AFIT/GIR/LAS/99D-2

NETWORK SECURITY VERSUS NETWORK CONNECTIVITY: A FRAMEWORK FOR ADDRESSING THE ISSUES FACING THE AIR FORCE MEDICAL COMMUNITY

THESIS

Franklin E. Cunningham, Jr., Captain, USAF

AFIT/GIR/LAS/99D-2

Approved for public release; distribution unlimited

The views expressed in this article are those of the author and do not reflect the official policy of position of the United States Air Force, Department of Defense, or the US government.

AFIT/GIR/LAS/99D-2

NETWORK SECURITY VERSUS NETWORK CONNECTIVITY: A FRAMEWORK FOR ADDRESSING THE ISSUES FACING THE AIR FORCE MEDICAL COMMUNITY

THESIS

Presented to the Faculty of the School of Engineering

and Management of the Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Information Resource Management

Franklin E. Cunningham, Jr., B.S.

Captain, USAF

December 1999

AFIT/GIR/LAS/99D-2

NETWORK SECURITY VERSUS NETWORK CONNECTIVITY:

A FRAMEWORK FOR ADDRESSING THE ISSUES FACING

THE AIR FORCE MEDICAL COMMUNITY

Franklin E. Cunningham, Jr., B.S.
Captain, USAF

Approved:

David P. Biros — 14 Dec 99

David P. Biros, Major, USAF, Ph.D. — date

Advisor

Alan R. Heminger — 14 Dec 99

Alan R. Heminger, Ph.D.. — date

Reader

Acknowledgements

Several people provided me with considerable assistance in this thesis project and deserve to be recognized. I wish to acknowledge the contributions of the support base and medical center representatives who graciously gave their time and knowledge in providing the Air Force and major medical center data that was so critical to this research effort. I also wish to thank the various faculty members of the Air Force Institute of Technology for their assistance in this endeavor. My thanks go out to Dr. Alan Heminger, Major Morris, Dr. Guy Shane, Major Paul Thurston, and Major Michael Rehg. The critical review and direction they provided to the thesis effort helped immensely. Lastly, I am indebted to my thesis advisor, Major Dave Biros, for his encouragement, direction, and assistance in the course of this endeavor. Without the significant contributions of all these fine people, I would have been unable to complete this research project.

In closing, I thank those closest to me for their unwavering support during this wonderful educational opportunity. To my son, Bryan, and my daughter, Emily, I wish to express my unwavering love and thanks. To my dearest Tina, my companion, my friend, my love and my wife, I thank you most deeply. You have always been there for me and for our family; you push me to excel and love me in spite of my failings. Your support during these last 18 months, as always, has been monumental and has allowed me to gain the most from this experience.

Table of Contents

List of Tables

Abstract

Air Force organizations have been directed to implement the Barrier Reef concept to secure their unclassified networks. The Air Force medical community relies on much of its network connectivity through the Air Force networks, yet it maintains other network links to numerous other governmental and civilian organizations. For the Air Force medical community to comply with Barrier Reef, it will either have to sever its external links or configure them in such a way that the links meet the requirements of Barrier Reef. These links are mandated by direction from the office of the Assistant Secretary of Defense for Health Affairs (OASD(HA)) and support more than 100 automated information systems. To resolve this problem, the OASD(HA) directed the Tri-Service Infrastructure Management Program Office (TIMPO) to develop a robust, secure, standards based an infrastructure that will interoperate with the Air Force, Army, and Navy networks and comply with each Service's network security measures. The TIMPO is moving forward with that direction. Of concern, however, is that there is not a clear understanding of all the underlying issues.

This research performed an exploratory study to further clarify the underlying issues. A framework of these network issues was developed from data collected by network field experts from the Air Force's major medical centers and the corresponding base network organizations. The issues from the collected data were compared to issues considered by TIMPO. The TIMPO plan matched closely to the framework developed directly from the research. The findings were combined into a single framework. The

composite framework that resulted more completely identifies network issues that any potential solution to the Air Force medical network dilemma should consider. The TIMPO plan seems to be on track. It addresses 13 of the 19 identified areas and partially addresses three other issue areas. The success of the TIMPO plan may be improved if the remaining issues can be addressed.

The remaining issues include the lack of central management for all military networks. TIMPO represents the Office of the Assistant Secretary of Defense for Health Affairs, and each Service has its own network controlling authority. No one organization directs the actions of all of these organizations. Additional issues include more consideration to social engineering issues, continuity of personnel, dependence of medical organizations on long-term contract partners. These issues have relevance for addressing potential network solutions for the Air Force medical community.

NETWORK SECURITY VERSUS NETWORK CONNECTIVITY: A FRAMEWORK FOR ADDRESSING THE ISSUES FACING THE AIR FORCE MEDICAL COMMUNITY

I. Introduction

In the past decade the Internet and other network activities have become integral parts of how the Department of Defense (DoD) conducts its official business. During this time, people intent on stealing, damaging, and destroying military information, or otherwise impacting its business have increasingly targeted the DoD networks (GAO/AIMD 96-84; Denning, 1999). Due to the growing dependence on its networks and the targeting of its systems, the Air Force has placed high importance on securing its information and networks (Libicki, 1997).

Air Force networks are not totally isolated from the rest of the Internet. As a result, the Air Force implemented a security plan called Barrier Reef to eliminate unauthorized access to its networked systems and information. According to Headquarters Air Force Communications Agency (AFCA) Information Protection Technical Services Branch,

> Protection of information and network resources has become an essential component of our national defense. This age of network inter-connectivity for the completion of our daily business, combined with the real threat of information warfare from any device linked to the Internet, has left the Air Force and Department of Defense information resources vulnerable to denial of service, theft, and destruction. *Joint Vision 2010* and the Air Force 21st Century vision document *Global Engagement* both confirm the key role of information superiority and call for increased management and protection of information. The proliferation of dissimilar

> protection systems being fielded by individual bases threatens logistical supportability and has not been successful in increasing the overall security of Air Force networks. An effort by the Air Force Communication and Information Center called Operationalizing and Professionalizing the Network is currently underway to fix these disconnects. The Barrier Reef, having been established by USAF/SC as the corporate Air Force concept for boundary protection of our information networks, provides Air Force professionals a process for building strong network perimeter defenses. (HQ AFCA/GCIT, 1997)

In a recent message, the Chief of Staff of the Air Force highlighted the importance placed on protection of Air Force networked systems, as follows:

> We need to redouble our efforts to put all networks on our bases behind the network control centers. The acting secretary [of the Air Force] and I will be personally reviewing our progress in getting every system on each installation behind the network control center and monitored and protected by the tools we have fielded. (CSAF, 1998)

The Air Force's network security concept of Barrier Reef affords controlled access to Air Force networks by authorizing users who are specifically granted access by network administration in accordance with Air Force policy and procedure. This security comes at a price. While protecting its own networks, the Air Force has not addressed the impact of this fundamental shift in policy and procedure on other organizations that ride its networks.

Barrier Reef is in conflict with the operation of the Military Health System (MHS) (TIMPO, 1999). The MHS delivers health care globally to all military components and uses/maintains more than 100 medical software applications in support of this mission (TIMPO, 1999). The Air Force component is the Air Force Medical Service (AFMS), which uses MHS to support its mission of providing military health care. Although the AFMS provides these services primarily in support of the Air Force, and typically resides on Air Force installations, it remains under the jurisdiction of the

Assistant Secretary of Defense for Health Affairs (OASD(HA)). That is, its budgets, personnel, and operations all lie under the OASD(HA)'s control (Johnson, 1999).

At the same time, the Air Force medical facilities work in close association with the bases they support. The main network connectivity for the medical facilities has been provided (funded and maintained) by the support bases, and other downward-directed network connections are supported as separate entities. One significant issue in this regard is interoperability. Prior to the Air Force directive to implement Barrier Reef, the AFMS was able to operate in a very open network configuration with numerous links to various governmental and commercial organizations. These other organizations were allowed direct access to the medical network for contractor provided support services (e.g. just-in-time medical supply service) for information sharing between military and commercial medical facilities and other reasons. Barrier Reef, however, directed that this open access be discontinued. All of the networked systems are protected with a series of security measures to ensure that only authorized personnel use the systems. To provide this protection, connectivity to any part of the network must come through the protected entry point of the Barrier Reef.

This leaves the medical community only two options with respect to its network connectivity. First, it can take action to comply with the requirements of Barrier Reef and stay behind that protection. This can be accomplished either by rehoming (changing the point of connectivity into the network) and reconfiguring its various network connections to come through the single access point to the protected network or by discontinuing them. Second, the medical community can isolate itself from the rest of the base network and operate in isolation. Neither of these options are simple fixes.

Significant investment in time, configuration management, equipment, and other expensive resources are involved as are various laws, mandates, and contractual obligations.

The job of rehoming the 100 plus MHS automated information systems (AIS) to comply with the restrictions of Barrier Reef is a big challenge. They are built to varying standards, and many are unique, proprietary configurations. Additionally, many of these legacy systems do not have current levels of security built into them, and the funding to add it now is not available (TIMPO, 1999). Instead of rebuilding the individual system, the cheaper, easier, and quicker decision is to secure the infrastructure that these systems use. There are complications with this idea too. Some of the required MHS AISs use high-risk protocols that are usually blocked by the base network security because of their high levels of risk (TIMPO, 1999). If these high-risk protocols are allowed past the network security measures, the base networks, and in turn the Air Force networks, are at significant and unnecessary risk. Therefore, another solution is needed.

In essence, the operational Air Force bases and the Air Force medical community have fundamental differences in their design and purpose. The two entities are also different from a connectivity perspective. The base information systems are set up in a flat architecture. They each have connectivity that is essentially independent of every other base. The MHS links are set up more hierarchically. Many of the Medical AISs link outlying facilities to regional centers that then relay the information to another regional center or to another facility within its span of control. That is, the major (regional) medical centers act as information hubs for all the facilities within a particular region. The smaller outlying medical facilities link to each other through these hubs and

share information on a variety of activities (Johnson, 1999). This design complicates the resolution of the MHS dilemma.

The medical centers are being forced to comply with the Air Force direction, impacting their network association with military units and their trading and commercial partners. If they do not comply, they will be isolated from the rest of the Air Force networks and left to deal with their network security issues without the support of the bases on which they reside. Most of these facilities lack the network equipment, personnel, and budget to effectively deal with this issue on their own.

The fundamental purpose of base information systems is to provide information in support of the warfighter while the purpose of the medical service is to facilitate information sharing in support of patient care. This difference may impact the way in which the two entities look to resolve the network security issue.

Assumptions and Definitions

The following key terms and concepts are important in this research:

- **Air Force Medical Treatment Facilities** are Air Force operated healthcare organizations that include Air Force hospitals and clinics of varying sizes.

- **Air Force Hospitals** are Air Force operated medical treatment facilities that have the capability of caring for inpatients. Air Force hospitals are hierarchically organized into three categories: medical centers, regional hospitals, and hospitals, depending on the number of inpatient beds in the level of staff specialization and ancillary services sophistication. Air Force hospitals of all sizes also support outpatient clinics that treat patients not requiring an overnight stay as an inpatient.

- **Air Force Medical Centers** are Air Force hospitals operating the largest number of inpatient beds. They also support a number of medical subspecialties with sophisticated ancillary services. These facilities receive referral patients from lower-level Air Force hospitals, provide specialized care and consultation services, and sponsor

residency programs for professional staff members and postgraduate specialty training.

- **Barrier Reef** is a 12-step process for configuring, monitoring, and protecting Air Force networks where access to the trusted portion of the network is restricted to users authorized by the internal network administration using specific Internet protocols and demonstrating the proper *virtual* credentials.

- **Electronic Commerce** describes an expanding world where businesses deal directly with customers without relying on *external* value-added network providers—clearinghouses (Segev, 1998).

- **Electronic Data Interchange,** as defined by private industry and the American National Standards Institute, is a technique by means of which formatted, transactional information is moved electronically from one organization's computer to another's (Payne, 1991).

- **Firewall** is a device that sits between an internal network and the rest of the network. It filters packets of information as they go by, according to various criteria settings (TIMPO, 1999).

- **INFOCONs,** or Information Conditions, are designations that let Air Force organizations know how safe their information exchange systems are, or if they should be used at all (Loftin, 1998). They work much like the threat conditions (THREATCONs) that inform personnel of the current threat of terrorist activity.

- **Internet Protocol (IP)** is the Institute of Electrical and Electronic Engineers (IEEE) standard for addressing network nodes and reference points for establishing network connectivity.

- **Network Security** is comprised of policies, procedures, and implementation of technical solutions to protect networks assets. Involves password and administrative management to allow authorized traffic and deny all else (HQ AFCA/GCIT, 1997)

- **Partner Access** refers to any connection that provides access from the corporate Intranet to another location outside the organization (Blackwell, 1999).

- **Public Key Infrastructure** (PKI) is the foundation for digital trust across an enterprise. (TIMPO, 1999)

- **Proxy** is an application-level gateway that does not allow data packets to pass directly between two networks. An initial connection is made with the proxy which determines whether to establish a connection from the proxy to the requested destination. Proxies can provide greater security but at the tremendous loss of performance (TIMPO, 1999).

- **Trusted Agent** refers to official users of computer/network systems who are specifically granted access to the network or network services by network administration in accordance with Air Force policy and procedure.

- **Trusted Network** is a network configuration where all authorized users stay within the *virtual* confines of the network and communicate with the outside world by proxy. That is, the network links the user to a computer or server outside the network and uses that computer to communicate (as an intermediary). The benefit is that people outside the network see the proxy as the site generating a link, but in theory that link can not be traced back to the original user. The original user uses the IP address of the proxy much as people use post office boxes for regular mail.

Statement of Problem

Both the Air Force and the Air Force Medical Service (by action of the OASD(HA)) have been working to address the networking concerns for the past three years. The Air Force continues to push for security of its systems while the medical community maintains its need for connectivity, and these two concepts appear not to be easily resolved. Many organizations have put forth ideas that address one area of interest or another; however, little research has been done to identify all the relevant areas. This has resulted in lack of clear understanding of all the issues involved in developing a solution to the Air Force medical network problem. This thesis collected data from Air Force major medical center network experts for establishing a framework of issues. The issues in the framework should be considered for any potential solution to the Air Force

medical community's problem of providing the required network connectivity while securing its networks.

To do this several areas require investigation. What is the importance of network security? What is the need for information system connectivity between trading partners? What is the network security and network connectivity situation for Air Force hospitals? What possible solutions are being looked at for the Air Force hospitals? Answers to these question areas may provide further insight into the research problem.

Summary

The Air Force's increased reliance on network connectivity to support its mission and the rise in attacks on its systems have led the Air Force to implement the restrictive network security concept of Barrier Reef. The result of this change in procedure has left the MHS of the medical community with a problem. To stay within the protection provided by Barrier Reef, the medical community needs to find a way to securely rehome the various network connections or they must sever them. If it chooses to isolate itself from the rest of the Air Force networks, the Air Force medical community would need to develop and maintain its own infrastructure. The purpose of this research is to uncover the underlying issues of any potential solution to the Air Force medical network dilemma.

Chapter II will cover the current research and general literature relevant to the area of Air Force and Air Force Medical Service network security and connectivity. Chapter III will explain the methodology used in this study to establish the framework of issues that any potential solution to this problem should include. Chapter IV will present the data analysis and results from the data collected. Chapter V will discuss the findings

of the study and their relevance to the problem. It will also present limitations of this study and recommendations for future research.

