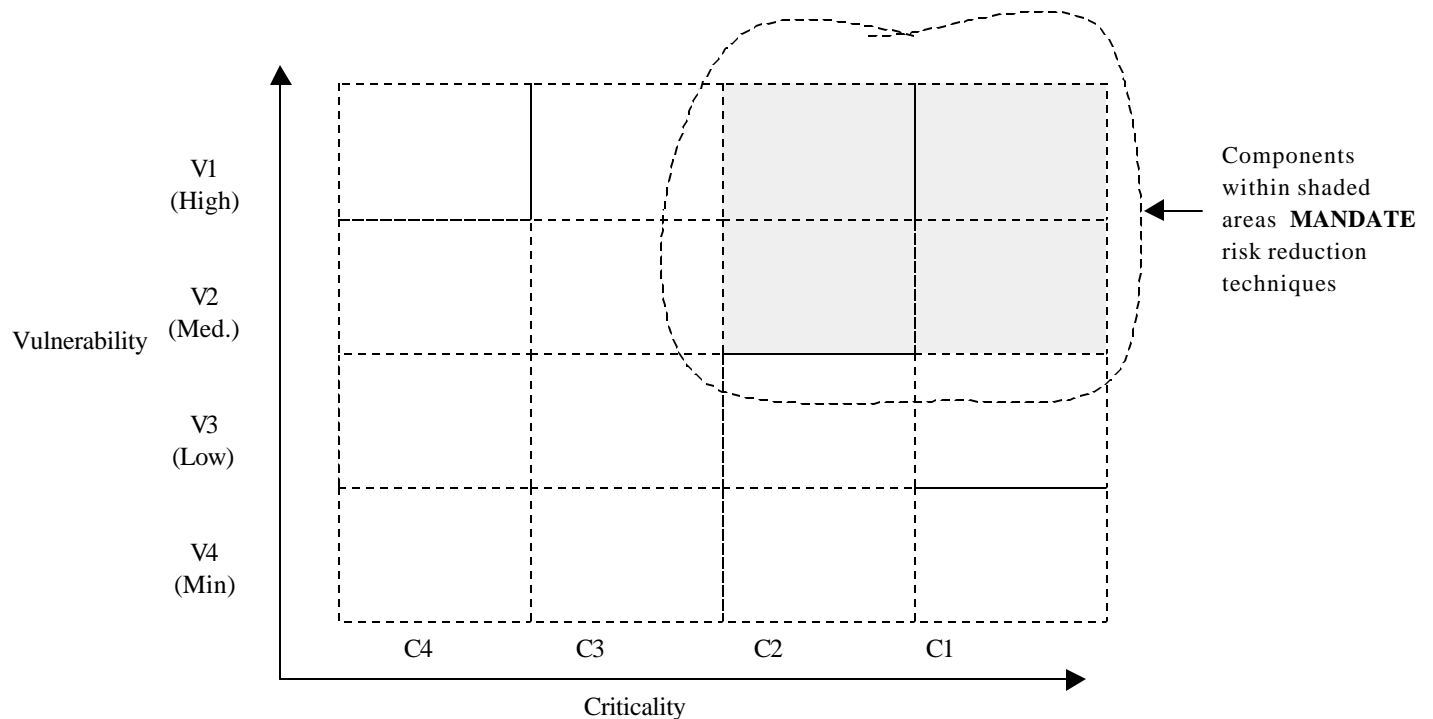

Fig.3. 4 X 4 Risk Qualifying Matrix – Vulnerability vs. Criticality

Vulnerability

The vulnerability axis is a qualitative rating of the potential of the system to be penetrated by unauthorized people or processes. The following vulnerability criteria apply to all identified networks and network elements in the scope of the assessment.

- *V1 - High Vulnerability.* The vulnerability exists; exploitation likely; detection would be difficult; and correction would be costly.
- *V2 - Medium Vulnerability.* The vulnerability exists; exploitation possible; detection possible; correction could be costly.
- *V3 - Low Vulnerability.* The vulnerability exists; exploitation possible; detection possible; correction costs are minimal.
- *V4 - Minimal Vulnerably.* The vulnerability exits; exploitation unlikely; detection is likely; corrective costs are minimal.