II. Literature Review

Introduction

As the Air Force moves to comply with the Air Force Chief of Staff's 1998 mandate to protect all of its networks using Barrier Reef, it is wrestling with the best manner to maintain needed connectivity to its various elements while protecting its information and information systems. The Air Force has become reliant on networks and the Internet for processing and transmitting information almost instantaneously to its dispersed organizations, to other federal offices and departments, and to outside organizations and individuals (Dodaro, 1998).

The need of the Air Force major medical centers to comply with Barrier Reef network security measures while maintaining outside connectivity with its affiliates requires further investigation. Its open configuration is prompted by downward directed programs from the Air Force and Department of Defense, and as a natural development to share information among medical professionals and organizations.

Security as a Necessary Endeavor

Increased Attacks on Information Systems. Attacks on Department of Defense information technology and networks are on the rise (GAO/AIMD 96-84; Denning, 1999). The same factors that benefit federal operations, speed and accessibility, also make it possible for individuals and organizations to inexpensively interfere with or eavesdrop on these operations from remote locations for purposes of fraud or sabotage, or other malicious intent (Dodaro, 1998). Recent General Accounting Office audit evidence

indicates that serious and widespread weaknesses in information security are adversely affecting the United States government's ability to adequately protect critical government operations, such as national defense. The assets associated with these operations are also at great risk for fraud, disruption, and inappropriate disclosures (GAO AIMD 98-92). Another source reported that significant information security weaknesses have been reported in each of the 24 largest federal agencies, with inadequately restricted access to sensitive data being the most widely reported problem (Dodaro, 1998).

An earlier report from the General Accounting Office identified attacks on Defense Department computer systems as a serious and growing threat (GAO AIMD 96-84). The same report cited the Defense Information Systems Agency as stating that the Defense Department may have experienced as many as 250,000 attacks in 1996. This number is only an estimate based on the actual number of reported attacks and adjusted for the "estimated" percentage of reported versus actual attacks (Smith, 1998). Even so, the high number of estimated individual attacks indicates that the Department of Defense is high interest target. Research indicates the number of reported cases is only a small fraction of the actual number of attacks that take place (CERT, 1999; GAO AIMD 96-84; Adams C., 1997).

According to Defense Information Systems Agency estimates, nearly two-thirds (65%) of all the estimated attacks were successful in breaching networked government systems (GAO AIMD 96-84). It also reports that the number of attacks is doubling each year as the size of the Internet increases and as the capabilities of hackers and hacker tools improve (GAO AIMD 96-84). Other assessments report different findings. The national-level Computer Emergency Response Team (CERT) Coordination Center

receives incident reports from both the public and private sector. Statistics provided by the CERT Coordination Center indicate that the number of incidences the Center handled rose dramatically from 1988 through 1994 but reached a plateau in that year. Table 1 reflects these findings, as well as the significant increase reported in the first three quarters of 1999.

Table 1. Computer Emergency Response Team Statistics, 1988 – 1999

YEAR	Number of Incidences Handled
1988	6
1989	132
1990	252
1991	406
1992	773
1993	1334
1994	2340
1995	2412
1996	2573
1997	2134
1998	3734
1999 (Quarters 1,2,3)	6844
	Total: 22,940

Effects of Attacks. The impact of computer system attacks can vary greatly. Cosmetic alteration of public access web pages, effectively graffiti on the Internet, is typically a nuisance crime. This type of attack alters very little data and can be perpetrated without gaining access to the entire system. Correction of these actions often requires minimal effort. However, other effects such as reduced trust and reliability concerns harbored by users of the information may be a greater problem. Some companies may be more concerned by the loss of customer confidence and its impact on future business (Stackpole, 1998).

A greater potential impact from a network attack is denial of service. A denial of service attack is defined as an incident in which a user or organization is deprived of a network service or resource that would normally be available (Denning, 1999). Affected resources could include electronic databases, mail service or Web site access (Whatis.com, 1999). This denial can result from many different factors such as computer virus, hacker attack, sabotage, hardware failure, natural disaster, an accident, or operator error. Whatever the cause, these loss-of-service attacks force one to conduct business without the support of automated systems (Stackpole, 1998). The effect of these attacks can vary greatly depending on the operating procedures of the organization and the extent to which the organization is dependent on the lost services. Additionally, there are valid concerns with respect to liability, or collateral losses, that are often associated with denial of service and data loss/theft costs. These liabilities may include fines for violating regulatory directives or civil penalties for failing to exercise due care.

In addition to loss of access to networks and networked data, another concern is the loss of data due to theft. Some data is highly desired, and the risk of theft for that data can be affected by the precautions taken. If an information system is left unprotected, an attacker can simply use software programs or other means to intercept, read, and redirect the data that he desires. The impact of the theft will vary. The impact of losing a single set of data may mean anything from not properly handling a $10 transaction to Coca-Cola's® secret formula being compromised. Attackers may choose instead to destroy or corrupt data using malicious logic or some other means of manipulation. Just as with data theft, the action of corrupting and destroying data can be accomplished without detection. The impact of these actions can have varied results.

At best, these attacks are a multimillion-dollar nuisance to the Defense Department; at worst, they are a serious threat to national security (GAO AIMD 96-84). Attackers have already gained access to critical information that could affect our work and capability. They have seized control of entire Defense systems, many of which support critical functions, such as weapons systems research and development, logistics, and finance. Attackers have also stolen, modified, and destroyed data and software (GAO AIMD 96-84).

During the Gulf War, five hackers from the Netherlands penetrated computer systems at 34 Air Force military sites, including some that directly supported operations Desert Shield and Desert Storm. The attackers were able to access information about precise troop locations, armament, capabilities, and movement of American naval vessels in the Gulf region. Unconfirmed reports also disclose that the Dutch hackers tried to sell the information to Iraq during the Gulf War conflict. Based on information he said was received from government officials, Eugene Shultz, then manager of the Department of Energy's Computer Incident Advisory Capability, reported to the British Broadcasting Corporation that Saddam Hussein had been offered the data through an intermediary. (Denning, 1999)

This is not an isolated incident. A General Accounting Office report recounted another well-publicized incident: an attack on Rome Laboratory, the Air Force's premier command and control research facility. Two hackers took control of laboratory support systems, established links to foreign Internet sites, and stole tactical and artificial intelligence research data. The potential for catastrophic damage is high. Organized foreign nationals or terrorists could use information warfare techniques to disrupt military

operations by harming command and control systems, public switch networks, and other systems or networks on which the DOD relies. (GAO AIMD 96-84)

Due to these continual onslaughts and known vulnerabilities, the Department of Defense has directed several security actions including protection, detection, and reporting of these cases. Based on this direction, the Air Force has initiated numerous protective measures for its computer networks. As a basis for developing these protective measures, understanding our vulnerabilities and the capabilities of our attackers are critical factors. In the words of Sun Tzu, "Know your enemy and know yourself" (Sun Tzu Translation by Griffith, 1963).

Methods of Attacking Networks. Much research has also been done to analyze the type and purpose of various attacks against networked systems (Blackwell, 1999; Dodaro, 1998; Howard, 1997, etc.). Depending on the nature of our adversary's intent, an attacker tends to take the precautions he feels are necessary to evade detection and prosecution (Caldwell, 1990). Insider attacks are reported to be the most prevalent and are estimated at 70 – 80 percent of all attacks (Debreceny, 1998). The attacks in this case may involve theft, damage, etc. to data the attacker has authorized access to. The attacks may also extend to unauthorized areas. These attacks are often more successful because much of the network security efforts is focused on keeping unauthorized people from gaining access to the system (Debreceny, 1998). Insiders bypass these outward looking measures.

The other avenue of attack involves attacks from outside the organization. These external attacks can be straightforward from the attackers computer system to the target system. However, to decrease the likelihood of being caught, the attacker can use a

technique called looping, where a number of intermediate systems are penetrated en route to the target system, to escape detection (Caldwell, 1990). The ability to involve intermediate systems and even to cross international boundaries further obscures the situation.

These attacks can occur in forms of varying complexity. A common means of performing an indirect attack is for an adversary to gain access to some third party's system and to use that system as a platform from which to launch an attack. Using one intermediate system is the most basic form of an indirect attack. One well-known example is the attack for which Kevin Mitnick, an infamous hacker of government systems, was eventually imprisoned:

> The attack began on another system—one owned by a colleague of Shimomura's—the authorized user whose system was the intended target. There the attacker looked for "trusted relationships" between this machine and other machines, such as Shimomura's. Once these were determined, the attacker broke into Shimomura's machine by using the other machine's address, pretending to be his colleague's machine. To cover his tracks, the attacker occupied the trusted machine with spurious requests to keep it from issuing error messages. Once the machine was broken into, the attacker installed software to assist in future illicit use of the station. The entire attack took less than 16 seconds. (Fisher, 1995)

Since the Department of Defense and other government agencies maintain the capability to trace an attack through multiple systems, its adversaries have employed the concept of looping to help hide their trail (Fisher, 1995; Denning, 1999). To further complicate tracing these individuals, the attackers can employ intermediate systems in a number of foreign countries. This inhibits the Federal government's ability to trace the attacker back to the source by involving international law and sovereign rights of these foreign countries.

Even if the attacks come from within the United States, the government is limited in the action it can take. The government must take steps not to violate the rights of its citizenry. In the Department of Defense's case, it is not allowed to take any action against citizens of United States. The privacy rights of the United States citizenry impede the tracing of attackers if they use a third party's system to facilitate an attack. Permission for access to and monitoring of intermediate systems must be gained by law enforcement official from the lawful owners. The law does not currently allow for use of "hot pursuit" to circumvent these restrictions. Thus, preventing successful attacks becomes even more important.

Risk Management. Federal agencies must take steps to understand their information security risks and implement policies and controls to reduce these risks (GAO/AIMD-96-110, 1996). In September 1996, the GAO reported that a broad array of federal operations was at risk due to information security weaknesses A common underlying cause for these vulnerabilities was inadequate security program management (GAO/AIMD-96-110, 1996). In that report, GAO recommended that the Office of Management and Budget (OMB) play a more proactive role in leading federal improvement efforts, in part through its role as chair of the Chief Information Officers (CIO) Council. Subsequently, in a February 1997 series of reports to the Congress, the GAO designated information security as a new government-wide high-risk issue (GAO/AIMD-96-110, 1996). More recently, in its March 31, 1998 report on the Federal government's consolidated financial statements, the GAO reported that widespread computer control deficiencies also contribute to problems in Federal financial management because they diminish confidence in the reliability of financial management

data (Dodaro, 1998). Clearly these are significant areas of concern that needed to be addressed.

Threat Identification. The first step in the process of risk management is risk assessment. This step involves the identification of assets to protect, the threat to those assets, the extent of the vulnerability, the likelihood of that threat coming to fruition, the loss that could result, and the potential safeguards that could be installed (Denning, 1999). Management must ensure that information security measures are appropriate in relation to the value of the assets and the threats to which they are vulnerable (Hayes and Ulrich, 1998). The security of information assets, with regard to the value of their confidentiality, integrity, and availability, and the security of the supporting information technology resources must be assured by well-informed owners, managers, custodians, or other responsible parties (IISF, 1999).

Research indicates a few discrete sources for the external threat to networked information systems: access to the system by hackers, infiltration of a system with malicious logic, access to the system by competitors, and damage caused by natural disaster (Loch, 1992, Denning, 1999). All of these concerns must be considered in terms of the damage that can result, and the preventive actions that can be put into place.

Proportionality Principle. The Generally Accepted System Security Principle (GASSP) of proportionality establishes the importance of balancing the security precautions taken to the risks of modification, denial of use, or disclosure of the information. In essence, security controls should be commensurate with the value of the information assets and the vulnerability. The value, sensitivity, and criticality of the information, and the probability, frequency, and severity of direct and indirect harm or

loss must be considered. This principle recognizes the value of approaches to information security ranging from prevention to acceptance. (IISF, 1999)

Some organizations determine information security measures based on an examination of the risks, associated threats, vulnerabilities, loss exposure, and risk mitigation through cost/benefit analysis using a Risk Management Framework. Other organizations implement information security measures based on a prudent assessment of "due care" (such as the use of reasonable safeguards based on the practices of similar organizations), resource limitations, and priorities. (IISF, 1999)

Periodic Reassessment. The nature of the network environment is constantly changing. New information needs, dynamic cooperative associations, and rapid technological advances are driving those changes. To stay up to date, all network security measures, policies, and procedures should be periodically reviewed for currency and completeness (IISF, 1999). Risks to the information, to its value, and to the probability, frequency, and severity of direct and indirect harm/loss should also undergo periodic assessment to identify and measure the variances from available and established security measures and controls (IISF, 1999). Based on findings in the reassessment, management can then make an informed risk management decision whether to accept, mitigate, or transfer the identified risks with due consideration of cost effectiveness (IISF, 1999). The list below provides some guidelines for when a reassessment is warranted:

Events that may trigger the need for a security assessment:

- A significant change to the information system
- A significant change in the information or its value
- A significant change in the technology
- A significant change to the threats or vulnerabilities
- A significant change to available safeguards

° A significant change in the user profiles
° A significant change in the potential loss of the system
° A significant change to the organization/enterprise
° A predetermined length of time since last assessment
(IISF, 1999)

Network security is a critical success factor in electronic commerce. The government has been better able to allocate funds to upgrade security for its information systems than has each element of the private sector. Many businesses have become quite skilled at protecting critical business information (patents, research and development, formulas, etc.) but typically have not allocated the resources to apply the same defensive capability throughout their enterprises (Segev, 1998).

IBM has taken network security steps similar to the Air Force's Barrier Reef concept. IBM has developed a 4-step checklist to help its customers perform risk assessment for their networked systems and take action for mitigating that risk (McMullen, 1998). McMullen details how this IBM checklist can form the basis of an integrated security policy. First, **Know your** [organization's] **value** and what information needs to be protected. This requires the organization to be able to assign worth to its information. Second, **Know your network**; this involves knowing all the systems entry/exit points. Many organizations run into security problems by not knowing how the system is linked to the outside world: modems, secondary network connections, etc. Additionally, many organizations only look to external sources when addressing vulnerabilities. As noted previously, 70 - 80 percent of all system abuses and network incidents can be attributed to internal threats (Debreceny, 1998). Third, **Know the threats**; this means keeping abreast of vendor-specific advisories and technological advances. Another possible source of vulnerability is from added interactivity between

the organization and its suppliers and customers. Fourth, **Know your plan**; here the importance of having a planned response to network problems that may occur is stressed. Proper planning for a virus or intrusion may allow for a more thorough reaction and allows for controlling the situation with minimal impact to the organization (McMullen, 1998)

Other efforts to establish fundamental guidelines for promoting effective network security have produced promising results. The International Information Security Foundation-Sponsored Committee developed and distributed Generally Accepted System Security Principles throughout the international community (ISSF, 1999). The principles form a framework that addresses many of the same concerns identified by the Department of Defense. The committee paid considerable attention to the role of management in establishing network security measures. It states that an organization's management shall ensure that policy and supporting standards, baselines, procedures, and guidelines are developed and maintained to address all aspects of information security. Specifically, the organizational management should consider the potential impact on the shared global infrastructure, e.g., the Internet, public-switched networks, and other connected systems when establishing network security measures. Another method of improving network security in support of electronic commerce is encryption.

Encryption. One strategy that may help reduce the risk posed by attackers is to keep a "low profile" on electronic networks and limit disclosure of security measures. Publicizing the robustness of a network's security measures only seems to invite hackers to attack the security system (Fotsch, 1996). In addition to the proliferation of management policies and procedures, many software and hardware developments have

enabled better protection of networked systems. Since the theft of information that resides on computer/network systems typically has been of interest for attackers, one mechanism for furthering the protection of network assets has been the development of robust encryption tools. Encryption in this area affords two main benefits: protection of data in transit and protection of that data as it resides on the network in servers or in other forms of data storage.

These practices have definite applicability in supporting both public and private sector networks. The National Security Agency, in collaboration with the National Institute of Standards and Technology, has developed the National Information Assurance Partnership (NIAP) which will meet the security requirements of both producers and users of security products and services. The NIAP initiative will help both public- and private-sector users to evaluate, compare, and select the security products and services that best meet their needs. Moreover, the Department of Defense is in the process of establishing an integrated, Department-wide Public Key Infrastructure (PKI) to provide a foundation for security services at multiple levels of assurance for secure interoperability within the DoD and with the Department's federal, allied, and commercial partners. The PKI refers to a means by which users can, with confidence, securely and privately exchange data and conduct other network transactions. This is done using a pair of electronic, encrypted keys (one public and one private) that are obtained and shared through a trusted authority. The public key is the foundation for establishing digital trust across the network (TIMPO, 1999).

Costs versus Benefits. One of the main focuses of business as it engages in economic activity is the concept of return on investment; and this return can be based on

both tangible benefits, such as income, and on intangibles, such as name recognition (Gwartney and Stroup, 1997). This determination is based on some form of assessment. With respect to this research, the assessment deals with weighing the benefits of computer/network security against the expense of the security and the potential loss (or risk) with respect to the system and the networked data. Organizations will make choices for how they will manage and mitigate the risk. Given the nature of for-profit organizations, these decisions need to be justifiable based on economic rationale. Organizations make business decisions not only on how to mitigate the risk of attack but also on economic impact of reporting or disclosing that attack and the loss incurred (Adams, 1998).

Additionally, there are valid concerns with respect to liability, or collateral losses, that are often associated with denial of service and data loss/theft costs. These liabilities may include fines for violating regulatory directives or civil penalties for failing to exercise due care. Some companies may be more concerned by the loss of customer confidence and the corresponding impact on future business than on the actual delays and other costs resulting from the attack (Stackpole, 1998).

Electronic Data Interchange (EDI) is a basis for electronic partnerships. A common method for supporting the interchange between organizations is Electronic Data Interchange (EDI). It is the application of computer technology designed to enhance productivity by migrating private and public sector businesses to a domain based solely on electronic transactions (Cohen, 1989). Electronic Data Interchange is the electronic exchange of formatted business transactions between one organization's computer system and another's computer system. These transactions are structured in such a way that the

computers recognize and process the transactions without the need for human intervention (Payne, 1991).

Another way to define EDI is by making a distinction between it and electronic commerce. Electronic data interchange is the inter-process (computer application to computer application) communication of business information in a standardized electronic form. Electronic Commerce includes EDI, but recognizes the need for inter-personal (human to human) and human to computer communications, the transfer of moneys, and the sharing of common databases as additional activities that aid in the efficient conduct of business. By incorporating a wide range of technologies, EC is much broader than EDI. (Houser, 1996)

The use of EDI in the private sector has developed more rapidly than that in the public sector including the Department of Defense. Its use in the government began in the transportation industry during the 1960's (Payne, 1991). However, the Department of Defense is now working with the concept of EDI. This follows a Deputy Secretary of Defense directive that EDI was to become the standard for conducting business with the Department of Defense. As a result, the Department of Defense formed an Electronic Data Interchange Standards Management Committee to conduct major research initiatives and to investigate how and where to best integrate EDI into Department of Defense activities and what benefits would be anticipated (EDISMC, 1999).

The Goal of Electronic Data Interchange. The Department of Defense goal for EDI is to provide a common method of interchangeability of EDI transactions with its suppliers (EDISMC, 1999). This requires the use of common data formats for EDI information, the definition of the network architecture to be used to provide two-way

access between the DoD its EDI partners. It also demands the assurance that the expected volume of traffic is supportable given existing and planned network capacities (Payne, 1991). One trend in the HMS world is to establish EDI relationships with commercial vendors wherever it is suitable (TIMPO, 1999). Services for medical supplies, pharmaceuticals, and even nutritional medicine are areas where the Air Force medical community already has EDI relationships (Johnson, 1999),

One of the key findings about the Department of Defense's implementation of Electronic Data Interchange is that using a standardized EDI format facilitates inter-operability of DoD systems. By minimizing, or in some cases eliminating the need for translation between Department of Defense data formats and those of its private sector partners, the speed and reliability of the data exchange significantly increase (Payne, 1991). Research identifies electronic mail as the preferable mode for handling EDI transaction (Payne, 1991). An exception to using electronic mail for EDI is for high volume, longstanding transactional relationships between a Department of Defense agency and the supplier or contractor, or for specific security reasons (Payne, 1991). This has specific implications for the Air Force medical community as it continues with its EDI relationships. In order to achieve the benefits of this automated process, the Air Force medical community must manage and protect this system.

Inter-organizational Trust. The cooperative relationship between these governmental agencies and private sector businesses continues to grow as the partners become more interdependent. The government has many providers with whom it can maintain an arms-length relationship; but more and more, it is becoming tightly coupled

with key business partners. As this happens a relationship based on inter-organizational trust emerges.

> "Security is fundamentally about people--those who develop, operate and use your systems. And there are only two types of people—those who have earned your trust and those you haven't caught yet." (Walsh, 1998)

The concept of trust is critical when assessing risk in that the existence of trust enables people to take risks (Jarvenpaa, 1998). From an information perspective, the Department of Defense continues to restrict access based on trust and the concept of "need to know."

Trust can also be explained as perceived (1) ability, (2) benevolence, and (3) integrity. Here, ability refers to the skills that enable the trusted person to be perceived competent within some context. Benevolence is the extent to which a trusted person is believed to be caring and concerned, and to be willing to do good to the trustor. Integrity is adherence to a set of principles thought to make the trusted person dependable and reliable, from the trustor's point of view (Jarvenpaa, 1998). Webster's Dictionary defines trust in the following manner:

> Trust: To place confidence in; to rely on, to confide in, or repose faith in.
> To risk; to venture confidently.
> (1998 Webster's Revised Unabridged Dictionary)

However, the idea of inter-organizational trust opens up another issue of risk. Some risk can be better managed when it is restricted to within the organization. Internal issues such as who is hired, who holds certain positions, and who has access to information, networks, etc., allow the organization to use its own policies and business rules to mitigate risk. In a relationship between organizations, some of this control is lost. The idea of inter-organizational trust, becomes a way for organizations to deal with this risk.

Research indicates that the closeness or dependence of the two parties has an effect on the development of trust (Grundy, 1998). The richness of the media in which the relationship develops is also of importance. Studies have demonstrated that video-teleconferencing, for example, significantly benefits the development of trust (Heberlie and Tolbert, 1999), even to the point of negatively affecting actions and decision making (Grundy, 1998).

The decisions involved in granting trust to individuals are driven by the business rules of the organization (Grundy, 1998). The decision to trust may be to turn a blind eye and hope that one's trust is not misplaced. It may also be built upon careful examination of to whom trust is granted and under what circumstances. Additionally, trust can be seen as situation dependent (Holland, 1998). For example, if you allow a person into your home and you do not lock your door, you have granted some measure of trust to that person. If, however, you lock the door to your home to protect its contents, then for the person you allow inside, you would seem to grant some greater measure of trust. That is, the trust requirement to allow someone behind a protective barrier may be higher. Another example is how the Department of Defense restricts access to certain information to persons demonstrating proper clearance and a "need to know."

The closing off or securing of Air Force networks has been mandated to help protect what has become recognized as a mission critical resource, even as a weapon system (AFCIC, 1999). In order to effectively protect its information and information systems, the Air Force is restricting access to its networks to what are commonly called trusted agents. For the Air Force, this means restricting access to military and civilian members of the armed forces, members of other U.S. government agencies, and certain

contractors and trading partners/affiliates that operate within authorized network domains. At issue then is how an Air Force major medical center and its contract agents and trading partners fits into this overall picture.

The granting of trust is a serious measure of risk management. In granting trust, there is a risk that the trust will be violated. By trusting personnel behind network protection the Air Force is taking a risk, but that trust is sometimes necessary for cooperative relationships between organizations.

Over the last decade, the increasing prevalence of co-operative behavior of "economic partners" has furthered the importance of trust as an integral part of any business strategy (Holland, 1998). As a result, organizations have developed methods for working with customers, suppliers, competitors, banks and other economic partners that rely much more on the development of trust and long-term business relationships (Naude and Holland, 1996) even to the point of developing strategic alliances. Development of this strategic trust is central to the development of the relationship; however, this is a concept that is difficult to clearly delineate given that each relationship is unique (Hart and Estrin, 1991). These interactions between organizations cannot be completely regulated by contracts that characterize market-style transactions nor by standard rules of ownership (Williamson, 1991).

Partner Access. One critical manifestation of inter-organizational trust comes in the determination of how inter-organizational access is granted in a secure network environment (Blackwell, 1999). Blackwell followed up this statement with a definition of partner access given by Michele Crabb, computer systems analyst for Cisco Systems who discussed partners' access at the Intranet Security Panel at Uniforum '97. There she

defined partner access as any connection that provides access from the corporate Intranet to another location outside the organization. (Blackwell, 1999)

The connection is typically configured based on the unique nature of the relationship and on the network security requirements of the two systems. She also addressed specific security concerns that must be addressed in coping with partner access:

> ° Security depends on the partner company—if not properly controlled on both ends, there could be major vulnerabilities.
> ° Access needs of the partner company may change over time
> ° The personnel at the partner organization are dynamic; reliance must be placed on the partner to grant and maintain access for only current users.
> ° There is never time to do proper analysis and implement controls with integrity; they are always needed immediately.
> ° As the number of partners multiplies, managing all the connections becomes an administrative nightmare.
> (Blackwell, 1999)

These problems can be minimized by knowing the partner organizations well and having well-defined guidelines and expectations. Initial policies and guidelines should be as strict as is reasonable since it is easier to loosen than restrict them later. All partner connections must be documented in detail including the names of the contact persons for each party. Needs should be reviewed on a frequent basis, and future growth taken into consideration. The military has the ability to mandate and enforce these standards through contracts with its commercial and trading partners, as long as the "restrictive provisions or conditions are necessary to satisfy the needs of the military or as authorized by law" (Arnavas and Ruberry, 1994).

People in the Loop. It has never been sufficient to entrust risk control and protection to machines, no matter how advanced. People are critical to the effort and as a

result are a liability. The decisions and actions of people can affect the successful application of information technology security measures. The employment of competent personnel is critical to the success of network security. The employees need to have sufficient knowledge and technical skill to perform their roles reliably, to comply with organizational requirements, and to maintain the proper controls on the network (IISF, 1999). These criteria should be evaluated for all personnel who access, control, and manage the information and information systems.

All of these issues revolve around the need for network security. The ability to interact successfully in a network environment is in some way affected by how protected the data is from theft and corruption. It is also impacted by how protected the systems themselves are to support the operations required of them. The use of these systems has become prevalent in the business world.

Increased Use of Information Systems for Business/Hospital Systems

Information systems are useful in the conduct of many business activities. These systems are used to support just-in-time delivery of products to minimize the business costs of storing finished goods and materials. They offer convenience for handling billing and other office automation functions. Benefits abound in how data warehousing and data mining can provide businesses with critical insight to consumer trends, payment risks, likes and dislikes (McFadden, et al, 1999) . The list of functions is long. One of the uses of business information systems is to learn about consumers and provide them with what they want so as to gain a competitive edge in the marketplace (Gwartney, 1997). Hospitals have also found use for information systems. For the Air Force medical

community, the MHS supports many of the hospital services (TIMPO, 1999). Medical logistics packages track the location and status of a hospital's patients.

The problems of network security and information protection are not restricted to government systems or organizations. The civilian sector has also been subject to attacks. Like the United States government, the civilian sector is also not allowed to take the law into its own hands (e.g. attacking the intruder to their systems). Businesses are left with identifying and reporting attacks and incidences to the proper authorities. As a result, they too must focus on shoring up the defense of their computer/network systems.

Attacks are on the rise. Just as in the public sector, attacks on the private sector are also on the rise (CERT, 1999). The attacks on private-sector systems are not a new problem; however, disclosure of those attacks is new. Companies and businesses of varying size have not seen fit to report attacks on their systems even when those attacks resulted in theft of even millions of dollars, intellectual or patented property. Again fear of a loss of reputation outweighs the loss from the attack. In light of the government's recent network security problems, it has begun to push for increased network security capability for both public and private organizations.

Air Force Hospital Scenario

The Air Force medical community is torn between providing an open trusting relationship with its partners and the need to protect its own systems (Futch, 1999). Many of the 100 plus systems of the MHS work on a significant degree of inter-organizational trust. That is, the interconnectedness of the Air Force medical networks provides partners direct access to more than just the MHS system being shared (Johnson,

1999). This community has also built EDI relationships with commercial contractors. The reordering of medical supplies, pharmaceuticals, and food stuffs for nutritional medicine (for the medical dining facilities) is often handled as EDI transactions (Johnson, 1999).

The Air Force medical community conducts its daily operations in a similar fashion to a civilian health management organization (HMO). That different mission requires a degree of network openness that creates additional risk to the Air Force organizations with which Air Force medical networks interconnect (Johnson, 1999). That is not to say that the medical networks do not need protecting. In fact, Presidential Directive 63 stipulates that medical information and information systems are critical resources that need to be protected apart from other networks (TIMPO, 1999). As a result of this directive, the Tri-Service Infrastructure Management Program Office (TIMPO) was established under the Department of Defense Health Affairs to pursue various initiatives to isolate and protect the medical service networks. TIMPO was created as an outcome of the Health Affairs reorganization of 1996. This reorganization identified TIMPO as the office responsible for the development and implementation of a Tri-Service medical networks infrastructure (Futch, 1999). The challenge to TIMPO is to provide an infrastructure that is robust, secure, standards based, and interoperable with the existing security of the three Services. To do this, TIMPO has been developing a broad systems architecture that is heavily influenced by the Defense Information Infrastructure (DII) (TIMPO, 1999). The Air Force medical community's responsibility in this endeavor is significant. It is primarily involved with the architectural and engineering design, security engineering, WWW management, and the overall

implementation and training support for the entire program (Johnson, 1999). The driving force behind this new direction has been the proliferation of military treatment facility (MTF) networks and the various clinical and office automation systems that ride the infrastructure (SRA Vol 1, 1998).

Other Impacts. The process of increasing the protection of Air Force networks has had repercussions throughout the Air Force medical community. When the Air Force designated its networks as a weapon system, the Air Force medical and legal communities identified a significant the Law of Armed Conflict (LOAC) concern. The potential problem with this designation lays in the fact that medical personnel and facilities are protected from attack in their roles as non-combatants (LOAC, 1999). The LOAC states that a non-combatant can be treated as a combatant if that person used a weapon (LOAC, 1999). If the Air Force networks are identified as weapons, what are the repercussions to the Air Force medical community? This issue is still under review.

Air Force Network Security Efforts

The Department of Defense has focused its efforts toward defending its networks systems from attack. The Air Force has measures in place to protect not only classified systems, but also its unclassified computer/information systems. In 1995, the Air Force allocated more than $80 million toward defensive network security measures. These funds were used to establish a base network control center at each Air Force installation to protect access to computers and communications and to monitor network activity with the intent of identifying and tracking system intruders (Fogleman, 1995). In 1998, the highest ranking communications officer in the Air Force, Lieutenant General William J.

Donahue, proclaimed that all Air Force information systems should be designated as mission critical systems, and as such, should be protected with the same diligence as other Air Force weapon systems (AFCIC, 1999).