Mission Impact or Criticality:

The impact criteria corresponds to the damage to an organization if a vulnerability were actually exploited. The following criteria are routinely used to qualify mission criticality based on long established AF and DoD processes:

- *C1 - Mission Critical.* The loss of the system and/or modification, disclosure or loss of information would cause an immediate end to a direct mission process or halt support of key mission operations and objectives.
- *C2 - Mission Essential.* The loss of the system and/or modification, disclosure, or loss of information would cause an eventual halt to direct mission support of key mission operations and objectives.
- *C3 - Mission Impaired.* The loss of system and/or modification, disclosure, or loss of information would have an effect on (but would not stop) direct mission support of key mission operations and objectives.
- *C4 - Non-mission Essential.* The loss of system and/or modification, disclosure, or loss of information would have no effect on direct mission support of key mission operations and objectives.

Threat: Although normalized in these examples, threats can be from people seeking to exploit the system, from malicious code (Trojan horses, logic bombs, and viruses) or from denial of service.   To simplify the analysis, threats exist all threats are considered uniform. This reduces the process to three major operations in two dimensions:

1. Identifying existing compensating controls that reduce the vulnerabilities.
2. Identifying proposed compensating controls that further reduce the vulnerabilities.
3. Performing the cost-benefit analysis based on both non-recurring (acquisition) costs and recurring (operational, training, and maintenance costs)

3.   AN EXTENDED *DEFENSE-IN-DEPTH* RISK MANAGEMENT PROCESS

In this section we combine all summarized concepts to develop a framework for an extended *Defense-In-Depth* risk management process that may be used in the pre-acquisition, architectural design or other phases of system evaluation to determine risk level. Our goal is a practical, cost-effective risk reduction and management process:

Step 1: Identify System Components and Elements

- Identify all the major system or network components.
- Identify all the inputs and outputs to the system.

Step 2: Define Scope and Boundary of the Problem

Most large heterogeneous interconnected networks cannot be analyzed as a single system. The problems and the tasks are too complex, the input-outputs too numerous, the analysis is time sensitive and the resources are always limited. Hence, the first step is to bound the problem by drawing a dotted line (boundary) around the system components in a logical manner, that:

- defines the major components, and
- defines the inputs and outputs to the system.

Examples of bounded problems/systems include:

- boundary protection devices and routers,
- the network management systems,
- the devices in a DMZ,
- the financial transaction centers,
- the email system,
- the IP backbone,
- the base ATM switch fabric, and
- the local telephone system.

The relationship of the constraining boundary that defines the problem's upper bound to the environment and system interactions should be graphically illustrated at a higher systems view.

Step 3: Identify Subsystems and Components in the Dotted Boundary (or Scope)

After drawing a dotted line around the system, identify the major subsystems, components, elements and software applications. Examples include:

- 10 "Your Favorite Brand" routers running IOS version(s),
- 2 NT DNS platforms running Windows NT v4.1 with Service Pack XXX,
- 2 "Brand Y" firewalls on HP-UX OS Version XZY running application(s) YYY, and
- Ethernet cables – 10BaseT, "Brand X" hubs and switches.

Each component should be given a unique identifier based on the following:

- N-xxx : A Network Component (i.e. router, hub, cable, switch),
- H-xxx: A Host Component (i.e. UNIX , NT server), and
- A-xxx: An Application Component (i.e. email MTA, WWW server, DNS server).

Where 'xxx' is a unique digit numeric identifier.

Step 4: Determine Mission Criticality Qualifier

- After identifying the major subsystems, components, elements, and software applications the relative mission impact should be clearly identified using the criticality scale referenced earlier.

Step 5: Identify Known Vulnerabilities of Each Subsystem in Step 3.

After identifying the major subsystems, components, elements and software applications clearly identify the vulnerabilities. Examples include:

- DNS Bind Version X.4.a on platform H-xxx.
    1. DNS 'named' daemon subject to cache poisoning
    2. DNS port subject to UDP packet flooding, etc.

- WWW Server in DMZ
    1. CGI-BIN hacks for WWW Server Version XYZ
    2. Password Attacks on User Accounts
    3. Denial of Service on HTTPD listening sockets, etc.

Step 6: Identify Existing Compensating Controls Mechanisms, Policies and Processes

After identifying the vulnerabilities, identify and document the existing compensating control mechanisms. Examples include:

- User Accounts on WWW server: Strong PW DLL in place... XYZ version 3.2
- Denial of Service attacks on WWW server: Default number of concurrent TCP/IP connections set to 2000 in kernel configuration
- CGI-BIN vulnerabilities: All CGI-BIN scripts removed, etc.