The goal of this network security is to maintain operability as well as provide for overall network security. According to Anita Jones, Director of Defense Research and Engineering for the Department of Defense Science and Technology Program, Defensive Information Warfare (IWD) is a high priority. She acknowledged that the Department of Defense now has broader focused systems that will survive under unfriendly behavior" (Adams, 1997). An extreme and expensive consideration would be to have the Department of Defense protect the publicly switched networks. The rationale for this goes back to the fact that approximately 95 percent of all DoD connections ride the publicly switched networks (Denning, 1999). The likelihood of that approach is minimal given current national policy (Adams, 1997).

Barrier Reef. As a result of this shift in policy, the Air Force Communications Agency (AFCA) at Scott Air Force Base IL, was directed to develop plans and procedures for protecting the Air Force information systems. AFCA developed a 12-step process to establish effective network security at all Air Force installations. As stated earlier, this protection is called Barrier Reef. It centers around the idea that effective network security is not developed piecemeal, but rather as the concerted effect of policies, procedures, and technical solutions (Segev, 1998). According to the Information Technologies branch at Headquarters Air Force Communications Agency,

> "Barrier Reef is the electronic equivalent of the *physical* perimeter defense provided on our Air Force bases by our security forces. Proxies and firewalls will act as electronic *gate guards* inspecting traffic and allowing

only the traffic that is authorized. Host-based security for base customers within the base perimeter will continue to be the responsibility of the functional community, but portions of the Air Force Base Information Protection effort will assist in providing additional host security. Functional communities with a security policy requirement more stringent than the agreed base policy can augment Barrier Reef security with additional network protection. Functional communities that are unwilling or unable to comply with the stated network security policy will be re-homed outside the Barrier Reef perimeter." (AFCA/GCIT, 1997)

This 12-step process is broken down as follows:

1. "Know thyself."
   A. Identify and reduce exterior network access points to a manageable number
   B. Conduct traffic analysis to determine protocols and data rates currently supported
   C. Map your network topology (physical and logical)
   D. Create a list of base customers including network administration points of contact and network information

2. Requirements determination
   A. Determine what traffic types and what access points are required to network
   B. Understand the uniqueness of each installation/base

3. Policy formation
   A. Create a base level network security policy, involving all tenants in functional areas
   B. Enumerate all allowable services; deny all others
   C. Review AFSSI 5024 for guidance on writing security policy

4. Packet filtering
   A. Take advantage of existing router access control list capabilities
   B. Block as many unsafe services as possible based on TCP/IP headers
   C. View a graphical representation

5. Network monitoring
   A. Integrate network monitoring device(s) such as the Automated Security Incident Monitor (ASIM) developed by the Air Force Information Warfare Center (AFIWC)
   B. Place the monitoring device outside of the boundary protection to monitor all attempted attacks

6. Network time sourcing
   A. protect base from the injection of false time (as from spoofing of Network Time Protocol)
   B. Integrate GPS receivers to provide a reliable, accurate time source for base systems

7. Consolidating dial-in communications
   A. Aggregate multiple functional dial-in solutions into one centralized service
   B. Protect access to the service via strong authentication of users
8. Worldwide Web proxying
   A. Direct all outgoing worldwide Web requests through a worldwide Web proxy device for the purpose of
      i. Hiding users' identities from Internet eavesdroppers
      ii. Reducing wide area network utilization and improving user response time
      iii. Providing positive control over Web access to unauthorized sites

9. Inter/intra services
   A. Provide a public "lobby" for e-mail entry and access to data for wide distribution
   B. Place in the protected boundary protection zone to reduce internal network access
   C. Provide a mechanism to keep public data updated from internal web servers

10. Proxies of common and special services
    A. Authenticate outsiders before granting access for dangerous services (Telnet, FTP)
    B. Implement controlled access for specialized Air Force services (e.g. Info Connect, CHCS)

11. Network concealment and security
    A. With all network traffic, use proxies to interact with systems outside the network, hides internal IP addresses
    B. Consider migration of IP version 6 or a 10.0.0.0 class A private network to seal "backdoor" leaks

12. Training, maintaining, and certifying
    A. Use logs, monitoring tools, and CERT advisories to identify new vulnerabilities
    B. Update access control lists, proxies, and authentication measures to oppose the threats
    C. Perform system certification to ensure proper accreditation

D. Keep system administrators trained

Effective network security is a combination of policies, procedures and technical solutions (Segev, 1998) and Barrier Reef provides these.

Detecting, reporting, and responding to attacks. The protective barriers are an essential part of network security; however, there is more required to adequately protect Air Force networks. The Air Force Information Warfare Center developed the means to track computer systems that enter an Air Force network's cyberspace (Cloutier, 1996). This tool, the Automated Security Incident Measurement (ASIM), is able to track and report intrusion attempts and possible internal abuses. It resides outside a base's virtual front door—the entry point for all traffic onto the base network. Recent upgrades to the ASIM monitoring system immediately alert network administrators to unauthorized or suspicious activity. Previous editions of the software only compiled reports every 12 hours delaying the effective response to what might be a network attack. With ASIM monitoring, network administrators can identify network addresses that the unauthorized person uses to access into the Air Force network. They can then act to deny access from these addresses. Essentially, tools such as ASIM help Air Force network administrators achieve the goal of blocking access to networks from unauthorized addresses even as someone from that point attempts to gain access to its network (AFI 33-115, 1997).

Governmental Response Teams. In addition to local monitoring and responding mechanisms, the Air Force has developed a centralized team to disseminate time critical information to all of its installations. This team is called the Air Force Computer Emergency Response Team, or AFCERT. The AFCERT has direct links to its United States government counterpart, the national CERT. Together with other representatives

of 30 international teams, comprise the Forum of Incident Response and Security Teams (FIRST). These teams are responsible for collecting information on existing threats and vulnerabilities and for determining courses of action for the protection of all government computer/networked systems within their purview (Mesevich, 1996). The Defense Information Systems Agency has also formed a special Information Security (INFOSEC) team to oversee the procurement of necessary protective technologies (Military Newswire Service, 1996).

The Dilemma

The Air Force has instituted Barrier Reef as the series of security measures to protect its networks. The Air Force medical community operates mandated network connectivity that is not compatible with Barrier Reef. To overcome this problem, the OASD(HA) directed TIMPO to develop an architecture that would protect all military medical systems and allow the systems to continue with existing connectivity requirements. More effort is needed to understand the issues involved with this dilemma. This research will establish a framework of significant issues that should be considered by any activity meant to solve the dilemma.

Possible Solutions for the Security-Connectivity Dilemma

In 1998, President Clinton signed Presidential Decision Directive 63, "Critical Infrastructure Protection" identifying OASD(HA) as a Critical Asset Owner in the Defense Information Infrastructure. This direction made the OASD(HA) solely responsibility for medical information assurance. Additionally, it expressly relieved the

operational military from responsibility and accountability for protecting medical computer applications or the medical network infrastructure (TIMPO, 1999). One interesting effect of this directive is that the Air Force community and its leadership can choose to cut their network ties to the medical systems. As noted earlier, medical information systems rely on their host bases for communications and computer support.

In response to the new authority, the OASD(HA) directed the Tri-Service Management Program Office to establish corrective action (TIMPO, 1999). The TIMPO charter was to establish a robust, secure, standards based architecture that was interoperable and consistent with the security measures of each service (Futch, 1999). The focus of the design has been on the use of encryption, and state-of-the-art protocols and hardware tools. Table 2 identifies various issues the plan addresses.

Table 2. Issues covered by TIMPO

Major Issues	Sub-Issues
Infrastructure	Connectivity Equipment Throughput Configuration Mgmt
Information System Policy and Management	Limited (MHS only) Centralized Management Coordination
Mission Needs	Medical Focus Base Focus
Security Management	Technology Capability Multi-level Security COTS Focus Management Policies Legal focus (Due Diligence)
Personnel Issues	Training (Limited) Manpower

The development of this new architecture involves the Army, Navy, and Air Force. The Air Force is involved in the architecture engineering and design, security engineering, and WWW management. It is also involved in customer support on the network and through Internet access. Lastly, it will be working with TIMPO on implementation and training support. The Army's role includes network management engineering support, network monitoring and performance, hardware maintenance and sparing, and circuit deployment and management. The Navy is involved in capacity planning and overall configuration management.

Summary

Exploitation of network system vulnerabilities has resulted in a change in how the Department of Defense has chosen to defend its networks. The Air Force has implemented a multi-part security plan, Barrier Reef, to provide adequate protection to all of its network assets. The Air Force medical community has numerous network connections that are not easily converted to operate behind the Barrier Reef protection. Many of the systems the Air Force medical community operates are stove-piped, and many others do not have any security features built in. As a result, the TIMPO was directed to develop a secure, robust architecture to allow the MHS to securely interact with the network systems of the Army, Navy, and Air Force. Still, nothing found in the research or in this traditional approach by TIMPO provides a clear understanding of the issues involved in solving the Air Force medical community network problem.

Chapter III will discuss the method used to collect the necessary data to begin the process of establishing a framework of issues that any potential solution to the Air Force

medical community network problem should include. Then in Chapter IV, the collected data will be analyzed and assessed to determine the primary factors that are needed to build that framework. Chapter V will discuss the results and the framework of issues. It will also include limitations of this research and recommendations for future research.

III. Methodology

Introduction

This research collected information to support a framework of issues relevant to resolving the Air Force medical community's problem of maintaining its assorted network connectivity while providing for security of its network. This chapter describes the methodology used to conduct this research and discusses its exploratory nature. Included in this chapter is a description of the population under study and justification for the selection criteria of respondents from whom the data was gathered.

Research Method

The literature review developed a number of related topics of interest to this study. Much has been written on risk assessment and risk mitigation. Beyond the literature on the actions of TIMPO, little research on the Air Force medical community network dilemma was found. For this reason, an exploratory study was conducted to provide a framework of issues that any potential solution to the Air Force medical community network problem should include.

The Air Force's major medical centers were selected as the subjects for qualitative study. Qualitative research on organizations refers to research that involves a small number of organizations whereas quantitative research typically requires a substantially larger n for analysis (Cash, 1989). In a similar study, AFCA successfully used case study methodology to assess the impacts of Barrier Reef at an operational site (AFCA/GCIT, 1997). A case study was identified as a suitable approach for dealing with

the exploratory investigation of management questions (Cooper and Emory, 1995). It is recognized that the amount of published data is seldom more than a small fraction of the existing knowledge in the field (Cooper and Emory, 1995). For that reason, it is productive to seek the input from those experienced in the field of interest (Cooper and Schindler, 1998). This case study used an experience questionnaire to help identify the areas of interest surrounding this Air Force medical community issue. The experience questionnaire is a useful tool for generating new hypotheses, models, or ideas requiring in-depth knowledge in areas lacking quality secondary data (Cooper and Schindler, 1998).

During the literature review no reliable historical data was found relating to the Air Force medical community's current network dilemma. A likely reason for this is that direction for implementing network policy and procedures has been directed by a number of separate organizations: Air Force SC (Communications and Information) and SG (Surgeon General) directorates, Office of the Assistant Secretary of Defense for Health Affairs (OASD(HA)), public law, and so on. These independent directions were provided on a case-by-case basis and typically involved systems that did not interact with each other, so little if any coordination was necessary. However, much information was identified relating to the general issues of network security and business partnering. To collect the necessary information, questionnaire subjects from the population of interest were selected.

The strategy for collecting this data was to pick a sample of the Air Force medical community population that would provide information that represented the considerations and concerns for the whole population. Collecting data from the Air Force's major

medical centers seemed likely to provide the data necessary for this research. That segment of the medical community tended to have a much higher degree of connectivity than did the smaller medical facilities. These centers acted as the information hubs in the medical community's infrastructure and tended to have larger network management functions and a pool of resident expertise.

The idea of choosing the major medical centers was that if the research produced significant findings with this segment of the population, then the research would likely have applicability for rest of the population of interest. This was inferred based on evidence found in research that if hypotheses can be supported using the selection of the strictest case within a population, then the likelihood for applicability to similar or lesser cases is improved (Cash, 1989). With these concepts in mind, this researcher examined a single Air Force major medical center for background, then developed a questionnaire for collecting data from all of the Air Force major medical centers.

Questionnaire Development

The Wright-Patterson Medical Center (WPMC) was used as the initial site for collecting background data. The data collection at this stage consisted of an unstructured questionnaire, documentation review and observation. These methods helped to define and refine the areas of interest for the questionnaire. Wright-Patterson Medical Center was involved in migrating its network systems to a position behind the base's network security (Barrier Reef). Wright-Patterson Medical Center was working diligently to find alternatives to its issue of maintaining connectivity with contracting and trading partners. Much information was collected from WPMC and used in the development of the data

collection instrument discussed shortly. The WPMC representative also confirmed the locations of the Air Force's major medical centers and provided points of contact for each of the facilities. The following complexes are identified as medical centers and are the subjects of this study:

Wright-Patterson Medical Center
Scott Medical Center
Travis Medical Center
Andrews Medical Center
Keesler Medical Center
Wilford Hall Medical Wing
Yokota AB Medical Center

These facilities comprise all of the Air Force's major (regional or higher) medical centers. As such, this study was performed as a census; here, census refers to data collection from all possible instances of major medical centers. In exploratory research, it is more important to pick sources that might provide insight than to look for a general cross-sectional representation (Cooper and Emory, 1995). These major medical centers are a clearly defined subset of the greater medical population. According to Cooper and Emory (1995), discovery is more easily carried out if the researcher can analyze cases that provide special insight. Due to the extensive medical services and much higher volume of personnel, patients, and (importantly) network activity they support, this group is identified as the strictest case of the population. Also the information systems experts are expected to provide the special insight into the issues surrounding the Air Force medical network dilemma.

With the findings from the WPMC background data and the literature review, a questionnaire was built for collecting data on all of the seven major medical centers. A combination of closed and open-ended questions was used for data collection. The

closed questions were used to ensure that all of the respondents were operating from a common understanding of the area of interest and to establish a general framing of the open-ended questions that were to follow. Research indicates that using open-ended questions in experience questionnaires is a good method for collecting data relating to general ideas, "what" questions, and specific experiences (Cooper and Schindler, 1998). For this research, the information surrounding the network security and connectivity issues will be drawn from the open-ended questions.

Validity. This research is intended to apply to the population of Air Force medical facilities. For this research, internal validity by means of content validity was used. Content validity of the measuring instrument is the extent to which it adequately covers the topic under study (Cooper and Emory). An accepted means for establishing validity in exploratory research is judgement and can be determined by experts in the field. (Churchill, 1983). This assessment occurred in the development and revision of the questionnaire as described earlier and in the background investigation and study of the Wright-Patterson Medical Center.

Reliability. Reliability, which addresses whether an instrument produces consistent and stable results, is a necessary contributor to validity. It is not, however, solely sufficient in demonstrating that condition (Cooper and Emory, 1995). In their research textbook, Cooper and Emory use the example of a bathroom scale to draw the distinction:

> If the bathroom scale measures weight correctly, (using concurrent criterion such as a scale known to be accurate), then the scale is both reliable and valid. If it consistently overweighs you by six pounds, then the scale is reliable but not valid. If the scale measures erratically from time to time, then it is not reliable and therefore cannot be valid.

The reliability of this instrument is difficult to establish given the open-ended nature of the questions and the exploratory nature of the research (Cooper and Schindler, 1998). The intent of this research is not to confirm consistency of responses; but rather, it is to gather as much information of relevance to the area of interest. Therefore, there is likely to be significant variance in the responses and explanations by the respondents.

Questionnaire. A researcher-guided questionnaire was used to collect data for this project. The questionnaire was divided into three sections (Demographics, Section A specifically for medical representatives, and Section B specifically for base communications support representatives). The questions in section B mirror those in Section A with one exception. A series of questions surrounding the issue of medical center dependence on outside agencies were asked only of the medical respondents since that group is the only one with that area of expertise. Based on insight gained from related literature and from data collected in the background study phase of this project, the researcher developed the questionnaire listed in Appendix A.

Specific questions were developed to ascertain the underlying issues with respect to cost, benefit, dependence, and risk. These constructs were developed from the literature review in Chapter II. Many references to various aspects of network security were addressed. These included a common theme of risk assessment. According to the literature, network risk assessment involves identifying the information of value, determining the existing vulnerabilities and threats that can take advantage of those vulnerabilities, and assessing what actions can be taken to mitigate the risk. It also included the need to conduct a cost-benefit analysis for the network security. For

example, risk assessment would conclude that it is not rational to spend more money on network security than the value of the asset. At some point the costs outweigh the benefit. Additionally, the issue of dependence moderates the valuation of the networked information/assets. Contracts, public laws, and other directives drive much of the Air Force medical community connectivity. The community is finding itself very dependent on the current connectivity arrangement because of unresolved issues of proprietary information systems that result in a lack of interoperability. The lost flexibility of the medical community to provide these connections through other means has complicated its network security situation. The questionnaire is intended to flesh out the issues that must be addressed for this medical community problem and will focus on the construct areas listed above.

The structure of the questionnaire was developed to promote responsiveness on the part of the representative providing data. Specific demographic questions were used to compare the two respondent groups' experience levels. More important to the development of the desired framework, open-ended questions were used to gather information on various constructs identified in the literature review and in the background research. These questions prompted the respondents for detailed and explanatory answers to the construct areas.

To avoid misunderstanding and ambiguity in the questionnaire and any bias based on a specific base's configuration, definitions for key concepts and issues of interest in the questionnaire were provided immediately prior to the series of questions related to those terms. Additionally, all of the questions were posed in "positive" form; that is, a question about Barrier Reef issues would have been asked, "What issues impact Barrier

Reef?" as opposed to asking "What are the issues that do not impact Barrier Reef." The positive form supported clarity for both the respondents during the interview as well as for the researcher during data analysis. All of the questionnaires were administered by a single researcher to promote consistency in the data collection process. The final questionnaire represented refinement from the culmination of numerous iterations based on input of faculty and local experts in network security.

Pretesting. The draft of the questionnaire was critically reviewed and pretested prior to administration to the respondents. Pretesting was accomplished in two distinct phases. Members of the Air Force Institute of Technology faculty reviewed the questionnaire for completeness and appropriateness. After sufficient revision and follow-up review, the questionnaire was deemed to sufficiently address the research and investigative questions. As a final step in the pretesting cycle, feedback was solicited from two colleagues. Both have extensive background in networks and network management. These two reviewers recommended minor word changes and more specific definitions to lessen the ambiguity of the questions in the instrument. Final modification reflected these recommendations, and then the updated instrument was put forth for final approval. The approval was granted and the scheduling of times to administer the questionnaire began.

Subjects

This researcher chose to conduct telephone interviews with specific points of contact representing each regional medical center's and each support base's network/computer organization. Obtaining information from both the major medical

centers and their support base organizations helped to ensure that no topic of interest was overlooked. To minimize the variability between respondents, criteria were established for whom was allowed to represent an organization in this research effort. To promote information gathering from the most knowledgeable of sources at each location, contact was made with the person in charge of each organization's networked information resources. This person tended to hold the position of branch chief, flight commander, or chief information officer for the organization.

Each manager was informed of the nature of the research and asked to provide the name and phone number of the most qualified person in their organization to answers questions within the defined area of interest. To ensure a representative had sufficient experience in networks as well as the represented organization, each was required to have at least one year of direct experience in management of network systems and personnel. Additionally, each needed to be currently in that type of position and to have held it for at least six months. This current familiarity with the represented organization's system configuration and management issues was considered essential. All of the information managers readily consented to participate and identified qualified respondents to participate in the data collection effort.

For this research, an $n = 7$ was used for the medical respondent group, one representative from all seven major medical center locations. For the support base respondents, an $n = 6$ was used. This reduction of one data point accounts for the autonomy of Wilford Hall Medical Center. Wilford Hall Medical Center operates and maintains its own networks due to its size and dislocation from its support base, Lackland Air Force Base.

The questionnaire respondents had a common frame of reference of network security. Each had direct experience dealing with the day-to-day management and operation of networked systems. The minimum criteria defined for the respondents was selected to ensure each had this experience and therefore the ability to discern specific issues relevant to the medical community's dilemma for maintaining network connectivity while meeting its network security requirements. The questioning of both the base support and medical network experts provided the opportunity to develop a thorough framework of the dilemma's issues.

Approach

During the evolution of the questionnaire, the researcher began contacting the seven locations hosting major Air Force medical centers to identify appropriate personnel to participate in the data collection effort. The merits of each participant were based on strict selection criteria. Each representative had to be in a position directly responsible for the operation, maintenance, and/or management of that installation's networks (medical or support base). The representative had to be recommended by the person in charge of that organization's network or information management to ensure a general level of experience and sufficient familiarity with network issues. Each representative was required to have at least 12 months of networking experience with at least 6 months at the location being represented.

The rationale for collecting data using a telephone questionnaire was to obtain the highest response rate possible in support of a census and to promote a more thorough response. Any level of non-response in this situation given the small sample size could

have had significant effect. Additionally, by personally conducting each questionnaire, the researcher was able to elicit a more detailed response to the questions. Without this added detail, the significance of this research effort would be considerably lessened. The estimated time required to administer each questionnaire was 45 minutes. The actual range was approximately 30 - 65 minutes and depended primarily on the time the respondents spent providing details. To assess the effectiveness of the series of questions, the questionnaire was pretested before administration to the representatives of the Air Force major medical centers and their support bases.

A total of 13 representatives were questioned in the data collection process, thereby obtaining the desired census. Each of the intended representatives was contacted by phone to discuss the research focus of this thesis and to schedule a convenient time to administer the questionnaire. Research indicated that it was important to disclose to each intended respondent the motivation for the data collection and specifically why each respondent was selected (Cooper and Emory, 1995). At the initial contact, commitment was obtained from 10 representatives; two representatives were not available for contact and the last refused to participate in the data collection effort. Later, this researcher discovered that the refusal of the last representative was based on recent attacks and infiltration of that organization's networks. The representative thought that the timing of the request for information was more than circumstantial. In the end, the respondent agreed to participate after receiving clarification from his information manager.

In conducting the telephone questionnaire, special attention was paid to inform the respondents of their rights during the questioning. They were informed that they had the option to answer all, any, or none of the question posed to them. They were also told

that they reserved the right to terminate the session at their discretion. They were also informed that the responses provided during the session would not be attributed to them or to their organizations. The demographics data collected and the specific questionnaire responses would only be used as pooled data for general analysis. With this understanding, all of the respondents were willing to proceed with the questions.

Summary

A census was conducted of the medical and support base organizations of the Air Force major medical centers. Experts from each organization were selected to answer a questionnaire to help build a framework of issues for dealing with a medical community problem. Again, the Air Force medical community's dilemma is trying to maintain network connectivity to all of its government and commercial partners while providing mandated protection of its network systems. The major medical centers were selected as the source for the experience data given the higher complexity of their network connectivity. Specific respondents were selected based on recommendations from the organizations' chief information manager (or equivalent) based on criteria to ensure sufficient expertise. An open-ended questionnaire was developed to promote respondent elaboration to the various questioned posed to respondent.

Chapter IV discusses the completed model and how the primary factors were derived. Chapter V will then provide a discussion of the results of this research and identify areas for future research.

IV. Analysis of Questionnaire Responses

Overview

The data collected from the base network personnel supporting these major medical centers is displayed in this chapter in the form of an issue framework. In addition to reviewing the demographic information for appropriateness of the responding groups, this chapter discusses the processes used to determine the issues that make up the framework from which to better address the medical community's network problem, and then explains the relevance of each developed issue.

Demographics

The demographic data were reviewed for two purposes. First, the data was reviewed to ensure that the respondents all met the minimum criteria established at the onset of data collection. The criteria were set to provide a measure of assurance that each of the respondents had sufficient familiarity with networks in general and their current organization's networks in specific. Each of the respondents met all of the initial criteria. Significant differences were noted between the two groups with respect to the average time each respondent has been in the current networks position as well as to how many other organizations the respondent has worked with. These differences have relevance with the continuity issue brought up by respondents and will be discussed in the following section. The second reason for examining the demographics was to determine if the respondents were the proper group to provide the information desired to support this research endeavor. Based on the scope and consistency of the responses, the

researcher was confident that the respondents were indeed the proper response group for this exploration.

Collection of Responses

Method of Analysis. All of the responses gathered from the telephone interview were transcribed into a spreadsheet (Appendix A). The transcription was done in note form and was not produced as a full reproduction of the respondents' comments. If a question was not asked of a particular respondent (i.e. medical specific questions were not posed to support base respondents), the block was marked N/A. There were times where the respondent did not provide a salient response to a question. The person conducting the interview determined that all comments related to this research were important. If in the course of asking a question, the respondent had touched on an area of his/her interest, the interviewer waited for a moment to redirect the respondent. This was done to allow the respondent freedom to convey issues and still control the direction of the conversation. In some cases, respondents wished to elaborate in some areas and not in others. The blocks with no response given are blank.

The findings were evaluated to determine trends between the medical and base respondents. The only area of note involved the question on the recommended choice of network security for the medical networks. The majority of support base respondents felt that Barrier Reef was adequate for the task. One respondent commented, "Barrier Reef should be able to work. It'll cost to work out all of the configuration issues, but we can do it." The typical response from the medical respondent stressed that Barrier Reef is not working. "Isolating the medical networks enables them to conduct business at the level

to provide needed service to physicians etc." (e.g. Physicians would have the ability to have full network access from home). Also healthcare is a regional activity, not base specific." Overall, respondents agreed that this isolation approach would be much more costly; but for the medical respondents, it is a necessary cost.

Unexpected Results. The major finding outside the expected response areas was the overwhelming opinion that many of the problems the medical community is facing occurred because there is no one organization with sole authority to implement network changes. Based on the time most of the respondents spent on this one area, this appears to be one of the critical areas that is lacking. Some of the comments follow. "The biggest problem is that the systems aren't deployed by the Air Force. Most are directed from beyond the Air Force's control and have different requirements. HA and SG are not working with SC." Also, "We really need a unified IT Plan. There is a big disconnect between the SG [Hospital] and SC [Base Computer and Communication] communities."

General Factors. In all, seven general factors were identified from the comments of the questionnaire respondents. The comments of the respondents were grouped based on subject area of the response. As an example of respondent comments, one expert specifically advocated the isolation of Air Force medical networks saying, "Isolation of the nets provides closer control and allows for configuration for a smaller number of users. This allows for better tailoring to mission needs." The subjects vary widely and address issues from the obvious architecture and equipment needs to the less often addressed issues of Social Engineering and Dependence. Here, Social Engineering refers to the manipulation of people to fraudulently obtain access to information that those people would not otherwise provide (Denning, 1999). Dependence refers not only to the

Air Force medical community's dependence on the their network connectivity but also to the organizations that it is partnered with. The following list identifies the issues that developed from the respondents' answers to the questionnaire:

Infrastructure
Information System Policy and Management *
Mission Needs
Security Management
Social Engineering
Personnel Issues
Dependence

* Denotes a post-hoc finding

Developed Issues for the Framework

The relevant issues for the medical community's network problem were identified using an experience questionnaire. Questions focusing on the constructs of risk, cost/benefit analysis, and dependence were used to promote the solicitation of ideas and issues from the respondents. The answers provided by each respondent were evaluated and then consolidated into various response groupings. These groupings were established based on how well the data seemed to describe or otherwise relate to the same issue. These groupings were examined for overlap and groups were redefined to clearly distinguish between issues. After further assessment, the final groupings were identified as individual issues for consideration.

Infrastructure. All 13 respondents discussed some issue with infrastructure costs. Within this issue are several related topics. Long-haul connectivity costs were identified as an area of significant area of impact given the numerous connections operated by the medical community. The costs will vary according to the final solution. Respondents

stated that isolating the medical networks will allow the medical community to bundle some of its network connections but will result in significant recurring costs for dedicated and general leased lines. The support bases currently pay for much of this cost. The Barrier Reef solution requires the medical connections to run through the base lines. The rehoming of all these medical connections is not only time consuming and manpower intensive, it may require increasing of the size of each base's pipe. The added traffic through the Barrier Reef entry point is analogous to adding traffic on a highway. The road may have to widen to alleviate congestion. Another area of interest dealt with the equipment required. While the effect of rehoming the services in Barrier Reef is not believed to require significant equipment costs, establishing an isolated network for the medical community requires a substantial equipment investment. The respondents all reported that the medical community would be required to duplicate all of the network architecture elements (routers, servers, etc.) in addition to the network security equipment necessary for it to continue network operations and services.

Information System Policy and Management. One of the most interesting outcomes of the questionnaire involved the issue of information policy and management. Without any questions directing attention to the subject, 8 of the 13 respondents identified the discontinuity of policy and lack of a central management for networked activities as an important issue to consider. Even support base respondents were consistent in identifying this as a problem. The Air Force and the Office of the Assistant Secretary of Defense for Health Affaire (OASD(HA)) have been at odds in developing and mandating network architectures. Unfortunately, these mandates are often worked within the policy directorate of the owning community with no outside coordination.

Respondents report that it is not unusual to have a system installation team show up at the base with no forewarning. The base and the medical facility are put in a position to work out arrangements on the spot and then worry over who will manage, operate, and maintain the system. On rare occasions, the installation team has been directed to stay on for some period to train system administrators on how to operate this new system.

Until recently, as described in Chapter II, the OASD(HA) had the authority to direct connections and network structure for the medical group with little say from the Air Force communications and information community which was tasked to support it. Recent directives have changed this way of doing business, but the two communities are still working out how to implement their designs for security and connectivity. The concern is still the lack of balance in the relationship between the medical community and the support base activities. The respondents feel that either some single authority should be in charge of all DoD networks or that clear lines of responsibility and authority be in place, possibly contractually, to support the relationship between the SG and SC communities. At the time of this research, TIMPO is in meetings with the Air Force Communications Agency (AFCA) to work on these arrangements.

Mission Needs. Along with the issue of information policy and management, a related issue developed. The respondents all commented (13 of 13) on the fact that the business of the medical community was somehow different from the support base community. First, the medical community networks are intended to support the provision of medical care to not only the active duty members in wartime but also to the member, member's dependents, and retirees in peacetime. The focus for the Air Force networks at large is to support the warfighter and leadership in peace and in war. In its peacetime

operations, the medical community is more similar to a civilian HMO than it is to the other support services of the military. There is an impression from the respondents that security is more of a concern for the medical community than it has been in the past. However, differences still exist; the support bases are more concerned about security while the medical community is more concerned about generally supporting medical services. One medical respondent commented, "[We] have multiple access points. [Our] focus is on the day-to-day medical needs and not on security." A similar response from a support base respondent was "... their focus is customer service and access to information for many groups; they have a decreased focus in security." When asked about the usefulness of Barrier Reef in protecting the support base networks, almost all of the respondents in both groups stated that Barrier Reef was sufficient for the bases' needs. When the same question was asked about Barrier Reef protecting the medical community networks, less than half of all respondents stated that Barrier Reef could provide the needed security. Respondents clearly felt that Barrier Reef will not provide the Air Force medical community the same protection that it does to the operational Air Force. The Tri-service Infrastructure Management Program Office (TIMPO) has been tasked with addressing difference in mission needs for all of the DoD services and has recognized that the security measures of each service cannot support the medical networks current connectivity.