Step 7: Qualify Vulnerabilities Based on Existing Controls

After identifying the vulnerabilities and compensating controls, qualify the risk (without considering mission impact) using the vulnerability qualifiers of section 2.3.

Step 8: Complete the 4x4 Risk Qualifying Matrix

At this point, each subsystem or component should have a unique identifier, a vulnerability qualifier and a criticality qualifier. In the following format**:**

component identifier (vulnerability level, criticality level) : description

Examples include:

- N-001(V1, C2) : Router 1, Vulnerability level high, mission essential – Access
- H-003(V2, C1): NT server, Vulnerability level medium, non-essential
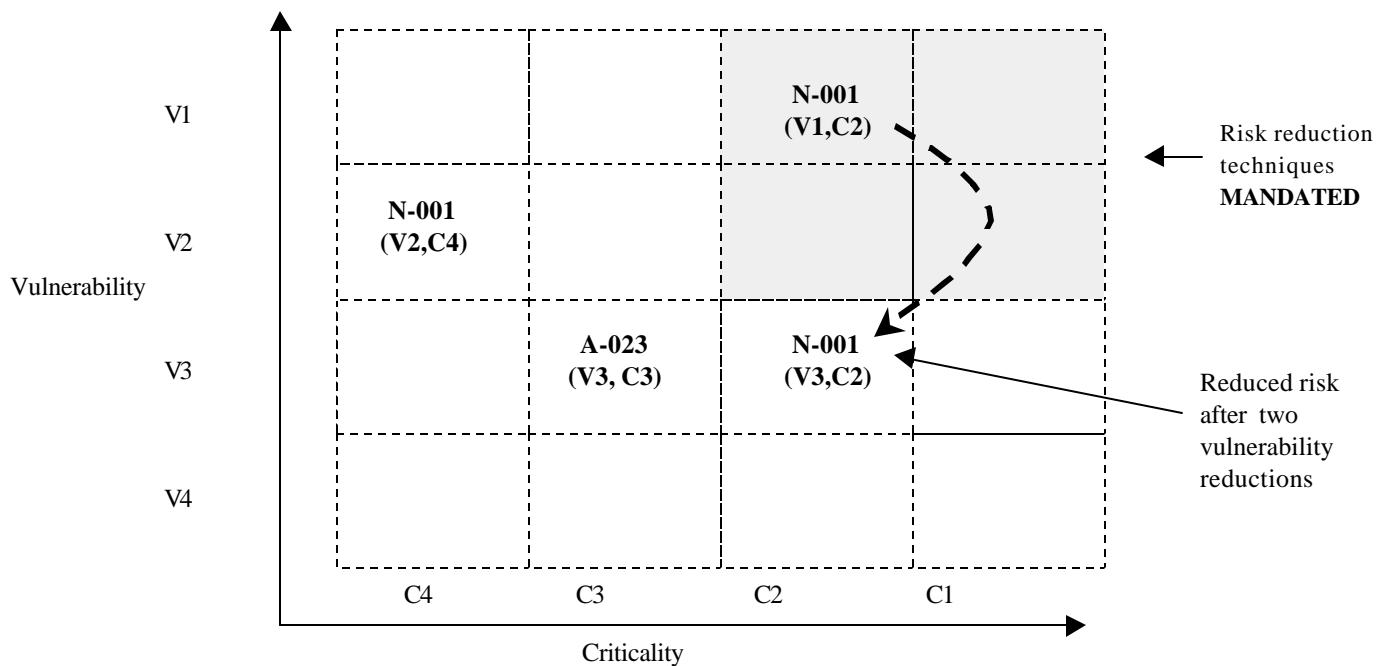- A-023(V2, C3): DNS, Vulnerability low, mission impaired.

Fig.4. Example Application of 4 X 4 Risk Qualifying Matrix

By placing the components on the 4x4 matrix, items that require immediate attention can be readily identified. For example router N-001 clearly falls into the area which has been defined as requiring attention to reduce it risk.

Step 9: The Process of Risk Reduction

The next step in the risk management process is to reduce the high risk components by implementing additional compensating controls. For each identified component, the original vulnerability qualification may be reduced by adding one or more compensating control mechanisms, either network-based, host-based, application-based, or policy-based.. The goal is to reduce the vulnerability by adding the most cost-effective compensating control mechanisms that also lower the risk to the largest numbers (or subsets) of components. The process continues by placing component N-001 in the following example matrix, where "R" equals risk and "CC" equals compensating control. R (primes) indicate reduced risk after specific compensating control mechanisms are applied.