Security Management. This refers to the various activities involved in minimizing the vulnerabilities of networked systems and information. A natural outcome of these actions is the overall reduction of risk. All of the respondents felt that the state-of-the-art in network security (encryption, advanced routing and filtering equipment,

system monitoring techniques and tools, etc.) has the potential to sufficiently secure all of the Air Force medical networks. Similarly, they all agree that the policy and political situation will prevent that from happening. A typical response was "The technology is there and it will work if politics and people use it to it's potential."

Social Engineering. A few (4 of 13) of the respondents identified people as the weak link in network security. One example of social engineering found in research is where an adversary tries to gain access to a network system by lying about his or her identity in an attempt to either gain direct access or to get information that will allow access (Caldwell, 1990). Despite the low number identifying this issue, it still may be significant when developing potential solutions. This issue is not addressed in the Air Force's Barrier Reef concept nor is it currently addressed by TIMPO. For example, Barrier Reef uses active controls to limit the use of weak passwords, but it does not deal with social engineering. The only actions the respondents see in use to minimize the impact of social engineering is through the posting of policy letters and that is not sufficient action. One respondent commented that "the technological capability to secure the networks is there. However, there is minimal attention paid to addressing human factors and social engineering." As Air Force network systems are made more impenetrable to unauthorized users, it is likely that an adversary will turn to other weak points. Research indicates that one of these areas is social engineering (Denning, 1999).

Personnel Issues. All 13 of the respondents identified concerns with manpower and the training of manpower. When measured against all of the other issues, 11 of 13 respondents stated that training and training related issues were the most important long-term concern. Nearly all stated that they would be hard pressed to support the increase in

training because of severely limited budgets. The medical community has a related problem in that it has no military-run schoolhouse to educate its members. The only exception came from one respondent who stated, "We are unique. Fortunately we have access to the enlisted communications technical training school since it's located here." To compensate, the Air Force medical community has taken to hiring the necessary expertise via contractors and federal civil service employees (Young, 1999).

Coupled with the training concern was another about overall continuity. This concern is particularly significant for military organizations. Historically, the military member tends to be reassigned more often than contractors and civil service employees. The support base respondents in this study were all active duty, and the medical respondents in this data collection were a mix of contractors, federal civil service, and active duty members. Not surprisingly then, the military members have been in their current positions less time and have worked more networking jobs per unit time than their medical respondent counterparts. Worthy of note is the fact that training was considered the highest long-term concern for both groups. In their words, "Training is biggest; no short cuts available in the Air Force; we train them and they leave for commercial sector." Another comment was, "Basically, we don't see more people coming down the pipe. More people and more training are required." Hiring expertise by medical respondents and providing schoolhouse training by support base respondents were not seen as sufficient answers to this problem.

Dependence. Because of outsourcing, networks are becoming more and more dependent on outside management. Respondents noted that "For Tri-care to work, it must have full access to provider information" and that "Overall the dependence on them

is increasing." When activities are outsourced, the manpower billets based on that activity go away (Young, 1999). For the medical community, the trend is for downward-directed programs to be funded at the top level and contracted out; the medical facilities just receive the contracted system (Young, 1999). Respondents additionally commented that "Existing systems are proprietary." This leaves the medical centers with fairly long-term (five-year) contracts and limited capability to easily change systems. One respondent commented that "the Air Force medical community is being taken advantage of. These long-term contracts limit its ability to pursue the benefits of free enterprise and non-proprietary systems." If the decision is made to bring these functions in-house, most agree that "it would take years and a lot of money to recreate what's out there right now." Without the ability to easily standardize systems and eliminate stove-pipe configurations, perhaps the next best option is to not attempt to use the TIMPO proposal and leave the current systems as is and take action to secure the infrastructure (TIMPO, 1999).

Proposed Framework of Issues

Table 3 depicts the framework of issues that respondents identified as having relevance to the current Air Force medical network problem. The mission needs issue appears to be a critical issue as it defines the comparison between the line and medical communities. Table 4 represents the developed issues in a side-by side comparison with the current TIMPO direction to provide a robust and secure medical network architecture. The TIMPO arrangement is directly in line with the Generally Accepted System Security Principles and has more of an architectural focus. This is appropriate since identification of a new architecture was TIMPO's stated focus.

Table 3. Respondent Issues

Major Issues	Sub-Issues
Infrastructure	Connectivity Equipment Throughput
Information System Policy and Management	Centralized Management Coordination
Mission Needs	Medical Focus Base Focus
Security Management	Technology Capability Political Limitations
Social Engineering	People as the Weak Link
Personnel Issues	Continuity of Personnel Training Manpower
Dependence	Service/Vendor Dependence Impact of Contracts

Table 4. Comparison of Respondent Issues to TIMPO Issues

Respondent Issues		TIMPO Issues	
Major Issues	**Sub-Issues**	**Major Issues**	**Sub-Issues**
Infrastructure	Connectivity Equipment Throughput Configuration Mgmt	**Infrastructure**	Connectivity Equipment Throughput Configuration Mgmt
Information System Policy and Management	Centralized Management Coordination	**Information System Policy and Management**	Limited (MHS only) Centralized Management Coordination
Mission Needs	Medical Focus Base Focus	**Mission Needs**	Medical Focus Base Focus
Security Management	Technology Capability Political/Management Decisions	**Security Management**	Technology Capability Multi-level Security COTS Focus Management Policies Legal focus (Due Diligence)
Social Engineering	People as Weak Link		
Personnel Issues	Continuity Training Manpower	**Personnel Issues**	 Training (Limited) Manpower
Dependence	Ability to do without Impact of Contracts		

Summary

The Air Force medical network issues framework identifies seven major areas that are important to address in the consideration of solutions to the Air Force medical community's dilemma in providing mandated network connectivity while protecting its networks. In addition, the demographic information supported the appropriateness of the responding groups for developing the issues framework. They all met the criteria indicating sufficient familiarity with general network issues and specific understanding of the issues in dealing with the Air Force major medical centers. The reason this group was specifically selected was addressed in Chapter III. This chapter discussed the process by which related areas of interest were put together into larger issues. These issues were explained to support their importance in solving the Air Force medical community's on-going network problem. Chapter V will discuss the implications of these findings and will provide recommendation based on the developed network issues framework.

V. Findings, Recommendations, and Conclusion

Review of the Dilemma

The Air Force has instituted Barrier Reef as the series of security measures to protect its networks. The Air Force medical community operates mandated network connectivity that is not compatible with Barrier Reef. This incompatibility results from various network protocols and configurations used in the more than 100 military health system (MHS) automated information systems (AISs). To overcome this problem, the Office of the Assistant Secretary of Defense for Health Affairs (OASD(HA)) directed the Tri-Service Management Program Office (TIMPO) to develop a robust, secure, standards based architecture that would protect all military medical systems and allow the systems to continue with existing connectivity. The plan proposed by TIMPO is based on issues developed in the generally accepted system security principles (GASSP) and on current network security technology. The plan is based on a current understanding of the networking issues and no background investigation into the completeness of those issues was conducted.

The Purpose of the Research

Without investigating the completeness of the issues surrounding the Air Force medical network dilemma, there is a potential for oversight of one or more important factors. The purpose of the research was to identify issues that should be considered in any potential solution to the Air Force's medical network dilemma. The nature of the research effort was exploratory. Following established research guidelines for an

exploratory study, an open-ended experience questionnaire was used to gather data from network experts representing each of the Air Force major medical centers and each corresponding support base. The findings from the exploratory study were grouped by subject area and compared to the issues covered by the TIMPO plan. These issues were then combined into a framework that is discussed below.

Overview of the Framework

The framework was developed to provide a more complete identification of the issues that require consideration as the Air Force medical community attempts to solve how it will protect its networked systems and still maintain its required connectivity. It is not enough to solve a problem based on the architectural needs of the system. Security issues should also be addressed along with a concerted forethought on how the actions will affect all of the users of the affected network. The developed framework points out some of the areas that may get overlooked. By paying attention to the less obvious issues from the start, they will be less likely to turn into obvious problems in the end. When combined, the issues identified by the respondent network field experts and TIMPO encapsulate the issues of interest. Table 5 provides a view of this consolidated framework of issues. Items not addressed in the TIMPO plan are underlined.

Table 5. Proposed Framework of Network Issues

Major Issues	Sub-Issues
Infrastructure	Connectivity Equipment Throughput Configuration Mgmt
Information System Policy and Management	Centralized Management Coordination
Mission Needs	Medical Focus Base Focus
Security Management	Technology Capability Multi-level Security COTS Focus Political/Management Decisions Legal focus (Due Diligence)
Social Engineering	People as Weak Link
Personnel Issues	Continuity Training Manpower
Dependence	Ability to do without Impact of Contracts

Comparison of the Network Issues Framework and the TIMPO Plan

The TIMPO plan is a major step forward in addressing the security woes of the military health system (MHS) in general. The TIMPO is chartered to design, provision, and deploy a standards based, common infrastructure throughout the MHS. The intent is to migrate the architecture to one that is tailored to the specific connectivity and security needs of the MHS. The plan TIMPO proposes is in line with the GASSP and appears to be a viable approach for dealing with the MHS requirements to operate in the Tri-Service environment. The TIMPO plan already addresses many (13 of 19) of the issues identified in this research. The plan clearly addresses the issues of Infrastructure, Mission Needs, and Security Management. Part of the issue of dependence is effectively neutralized

from the standpoint of securing the system and ensuring adherence to standards for future systems. Additionally, TIMPO has been established as the central management element to provide MHS to all the Services. This does not resolve the disconnect between the OASD(HA) and the Air Force SC community. TIMPO is an office under OASD(HA) and is working medical network issues; however, TIMPO does not direct or otherwise control Air Force SC actions. Therefore, the issue of centralized management has not changed. Hopefully, a tighter coupling will develop between TIMPO and the Air Force SC community. Evidence of this closer working relationship is taking shape as representatives of AFCA and TIMPO are in meetings to ensure that the strategies of both organizations are considered as TIMPO moves forward.

The TIMPO plan also encompasses some personnel issues. Medical community manpower requirements were considered and some training standards have been identified for the new architecture. The issue of personnel continuity is not addressed and may be outside the plan's scope. The same may be true for the dependence issue of contract length. These two issues seem to focus more on implementation of new systems, whereas the TIMPO plan is an architectural change primarily in support of existing systems. The one area where more attention would be of significant benefit is in social engineering. This is an area of security that the research respondents said is under-emphasized.

Implications for Practitioners and Researchers

By combining the two points of view, a more complete framework is provided that better represent the issues that should be considered for any potential solution to the

Air Force medical community's network problem. The implication for practitioners is to use the issues framework. This framework identifies major issues and their specific elements that should be considered. By giving attention to all of the issues, there is a better opportunity for successful implementation. For researchers, this study provides an opportunity to better identify the issues related to network security.

Limitations of the Research

Key limitations of this research include the potential for bias and the defined population of interest. Specifically, the literature review describing the existing network security situation and the classification of the various elements and issues as relevant are potentially biased. While much of the findings in the literature were from independent organizations (i.e. the General Accounting Office), the remainder was from a variety of published sources that may have hidden biases. To minimize this impact in this research, unsubstantiated views were not considered. Further, the data collected from questionnaire respondents is subject to their biases and to any ambiguity of the data collection process. The respondents gave information based on their familiarity with network systems and issues; their responses are limited by these biases.

Finally, the limited scope of the research in turn limited the breadth of the conclusions. This exploration was conducted on the Air Force's major medical centers with the intent to apply throughout the Air Force medical community. Any potential external application (such as for the Army or Navy's major medical centers) was referenced as an area for future research and not addressed as a conclusion.

Recommendations

The research findings indicated that two types of recommendations appear necessary. The first involved recommendations for action by the Air Force and the Air Force Medical Service. The second group of recommendations involved academic interests; these were presented as areas for future research and are areas this research effort would have include given sufficient opportunity.

Recommendations for Research. In addition to the recommendations for action by practitioners, many opportunities to expand and refine this research were identified. With respect to this research effort, repetition of this research is needed to confirm the identification of the seven-issue framework that should be used when assessing network solutions for the Air Force medical networks. Additionally, there is potential value in expanding this research effort to include an evaluation of all the Air Force medical facilities. Further inclusion of DoD medical facilities would also be of value given the attempts of TIMPO to develop a Tri-Service solution. Another important area for future research is a closer analysis of the framework. This should be done in direct comparison to GASSP and the TIMPO plan. Potentially, the issues developed in this research could be included as part of the GASSP.

Conclusion

The framework developed in this research effort is proposed as a more complete set of issues that have bearing when considering a potential solution to the Air Force's medical network dilemma. It is an important step toward a better understanding of the impact of various network issues. The new issues identified by network experts

representing each of the Air Force's major medical centers and their corresponding base network organizations should be considered in addition to those typically addressed in medical network solutions. Social engineering, dependence of the medical establishment on outside organizations, and contract length should also be considered. Additionally, the lack of an overarching controlling authority for DoD networks remains a concern. This last issue is seen by most of the respondents in this study as a major problem in promoting a unified IT plan. Implications for practitioners are significant and provide support for evolve how network security decisions are made. By understanding the network security nuances and the issues involved for effective, efficient decision making, mistakes could be avoided that limit the benefit, increase costs, or risk mitigation.

Appendix A: Data Collection Tables

	A	B	C
3. Services provided by networked affiliates	MX on software; Data interpretation; EDI for medical supply ordering; Claims/ Appointments for Tri-care (Allied Health)	N/A	Central Appts; "SIERRA" is not stand alone. General supplier and Pharacy stuff provided over internet
4. Comparison between major med centers and the rest	Quite varied, but same general services	N/A	Med centers are unique; much higher volume, and overflow of patients from other locations. Also the number and variety of services provided is much greater.
6. What drives the AF med dependence on affiliates	Everything on the line side (base) is equally outsourced, somewhat the same for med.	N/A	reliance on partners for appointment scheduling
8. How able is the AF med able to do without the services provided by affiliates	Health care is the primary mission--still can do this even without the other services	N/A	
10. How able is the AF med able to perform affiliate services in-house	Existing systems are proprietary--would take years and $$$ to recreate what's out there right now.	N/A	
12. How able is AF med to obtain affiliate services from other sources	We're stuck with Some systems because of the proprietary issue. Others are more open.	N/A	
14. How long-term are AF med relationships with its affiliates	Contracts are typically 5 years with series of 5 1-year options.	N/A	Some mandates by DoD; can still change, just takes longer
16. How able is the AF med to change which affiliates it does business with	Personnel can adapt but current contracts limit our abliity to change.	N/A	
18. Benefit areas: Impact of migration of No BR to BR	Have to pay for multiple lines.		
20. Benefit areas: Impact of migration of No BR to I BR	Might have hubs, etc. outside our control. Accessibilitiy restricts access to those who need the data		
22. Benefit areas: Impact of migration of BR to I BR	the human component is still an issue for maintaining info integrity		
24./69. What's the most beneficiial aspect of net security	People want to know "when" theycan get the data; they want it now!	reliability	This is what we're trying to protect
26./71. Cost areas: Impact of migration of No BR to BR	Support base picks up the burden	DMZ of Barrier Reef; servers moved out of DMZ - duplicates	
28./73. Cost areas: Impact of migration of No BR to I BR		Big initial equipment costs	duplication of effort and equipment
30./75. Cost areas: Impact of migration of BR to I BR	due to movement of responsibility of Comm SQ to the maintainers and operators of the i BR network.	same as 28	duplication of effort and equipment
32./77. Added Cost areas: Impact of migration of No BR to BR	Long haul might be affected by fee for service. Liability is affected because of increased protection of info. Reduces the likihood of a HIPA violation	additional mngt.	

	D	E	F
3. Services provided by networked affiliates	N/A	EDI for nutritional medicine (tracking chowhall supplies), for pharmacy supplies and refill; and for general med supplies	N/A
4. Comparison between major med centers and the rest	N/A	more technically advanced. More robust system (had money to throw at it). Dramatically higher volume of traffic.	N/A
6. What drives the AF med dependence on affiliates	N/A	For Tri-care to work, must have full access to provider information. Overall the dependence is increasing	N/A
8. How able is the AF med able to do without the services provided by affiliates	N/A	Not much of the med community is directly tied to the services, but all would feel the impact	N/A
10. How able is the AF med able to perform affiliate services in-house	N/A		N/A
12. How able is AF med to obtain affiliate services from other sources	N/A		N/A
14. How long-term are AF med relationships with its affiliates	N/A	To a point, the AF med is being taken advantage of. . .lonterm contracts limit the community to see the benefits of free enerprise and non-proprietary systems	N/A
16. How able is the AF med to change which affiliates it does business with	N/A		N/A
18. Benefit areas: Impact of migration of No BR to BR			
20. Benefit areas: Impact of migration of No BR to I BR		Don't see how IBR is beneficial all the added costs with little to show. Just need to pay more for a bigger pipe.	
22. Benefit areas: Impact of migration of BR to I BR			
24./69. What's the most beneficiial aspect of net security	Nature of what we do - high reliance on pure info		
26./71. Cost areas: Impact of migration of No BR to BR		Unique at this base: have access to the 3CO etc. technical training since it's located on station.	Hospital has same net; firewalls managed by AFNCC
28./73. Cost areas: Impact of migration of No BR to I BR	Bases are funded for the long-haul stuff		Multiple firewall, etc.; cost is currently absorbed by base; would have to shared out by all
30./75. Cost areas: Impact of migration of BR to I BR		duplication of all the support base equipment is very expensive	same issues as before but some spt equip would be no change
32./77. Added Cost areas: Impact of migration of No BR to BR		contract issues will require more attention. Secure socket links reduces their liability	

	G	H	I
3. Services provided by networked affiliates	Appointment Scheduling	N/A	MedLOg (supply procurement system; CHCS services
4. Comparison between major med centers and the rest	Much bigger. More problems working integration of more services and connectivity requirements	N/A	Bigger has better high-tech initiatives. Smaller facilities usually have same services the are directed (regionally managed) by the major medical centers.; they have much less volume. Often, the O&M $$ goes toward med treatment first, support second.
6. What drives the AF med dependence on affiliates		N/A	
8. How able is the AF med able to do without the services provided by affiliates		N/A	
10. How able is the AF med able to perform affiliate services in-house		N/A	Cost prohibitive. Many must contract out to provided needed expertise.
12. How able is AF med to obtain affiliate services from other sources		N/A	Very Low due to proprietary issues
14. How long-term are AF med relationships with its affiliates		N/A	DoD and AF contracts are not set up for short term
16. How able is the AF med to change which affiliates it does business with		N/A	
18. Benefit areas: Impact of migration of No BR to BR			Accessibility still hasauthentication requirements so it's still somewhat restricted.
20. Benefit areas: Impact of migration of No BR to I BR			
22. Benefit areas: Impact of migration of BR to I BR			
24./69. What's the most beneficiial aspect of net security		Even though not challenged the BR sacrifices speed for info integrity	Infrastructure is in place to provide availability
26./71. Cost areas: Impact of migration of No BR to BR	slightly higher; typically not starting from ground zero.	Adding proxies, firewall, extra SMTP relays, and certification to operate - increase	Suport Base gets stuck with the equip costs. Same with personnel issues
28./73. Cost areas: Impact of migration of No BR to I BR	More people to work/manage the different systems are required.	Added equip and systems	
30./75. Cost areas: Impact of migration of BR to I BR	Basically , we don't see more people coming down the pipe. More people and more training is required for localized management	fine tuning to various customers will increase prices	Individual purchases of support equip (server farms, etc.) is costly. No sharing of equipment
32./77. Added Cost areas: Impact of migration of No BR to BR	More work, more costs		with them meeting connectivity standards the comtractors will have to raise costs

	J	K	L	M
3. Services provided by networked affiliates	N/A		EDI for drug/generla med supplies	N/A
4. Comparison between major med centers and the rest	N/A	Much biger pipes and equipment requirements to handle the larger volume of traffic	Med centers have much bigger volume of network traffic. Budgets allow for tral projects to support unique services	N/A
6. What drives the AF med dependence on affiliates	N/A		Much of services is outsourced; short supply of options	N/A
8. How able is the AF med able to do without the services provided by affiliates	N/A			N/A
10. How able is the AF med able to perform affiliate services in-house	N/A		not trained/educated for that	N/A
12. How able is AF med to obtain affiliate services from other sources	N/A		budgetary and personnel restrictions limit the options	N/A
14. How long-term are AF med relationships with its affiliates	N/A		Tightly bound by DoD contracts	N/A
16. How able is the AF med to change which affiliates it does business with	N/A		limited by length of contracts	N/A
18. Benefit areas: Impact of migration of No BR to BR				
20. Benefit areas: Impact of migration of No BR to I BR				
22. Benefit areas: Impact of migration of BR to I BR			Multiple DISN POPs is costly	
24./69. What's the most beneficiial aspect of net security		Information Resource Protection is the primary focus; everything else falls out by having this	That's what it is intended to support	wouldn't mind getting slower info as long as it is reliable
26./71. Cost areas: Impact of migration of No BR to BR				
28./73. Cost areas: Impact of migration of No BR to I BR	duplication of hw & sw			all the different systems to take care of, etc.
30./75. Cost areas: Impact of migration of BR to I BR				
32./77. Added Cost areas: Impact of migration of No BR to BR			Closing redundant circuits helps long-haul costs. Also HIPA may lessen the liability issue for contractors	Minimal increase in QAE; Yokota forces them to give better protection

	A	B	C
34./79. Added Cost areas: Impact of migration of No BR to I BR	(Same)		much more management required on contracts
36./81. Added Cost areas: Impact of migration of BR to I BR		duplication	
38./83. How capable is SOTA in Net Sec for AF med nets	Technology exists, just not allowed to fully implement		
85. How capable is SOTA in Net Sec for AF nets	same as 83		
40./87. Attacker interest in networked data	Not every hacker wants access to med/other data unless they're after money making opportunities.		
42./89. Vulnerability of netorked data	There are alwayss vulnerabilities since we make mistakes and compromises on policy	Emphasis is better on mission; day to day become complacent	a lot of the information is vulnerable. People don't use proper safeguards.
44./91. Attacker ability to gain user access	Depends on the purpose of the hacker.		We can limit their direct access but too many other options exist for them to gain access.
46./93. How likely will attackers be dissuaded from attacking based on net sec	Some will always try, even if just for the challenge.		
48./95. User Trust Ordering of net sec options	Isolation of the net provides closer control and allows configuration for a smaller # of users; better tailoring to misison needs	Amount of confidence for isolated mngt. Vs. central mngt.	BR has name recognition and has been touted as the way to go. People will believe that.
50./97./99. How does net sec config. Reflect trust of users			
52./101. How trust-worthy are AF med nets	Average. Have some protective measures	they need to deal with DoD, commercial, causes management/ security problems	Not bad. We have a lot of external connectivity but it's managed well.
54./103 How trust-worthy are the AF med nets perceived	Thought of as the weak link, the finger has been pointed at our other connectivity		
56./105. What net sec config is best for AF med nets	Should be able to work out all ot the configuraiton issues. It'll cost, but we can do it	they need protection; IBR cost savings	Due to uniqueness of the mission, patient load and types of sensitive information.
57./106. What's the area of greatest expense in the config chosen in 56./105.	Training and establish new mindset	Design & implement of intelligent systems	Short term: Infrastructure Long Term: Training
59./108. What net sec config is best for AF nets	1/2 million people in the .mil pie. Breaking into smaller pieces will crease less opportunity for exploitation. Can provide multiple levels of security		serves the needs for that group. Commonality of function, mission, etc.
60./109. What's the area of greatest expense in the config chosen in 59./108	Net Sec Equipment and Infrastructure	Infrastructure	Training
61./110. What other areas of consideration have impact in choosing net sec config	Business partner vulnerabilities (middlemen)	Top down direction/Buy in; Each service on own/interop	look at the uniqueness of each base. Training of network staff (3CO's) not available to med net personnel
62./111. What other net sec alternatives could be included			

	D	E	F
34./79. Added Cost areas: Impact of migration of No BR to I BR			still same link to outside
36./81. Added Cost areas: Impact of migration of BR to I BR			can go up an item depending on complexity
38./83. How capable is SOTA in Net Sec for AF med nets		Capability to overcome vulnerabilities is there.	
85. How capable is SOTA in Net Sec for AF nets		same as 83	
40./87. Attacker interest in networked data		nature of the attacker is to go after the most critical info.	Most hackers go for publicity (hacking web sites); maliscious hackers will go for the most damaging or sensitive info
42./89. Vulnerability of netorked data	Mission stuff is likely on classified network; good emphasis to stay on top of this	We have too many connections to manage.	all equal since for most part they are protected
44./91. Attacker ability to gain user access		Barrier Reef has reduced their ability	AF much better protected than civilian
46./93. How likely will attackers be dissuaded from attacking based on net sec		based on a risk of prosecution	
48./95. User Trust Ordering of net sec options	An isolated configuration makes easier to defend so increases reliability		different- they usually go elsewhere because they go for targets that have an area easy to exploit
50./97./99. How does net sec config. Reflect trust of users			
52./101. How trust-worthy are AF med nets	Low; backdoors	they can be a lot better. But are better than other expect	Do have protective measure = those w/BR
54./103 How trust-worthy are the AF med nets perceived			Most believe hospital networks are unprotected
56./105. What net sec config is best for AF med nets	Isolation has good points; some exception (outgoing modems only) for quick movement of life critical info	Cuts down on access points	
57./106. What's the area of greatest expense in the config chosen in 56./105.	Training of personnel	TRAINING!	BR costs would be covered by base; no real increase in costs
59./108. What net sec config is best for AF nets	Same & better to work w/single front door		
60./109. What's the area of greatest expense in the config chosen in 59./108	Training	Training again but to a lesser degree	Training is biggest; no short cuts available in AF; we train them and they leave for commercial sector
61./110. What other areas of consideration have impact in choosing net sec config	Greater bandwidth to accomadate speed/throughput	AF addresses everything in terms of costs as opposed to best value. Also standardization of solution (BR) can lead to a common vulnerability. Using multiple, equally effective configurations would minimize this.	downward directed programs from many sources; AF base level is also an issue
62./111. What other net sec alternatives could be included		BR is the way to go.	

	G	H	I
34./79. Added Cost areas: Impact of migration of No BR to I BR	More work, more costs	dedicated contract support and move lines	More connections requires more contractor support and more oversight
36./81. Added Cost areas: Impact of migration of BR to I BR		same as 79	
38./83. How capable is SOTA in Net Sec for AF med nets	It's there; it'll work if politics and the "people" use it to its potential.	capability is there (equip) to lock things; minimal addressing of human factors social engineering such as weak passwords, shared access, etc.	Technology definitely exists; but would severely limit current support capability for sharing critical info.
85. How capable is SOTA in Net Sec for AF nets	same as 83	same as 83	same as 83
40./87. Attacker interest in networked data		mission is always an area of high interest	
42./89. Vulnerability of netorked data	SOTA in net sec is not implemented	social engineering and political factors keep us from walling up all the holes; impact customer service too	
44./91. Attacker ability to gain user access	most have sufficient protection	same as 89	monitoring and audits of network activity (provided by BR) keep this down
46./93. How likely will attackers be dissuaded from attacking based on net sec	attackers will go where its easiest to get in	would get better results if could fully implement to the capability threshold	
48./95. User Trust Ordering of net sec options		there is some lack of trust in all but ranked as indicated	They have more trust for the configuraiton that is more in their control (closer to them) and that keeps others out
50./97./99. How does net sec config. Reflect trust of users		increases in security measures indicate decreases in trust of users	
52./101. How trust-worthy are AF med nets	Have multiple access points. Focuses on the day-to-day med needs and not on security	not sure but their focus is customer service and access to info for many groups; so decreased focus in security	There are still backdoors.
54./103 How trust-worthy are the AF med nets perceived		same	Yes there are backdoors, but others don't fully understand how the system is set up and what the vulnerabilities actually are
56./105. What net sec config is best for AF med nets	Isolation of the medical networks will cost through the nose, but it will give both the base and the medical neetworks the chance for security	none really answer all problems so BR would be a default	Enables Med to conduct business at the level to provide needed service to physicians etc. (tel-net from home). Also healthcare is a regional activity, not base specfic
57./106. What's the area of greatest expense in the config chosen in 56./105.	Getting the technology and the equipment in place	political factors; dealing with decreased customer service	Net Sec equip is important in the short term then Training becomes the focus
59./108. What net sec config is best for AF nets		Mission critical info is minimal on SBU nets and secret should be first focus	Each base has diferrent mission requirements
60./109. What's the area of greatest expense in the config chosen in 59./108	Initial Equipment, then Training of personnel	Maint. & training	Net Sec equip is important in the short term then Training becomes the focus
61./110. What other areas of consideration have impact in choosing net sec config		the need for continuity leads the network jobs to being GS or contractor not GI	Really need a unified IT Plan. There is a big disconnect between the SG and SC communities. Civilian continuity would reduce training issues (costs) , etc.
62./111. What other net sec alternatives could be included		No solution will fix all problems	

	J	K	L	M
34./79. Added Cost areas: Impact of migration of No BR to I BR			Again Providing more POPs is costly	same
36./81. Added Cost areas: Impact of migration of BR to I BR				
38./83. How capable is SOTA in Net Sec for AF med nets	The authority is the limiting factor; the leadership wants access			People are the limiting factor; they trust too much when they shouldn't
85. How capable is SOTA in Net Sec for AF nets	same as 83			same
40./87. Attacker interest in networked data		The attackers are interested in anything they can get a hold of.		
42./89. Vulnerability of netorked data	we are protecting those assets but there are always new hacker tools			back doors lead to problems
44./91. Attacker ability to gain user access			Given that not all have moved from No BR, IPAP instpections have revealed many weaknesses	backdoors exist
46./93. How likely will attackers be dissuaded from attacking based on net sec	they do it because they want to and we can't retaliate	BR and IBR may have some effect. Limits the direct access to the systems and individual terminals on the network		Isolated BR gives more front doors to potential attackers
48./95. User Trust Ordering of net sec options				closer control of BR will give more sense of control and security
50./97./99. How does net sec config. Reflect trust of users				
52./101. How trust-worthy are AF med nets	Must deal with their outside connections	In some cases they are being blocked out; some vulnerabilties still exist.		back door
54./103 How trust-worthy are the AF med nets perceived		Red-headed stepchild--its easiest to point to us, even when not warranted	Outages of network service and backdoors give the impression we don't know what we're doing.	
56./105. What net sec config is best for AF med nets	under organizational control won't have incompatibilities of lower units	Must maintain affiliation with outside agencies and other medical facilities despite the security issue	Nature of the medical info systems (dependent on outside sources of info--private hospitals, doctors, DoD and AF too) requires a different approach. Focus isn't on security	
57./106. What's the area of greatest expense in the config chosen in 56./105.	Start up costs: Training & Equipment	Number and training of personnel to handlethe load	Get and Pay for Personnel	Time, the other stuff is in place (sunk costs)
59./108. What net sec config is best for AF nets			Med is only one having real probs with BR. It seems to work for everyone else.	On the SBU side we can control things better if allowed to
60./109. What's the area of greatest expense in the config chosen in 59./108	same as 106	Number and training of personnel to handlethe load	Training Personnel	no change
61./110. What other areas of consideration have impact in choosing net sec config	Sell ideas to descision makers and users - need top down support; BR process: SC community in full control of Hospital rather than SC and butting	Cutting across services causes problems in moving past parochial interests (each has different focus that the medical service must contend with. Need One POC for managing it all to deal with this.	Biggest problem is that the systems aren't deployed by the Air Force. Most are directed from beyond the AF's control and have different requirements. HA and SG not working with SC.	Building Firewalls behind the front door firewall
62./111. What other net sec alternatives could be included		Use something like Cisco's Pix Firewall to increase throughput for the customers		

Bibliography

Adams, Charlotte. "DOD information security takes big strides but still lags behind threats." *Military & Aerospace Electronics*, Jan97, Vol. 8 Issue 1, p17, 3p, 1 diagram, 2c

Adams, James. *The Next World War.* New York: Simon & Schuster. 1998.