Component	$R_{original}$	CC_{net}	R'	CC_{host}	R''	CC_{app}	R'''
N-001	V1, C2	IP Filters	V2,C2	TACACS+	V3,C2	n/a	n/a

N-001 identifies a common router vulnerability: remote login access to the router via TELNET . In the original risk analysis (example) the router was found to be vulnerable. The suggested compensating controls are:

N-001- R'	$CC_{net:}$ Allow TELNET access to router from only LAN IP address. Reduces risk to (V2,C2)	Acquisition Cost: Minimal Training Cost: Minimal Maintenance Costs: Minimal
N-001- R''	$CC_{app:}$ Required all TELNET access to be authenticated and logged using TACACS+. Reduces risk to (V3,C2)	Acquisition Cost: Minimal Training Cost: Medium Maintenance Costs: Medium

However, are more than one way to reduce risk. Here is another way to accomplish our objective:

N-001- R'	$CC_{net:}$ Allow TELNET access to router from only LAN IP address. Reduces risk to (V2,C2)	Acquisition Cost: Minimal Training Cost: Minimal Maintenance Costs: Minimal
N-001- R''	$CC_{net:}$ Provide secure TELNET via VPN access from authenticated IP address(es). Reduces risk to (V3,C2).	Acquisition Cost: Minimal Training Cost: Minimal Maintenance Costs: Minimal

Here is a more expensive way to reduce the risk.

N-001- R'	$CC_{net:}$ Provide Cisco Secure AAA Services for all Router Access (V3,C2)	Acquisition Cost: Substantial Training Cost: Substantial Maintenance Costs: Substantial

Compensating controls are applied to component N-001 until it moves from the high-risk area identified in the matrix to a lower area. The same process is followed for all components in the high-risk area until the risk of all components

is acceptable. In some cases compensating controls may be available that address vulnerabilities across many components, such as virtual private networks (VPNs) or link encryption. In these cases the boundary must be adjusted to allow the enterprise compensating control to be applied in such a way that it addresses the risk concerns of the defined system.

In the preceding example (provided for illustrative purposes only), the second proposed combination of compensating controls, based on the an organizations future VPN assumption, would be the most cost-effective and would be documented and recommended as the risk reduction measure.

CONCLUDING REMARKS

Boundary protection, generally accepted as the DoD's current *Defense-In-Depth* theme, may have limited usefulness and scaleability in complex internetworks. This paper applies traditional risk management techniques in a uniform network-centric information assurance construct. In particular, the DoD *Defense-In-Depth* model is extended to logical, layered and virtual "boundaries" beyond more traditional physical and geographic boundaries. This approach provides a baseline framework for understanding how *Defense-In-Depth* could be extended to increasingly complex operational environments.   High levels of cost-effective information assurance may be achieved by consistently applying a uniform risk management methodology to systems and processes; for example, the methodology presented in this paper. The acquisition of network security technology without a uniform risk management process is significantly less secure and less cost-effective than a simple, uniform and disciplined risk management approach.

Effective risk management methodologies must be traceable and complementary to the systems requirements and design process. The qualitative methodology presented in this paper provides an expanded *Defense-In-Depth* framework that will significantly reduce operational risk, optimize system resources, reduce costs, document processes and the application of compensating controls. The method outlined has been successfully applied to many organizations including commercial financial systems, military systems, and other large organizations that depend on network-centric operations for their core business/mission processes. We hope the reader will carefully consider the economic and information assurance benefits of extending the *Defense-In-Depth* boundary protection model to a uniform risk management model that is based "less on the acquisition of boundary protection technology" and more on "the application and rigor of a structured risk management process."

REFERENCES

[1]   "Information Assurance through Defense-in-Depth," Directorate for Command, Control, Communications, and Computer Systems, U.S. Department of Defense Joint Staff, February 2000.

[2]   Rochin, Gene, "Trapped in the Net: The Unanticipated Consequences Computerization," Princeton University Press, Princeton, NY, 1997.

[3]   Abrams, M., Jajodia, S., and Podell, Editors," Information Security: An Integrated Collection of Essays," IEEE Computer Society Press, Los Alamitos, CA, 1995.

[4]   Mollema, K., "Audit of Information Processing," Elsevier Advanced Technology, Oxford, United Kingdom, 1989.

[5]   Jackson, K., Hruska, J., and Parker, D., editors, "Computer Security Reference Book," CRC Press, Butterworth-Heinemann, Ltd., Boca Raton, FL, 1992.