Air Force Communications Agency/Information Protection Technical Services Branch (AFCA/GCIT). "Barrier Reef Home Page." WWWeb page, n. pag. http://www.afca.scott.af.mil/gc/gci/techserv/index.htm 13 July 1998.

Air Force Communications Agency/Information Protection Technical Services Branch (AFCA/GCIT). "The Information Protection Barrier Reef 12 Step Process: Barksdale AFB Case Study." WWWeb page, n. pag. http://www.afca.scott.af.mil/gc/gci/techserv/index.htm 19 Aug 1997

Air Force Communications and Information Center (AFCIC). "Boundary Protection for Air Force Networks - Barrier Reef," HQ USAF/SC, Washington D.C. 27 May 1997.

Air Force Communications and Information Center (AFCIC), *Communications and Information Strategic Plan.* United States Air Force Communications and Information Directorate, Washington D.C. Sept 1999, p. 1.

Air Force Computer Emergency Response Team (AFCERT). "Welcome to the AFCERT." WWWeb page, n. pag. http://afcert.csap.af.mil/index.html 13 July 1998.

Alberts, David S. *Defense Information Warfare.* Washington D.C.: U.S. Government Printing Office, 1996.

Arnavas, Donald R, Ruberry, William J. *Government Contract Guidebook.* Federal Publications Inc. Washington D.C. 1994.

Blackwell, Ed. "Building a solid foundation for Intranet security." Information Systems Security, Spring99, Vol. 8 Issue 1, p45, 9p, 1 chart.

Caldwell, Bruce. "Keeping the PBX Secure." *2600.* CMP Publications, Inc. 15 Oct 1990, 291:25. http://www.2600.com/phrack/phrack32.html

Cash, Jr., James I. and Paul R. Lawrence. "The Information Systems Research Challenge: Qualitative Research Methods," *Harvard Business School Research Colloquium, Vol. 1*, 1989.

CERT Coordination Center. "CERT/CC Statistics: 1988 – 1999." Carnegie Mellon, 1999. Available On-Line: http://www.cert.org/stats/cert_stats.html

Cloutier, Wayne. "Building the Cyber Wall." *The Connection: The Air Force Information Protection Journal*, HQ AFCA/SYSI. December 1996. Available On-Line http://www.afca.scott.af.mil/gc/gci/sate/connect/dec96.htm

Cohen, D. *Electronic Commerce*, Information Sciences Institute, Marina Del Rey, California, 1989.

CSAF, Washington D.C. *Information Assurance--Protecting Our Networks.* Electronic Message. 272351Z OCT 98.

Churchill, Gilbert A. Jr. *Marketing Research: Methodological Foundations.* The Dryden Press, New York, 1983.

Cooper, Donald R. and Emory, C. William. *Business Research Methods, 5th ed.* Charles D. Irwin, Inc. Chicago, 1995.

Cooper, Donald R. and Schindler, Pamela S. Business Research Methods. Irwin/McGraw-Hill, Boston, 1998.

Dacey, Robert F. *USDA Information Security–Weaknesses At National Finance Center Increase Risk Of Fraud, Misuse, And Improper Disclosure: Report to the Secretary of Agriculture.* United States General Accounting Office, Accounting and Information Management Division, Washington, D.C. 20548

Debreceny, Roger. *Computer Crime is an Inside Job.* Available (On-line) http://www.rutgers.edu/Accounting/anet/lists/AAUDIT-L/0907.html

Denning, Dorothy E. Information Warfare and Security. Reading, Mass: Addison-Wesley Press, 1999.

Department of the Air Force. *Compliance with the Law of Armed Conflict.* AFPD 51-4. Washington: HQ USAF, 26 April 1993.

Department of the Air Force. *Network Management.* AFI 33-115. Washington: HQ USAF, 1997.

Department of the Air Force. *Security Engineering Strategic Business Function: Concept of Operations.* Brooks AFB San Antonio: HQ AFMSA/SGSI. 18 August 1998.

Dodaro, Gene L. "Information Security-Serious Weaknesses Place Critical Federal Operations and Assets at Risk," *Report To The Committee on Governmental Affairs, U.S. Senate.* Washington D.C. 28 Sep 1998.

EDISMC. Notes on Committee Responsibilities. Department of Defense Electronic Data Interchange Standards Management Committee. WWWeb page, n. pag. http://www-edi.itsi.disa.mil/management.html

Fisher, Sharon. "Guarding Against Network Attacks," *CommunicationsWeek*, 2/27/95 Issue 545, p1, 2p, 1 diagram, 3bw

Fogleman, Ronald R. "Fundamentals of Information Warfare—An Airman's View," Speech to the National <Security> Industry Association-National Defense University Foundation Conference on The Global Information Explosion, Washington, D.C., May 16, 1995

Fotsch, Edward. *Securing On-line Data.* Healthcare Financial Management Association, November 1996.

Futch, Lee. Public Relations Representative, Tri-Service Infrastructure Management Program Office, Fort Sam Houston Army Post, San Antonio TX. Personal Interview, 10 Dec 1999.

General Accounting Office (GAO/AIMD-96-110). "Information Security: Opportunities for Improved OMB Oversight of Agency Practices (GAO/AIMD-96-110)"

Griffith, Samuel B. *Sun Tzu: The Art of War (Translation).* Oxford University Press, London. 1963.

Grundy, John. "Trust in Virtual Teams," *Harvard Business Review*; Section: Letters to the Editor, November 01, 1998

Gwartney, James D., Stroup, Richard L. MicroEconomics, Private and Public Choice, 8th ed. The Dryden Press, Fort Worth TX. 1997.

Hart, P. and D. Estrin. "Inter-organization Networks, Computer Integration, and Shifts in Interdependence: The Case of the Semiconductor Industry," *ACM Transactions on Information Systems,* Vol. 9, No. 4. pp. 370-398, 1991.

Hayes, Ian and Ulrich, William. "It's All About Managing Risk," *Software Magazine*, 04/15/98, Vol. 18 Issue 6, p12, 4p, 2c, 1bw

Heberlie, Brian and Tolbert, Mary. *Impact Of Actual Facilitator Alignment, Co-Location And Video Intervention On The Efficacy Of Distributed Group Support Systems.* MS thesis, AFIT/GIR/LAS/99D-4. School of Engineering and Management, Air Force Institute of Technology, Wright-Patterson AFB OH, December 1999.

Holland, Christopher P. "The Importance of Trust and Business Relationships in the Formulation of Virtual Organizations," *Organizational Virtualness: Proceedings of the VoNet – Workshop, April 27-28, 1998.* Institute of Information Systems, Department of Information Management, University of Bern.

Houser, W., et al. "EDI Meets the Internet." Department of Veterans Affairs, Washington D.C., Jan 1996. Available (On-Line) http://www.cis.ohio-state.edu/htbin/rfc/rfc1865.html

Howard, John D. "An Analysis of Security Incidents on the Internet: 1989 – 1995." Carnegie Mellon University, 1997.

HQ AFCA/GCIT. *The Information Protection Barrier Reef 12 Step Process: Barksdale AFB Case Study*. HQ AFCA/GCIA, Scott AFB, 1997.

International Information Security Foundation (IISF). *Generally Accepted System Security Principles (GASSP) Version 2.0.* Information Systems Security, Fall99, Vol. 8 Issue 3, p32, 20p, 1 chart, 2 diagrams

Jarvenpaa, Sirkka L. et al. "Is anybody out there? Antecedents of trust in global virtual teams," *Journal of Management Information Systems*, Spring98, Vol. 14 Issue 4, p29, 36p, 7 charts, 2 diagrams

Johnson, Lynn. Deputy Chief Technology Officer, Air Force Medical Service, Brooks AFB TX. Personal Interview. 23 Nov 1999.

Libicki, Martin C. *Defending Cyberspace: and Other Metaphors*. Washington D.C.: U.S. Government Printing Office, 1997.

Loch, Karen D. and Carr, Houston H. "Threats to Information Systems: Today's Reality, Yesterday's Understanding," MIS Quarterly, Vol 16 Issue 2, p173, 14p. June 1992.

Loftin, Jeff. "PACAF bases foil cyber terrorism in Beverly Morning exercise," *Air Force News*: May, 1998

McFadden, F.R., Hoffer, J.A., and Prescott, M.B. *Modern Database Management, 5th ed.*, Benjoamin?cummings Publishing Company, Redwood City CA, 1999.

McMullen, Melanie. "The Big Hack Attack," *Internet Business*: 46-55 (October, 1998).

Mesevich, Alex. "FIRST contributes to computer security," *Connection: The Air Force Information Protection Journal.* AFCA/SYSI. December 1996. Available On-Line http://www.afca.scott.af.mil/gc/gci/sate/connect/dec96.htm

Military Newswire Service. "Pentagon Steps up Fight Against Computer Hackers," *Connection: The Air Force Information Protection Journal.* AFCA/SYSI. December 1996. Available On-Line http://www.afca.scott.af.mil/gc/gci/sate/connect/dec96.htm

Molander, Roger C. and others. *Strategic Information Warfare: A New Face of War.* National Research Defense Institute; RAND, 1996.

Naude, P. and C. P. Holland. "Business-to-business Marketing," *Relationship marketing: Theory and Practice,* pp. 40-54, Paul Chapman Publishing Ltd, London

Payne, Judith E. and Anderson, Robert H. *Electronic Data Interchange (EDI): Using Electronic Commerce to Enhance Defense Logistics.* National Defense Research Institute; RAND, 1991.

SANS Institute. "Roadmap to Intrusion Detection and Vulnerability Detection Tools." WWWeb page. n pag. Http://www.sans.org/tools_roadmap.htm

Segev, Arie and others. "Internet Security and the Case of Bank of America," *Communications of the ACM, 41*: 81-87 (October 1998)

Smith, George. "An electronic Pearl Harbor? Not likely." *Issues in Science & Technology*, Fall98, Vol. 15 Issue 1, p68, 6p

SRA International, Inc. Military Health System Systems Architecture and Design Guidance: Introduction to the Systems Architecture for Infrastructure. Vol. 1. San Antonio TX. 15 Sep 1998.

SRA International, Inc. Military Health System Systems Architecture and Design Guidance: Enterprise Security Architecture. Vol. 7. San Antonio TX. 24 Sep 1998.

Stackpole, Bill. "Thinking Right About Network Security," *Information Systems Security*, Fall98 Vol. 7 Issue 3, p16, 2p

TIMPO. "Critical Infrastructure Protection: DOD Medical Infrastructure Security Requirements and Issues." MHS Infrastructure Security Policy, 16 Aug 1999.

Walsh, Brian. "Mischief, malfeasance and misplaced trust.," *Network Computing*, 05/01/98, Vol. 9 Issue 8, p35, 2p, 1c

Williamson, O.E. "Comparative Economic Organization: The Analysis of Discrete Structural Alternatives," *Administrative Science Quarterly,* Vol. 36, No.1, pp. 269-296, 1991.

Yin, R. K. *Case Study Research: Design and Methods.* Newbury Park, California: Sage, 1989.

Young, Rob. Chief, Network Management Element, Wright-Patterson Medical Center, Wright-Patterson AFB OH. Personal Interview. 12 May 1999.

Vita

Captain Franklin E. Cunningham, Junior, is the son of Chief Master Sergeant and Mrs. Franklin E. Cunningham, Senior, United States Air Force, (Retired). He was born on 3 May 1966 in Naples, Italy. He graduated from Judson High School in Converse, Texas, in 1984. On 12 May 1990, he graduated from Saint Mary's University in San Antonio, Texas with a Bachelor of Science Degree in Biology. On 26 May 1990, he married Ms. Christine Ann Huckobey and they settled in San Antonio, Texas. Before his selection to Air Force Officer Training School, Frank conducted research at the Southwest Research Institute in San Antonio, Texas. On 7 September 1991, he and his wife became first-time parents with the birth of their son, Bryan Kyle. A few months later on 8 April 1992, Frank was commissioned into the Air Force and has served in a variety of duty positions at Seymour Johnson Air Force Base, North Carolina and Francis E. Warren Air Force Base, Wyoming. While stationed in North Carolina, he and his wife celebrated the birth of their daughter, Emily Nicole. Frank entered into the Air Force Institute of Technology (AFIT) Graduate School of Engineering and Management, Wright-Patterson Air Force Base, Ohio in May 1998. He and his family will remain stationed at Wright-Patterson after completion of his AFIT education.

Permanent Address: 158 Amistad Boulevard

Universal City, Texas 78148

REPORT DOCUMENTATION PAGE	Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	December 1999	Master's Thesis

4. TITLE AND SUBTITLE
NETWORK SECURITY VERSUS NETWORK CONNECTIVITY:
A FRAMEWORK FOR ADDRESSING THE ISSUES FACING
THE AIR FORCE MEDICAL COMMUNITY

5. FUNDING NUMBERS

6. AUTHOR(S)
Franklin E. Cunningham, Jr., Captain, USAF

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Air Force Institute of Technology
2950 P. Street
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER
AFIT/GIR/LAS/99D-2

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
HQ AFCA/GCI (Mr. Garry Lee)
203 West Losey Street, Room 2040
Scott AFB IL 62225-5222
(618) 256-4450

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES
David P. Biros, Major, USAF
Phone: (937) 255-3636 (x4826)
E-mail: david.biros@afit.af.mil

12a. DISTRIBUTION AVAILABILITY STATEMENT
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

The Air Force has instituted Barrier Reef to protect its networks. The Air Force medical community operates network connections that are incompatible with Barrier Reef. To overcome this problem, OASD(HA) directed the Tri-Service Management Program Office (TIMPO) to develop an architecture that protects all military health systems and allows them to link with all three services and outside partners.

This research studied the underlying networking issues and formed a framework based on data from network experts from the Air Force's medical centers and their base network organizations. The findings were compared TIMPO and a composite framework was developed that more completely identifies network issues. TIMPO's plan seems on track. It addresses 13 of 19 identified issues and partially addresses three other issues. The TIMPO plan may be improved if the remaining issues are addressed. One issue is lack of central management for all military networks. Each Service and OASD(HA) has its own network controlling authority. No one organization directs the actions of all of them. Additional issues include social engineering, personnel continuity, and medical organization dependence on long-term contract partners. These issues have relevance for addressing potential network solutions for the Air Force medical community.

14. SUBJECT TERMS	15. NUMBER OF PAGES
Information Systems, Biomedical Information Systems, Antiintrusion Devices, Electronic Security, Data Processing Security	97
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL