3-2005

Medical Devices, Support Networks, and their Vulnerabilities: A Case Study of the Integration of Medical Networks into the Air Force Information Network

Paul G. Oleksiak

MEDICAL DEVICES, SUPPORTING NETWORKS, AND THEIR VULNERABILITIES

A CASE STUDY OF THE INTEGRATION OF MEDICAL NETWORKS INTO THE AIR FORCE INFORMATION NETWORK

THESIS

Paul G. Oleksiak, MSgt, USAF

AFIT/GIR/ENV-05M-13

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITYAIR FORCE INSTITUTE OF TECHNOLOGY
Wright-Patterson Air Force Base, Ohio

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the U.S. Government

AFIT/GIR/ENV/05M-13

MEDICAL DEVICES, SUPPORTING NETWORKS, AND THEIR VULNERABILITIES
A CASE STUDY OF THE INTEGRATION OF MEDICAL NETWORKS INTO THE AIR FORCE INFORMATION NETWORK

THESIS

Presented to the Faculty

Department of Systems and Engineering Management

Graduate School of Engineering and Management

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

Paul G. Oleksiak, BS

MSgt, USAF

March 2005

AFIT/GIR/ENV/05M-13

MEDICAL DEVICES, SUPPORTING NETWORKS, AND THEIR VULNERABILITIES
A CASE STUDY OF THE INTEGRATION OF MEDICAL NETWORKS INTO THE AIR FORCE INFORMATION NETWORK

Paul G. Oleksiak, BS

MSgt, USAF

Approved:

/signed/

_____ _____

Dr. Kevin L. Elder (Chairman) date

/signed/

_____ _____

Captain David. D Bouvin (Member) date

/signed/

_____ _____

Dr. Dennis D. Strouble (Member) date

Abstract

With the implementation of “one Air Force, one network” under way it is important to look at how the Air Force plans to incorporate the medical field and its unique systems, networks, and mission. The medical field presents distinctive problems not seen in other areas. Open network vulnerabilities in the medical information systems not only pose a problem for the individual, but to the military service also.

Possible security holes provide both access to vital military & personal information (end strength numbers, current status of personnel, social security), and a door way into the “network”. Intruders now can possibly access command & control systems and other weapon systems. This research provides insight into the current & future information initiatives dealing with the Air Force’s medical field and the Department of Defense’s approach to system security.

This research additionally looks at the laws and regulations dealing with privacy and ethical issues. This purview starts with the recently enacted Healthcare Insurance Portability and Accountability ACT (HIPPA), and concludes with the Laws of Armed Conflict. The research questions were answered through the use of a Case Study and a comprehensive literature review. The medical and network support teams from two Air Force medical facilities were the basis of this study.

Acknowledgments

I would like to express my sincere appreciation to my faculty advisor, Dr. Kevin Elder, for his guidance, support, and tolerance through out the course of this thesis effort. The insight and experience was certainly appreciated. I would also like to thank my fellow classmates for their help and guidance through this journey. Finally, I would like to thank my family and friends, especially my children for their love and support.

Paul G. Oleksiak

Table of Contents

Page

Page

List of Figures

Figure Page

List of Tables

MEDICAL DEVICES, SUPPORTING NETWORKS, AND THEIR VULNERABILITIES:

A CASE STUDY OF THE INTEGRATIONOF MEDICAL NETWORKS INTO THE THE AIR FORCE INFROMATION NETWORK

I. Introduction

Background

Forty minutes. The amount of time that the missile missed its intended target was a mere forty minutes. Saddam Hussein and his sons had left the restaurant forty minutes prior. Had the information been received earlier or processed faster the war in Iraq could have possibly taken a different twist. What if a cyber attack on our Information Systems (IS) was the reason for the delay?

In today's joint world of operations it is all about the information. This is true regardless of the nature of the information. The Air Force is increasingly concerned about protecting information and the systems and networks that it uses to store, process and transmit this information. In today's globally networked environment the Air Force has a growing dependence on information to enable their sophisticated combat capabilities.

We are increasingly vulnerable to potential disruption of our military capability due to system failure, human mistakes or errors as well as a range of deliberate attacks from adversaries who can leverage readily available, easy-to-use, low-cost technologies.

Protecting our information systems and networks requires a multi-faceted approach. In addition to sound engineered and implemented technical capabilities a singular direction, policy, procedures, and trained personnel are necessary.

The Air Force is in the midst of a transformation to a force capable of rapid expeditionary joint operations. The Air Force's *Vision 2020 — Global Vigilance, Reach and Power* captures that philosophy. This strategic plan implements this vision by linking the capabilities the Air Force needs in the future with its core competencies which are outlined in *AF 2020.*

Information Superiority- The ability to control and exploit information to our nation's advantage-ensuring decision dominance. (USAF, 2001)

Former Air Force chief of staff Gen Ryan stated this:

"Air Force Vision 2020 acknowledges information superiority as a core Air Force competency because it provides our joint team the ability to control information to our nation's advantage and ensures we have decision dominance. Decision dominance means we can make smart decisions faster than our adversaries can. Wiser use of information technology is our edge... We must continue to expand this decisive, network-enabled combat edge. Modernizing our information systems ranks with other top Air Force modernization priorities. The combat power of our top-of-the-line weapon systems is enabled by our information network's ability to tie critical information together faster than anyone else can". (Ryan 2001)

General Ryan and Secretary of the Air Force Dr. Peters realized that the Air Force was failing in this regard.

"General Ryan and I are convinced that we can no longer run the Air Force with one foot in the future and one foot in prehistoric times," Secretary Peters said. "We need an over-arching Air Force information technology architecture that draws on the Internet and best commercial practices and a migration plan that moves us over time into compliance with this architecture. Equally important - indeed, perhaps more important - we need to reshape our business processes to make optimal use of information technology." (Peters, 2001)

General Ryan and Dr. Peters held a conference with *Fortune 500* Chief Executive Officers (CEO) and CIOs (Chief Information officers) to discuss their companies approach to information. The results of this summit *Air Force Information Technology Initiatives: Information Technology services consolidation* (2001) included goals to have integrated centrally managed AF IT enterprise services and trusted delivery of information supporting the war fighter. The main concept revolves around an enterprise, or corporate networking environment, and capitalizes on industry best practice. The goal is to give Air Force people worldwide instant desktop access to information they need to conduct peacetime and combat operations.

Information Technology Initiatives

There are numerous initiatives under way in the implementing the strategic goals outlined under the *One Air Force, One Network* policy. The *Combat Information Transport System* (CITS) is one of these initiatives. It will modernize the information transport capability at each Air Force base replacing obsolete copper cable with the fiber technology, improve network management and upgrade voice phone service with new digital switches. *Medical Information Technology Transition* (MITT) is part of CITS. The critical nature and volume of medical information accompanied with possible life and death situations present significant hurdles to system security and limiting vulnerabilities to the entire Air force network.

Research Objective/Questions

The purpose of this study is to assess the Air Force's implementation of the transition (MITT) of medical information systems into the Air Force Network

Research Question

This research seeks to answer the question: How is the Air Force addressing the integration of the medical systems and networks under the policy of "One Air Force, One Network" (Ryan 2001)?

Investigative Questions.

Multiple questions will be addressed in order to answer the research question:

1. How are medical devices integrated into the medical facilities networks?
2. How does the plan address adherence to HIPPA?

3. Does the integration of the medical information systems into the base networks change the classification of the system under the Laws of Armed Conflict (LOAC)? If so, does this make them more susceptible to attack?
4. Is the implementation of several projects/initiatives increasing the possibility for security vulnerabilities?
5. Is direction being given from a single point or multiple agencies/commands?
6. Are there other issues that are not addressed under the current plan?

Research Focus

The focus of the research is the implementation of MITT at Site 1 and Site 2. This research will concentrate on the hospital and network support staff efforts to integrate the medical information systems. This is not an assessment of the facilities or their respective staffs.

Proposed Methodology

The research will be conducted as a Case Study since no control over the behavioral events can be accomplished. The study will be completed in two phases. The first phase will consist of face to face interviews with Site 1 personnel. The second phase will consist of telephone interviews with Site 2 medical and communication personnel.

Assumptions/Limitations

The current AF Initiative (MITT) identifies 90 facilities worldwide which have been chosen for integration. This research focuses on the integration of only the medical communities at Site 1 and Site 2. By limiting the study to two bases some areas of concern may be neglected due to the uniqueness of their individual locations, units, and

existing networks at those two locations. Little research exists on the current Air Force projects. As a result, there is not much to build upon. Since the research is only being conducted at two locations it is possible that the findings will not be representative of the entire Air Force. Time represents the final major limitation for the study. The importance and difficulty of this study command more time than this effort can provide. This study aims to establish the basis for additional research.

Implications

During 2000, Air Force security enforcement tools identified and denied 315 million suspicious connection attempts. The AF experienced one unauthorized access to its networks by an unauthorized outsider for every 20 million suspicious connection attempts. During 2001, the number of suspicious connections jumped from 315 million to over 1.1 billion. Fortunately the rate of unauthorized connections by an outsider declined to one for every 84 million suspicious connections attempts(Gilligan 2002). The addition of the medical networks to the overall network provides a greater opportunity for those who want to gain access or due damage to the Air Force networks. This research will aid in pinpointing possible weaknesses (extensive use of waivers for security patch implementation, Food and Drug Administration governance of medical devices, numerous ongoing AF network initiatives) in the existing information assurance policies and procedures governing the medical networks.

Preview

This chapter provided a basis for the need for information security for medical networks. The Air Force vision for information technology and ensuring that the war fighter has the tools he or she needs to do their job was discussed. Chapter II will cover current plans to accomplish that vision and general literature relevant to the dilemma of integrating the Air Force medical networks, network security, personal privacy, and the Laws of Armed Conflict (LOAC) and how they might affect the efforts.

Chapter III will explain the methodology used in this study to establish the framework of issues that the Air Force plan might present during implementation. Chapter IV will present the data analysis and results from the data collected in this study. Chapter V will discuss the findings of this case study and their relevance to the problem. It will also present limitations of this study and recommendations for future research.

II. Literature Review

Overview

Today there is rapid movement toward increased use of interconnected networks. Although this trend promises many benefits, it also poses many risks. The military medical field and its technology introduce unique aspects in regards to systems and network connectivity. Partnerships with civilian healthcare facilities exist due to today's business environment and scarceness of qualified Air Force personnel. Open network vulnerabilities in the medical information systems not only pose a problem for the Medical Healthcare System (MHS), but to the military service itself. Ill guarded medical information systems provide a doorway in the Air Force's network. Command & Control and personnel information is now accessible. Potential attack to systems carrying this information as well as weapon and intelligence systems are possible.

The purpose of this research is to assess the Air Force's handling of those unique aspects under the current initiative to transition medical information technology into the Air Force Network.

This literature review examines the writings relevant to the research topic of integrating the Air Force medical networks. This endeavor will provide necessary information vital to the assessment of the Air Force's plan. First, the guiding principles and reasons for coordinated implementation of information technology projects are discussed. The examination will cover both the Air Force's current IT strategy and several of the numerous information technology projects underway. Following this is a look at the legal implications inherent to integrating the medical networks into the Air Force's network. Lastly, a review of the benefits gained by standardization will be performed.

Coordinated Implementation

Air Force Vision 2020, Air Force Information Strategy, and One Air Force, One Network

As stated in chapter one the Air Force is under going a transformation to a force capable of rapid expeditionary joint operations. The Air Force's *Vision 2020 — Global Vigilance, Reach and Power* captures that philosophy. It provides the direction and foundation for subsequent Air Force IT doctrine. The plan states that the Air Force will develop and field the critical future capabilities to sustain its core competencies, and the command and control through which it employs them (USAF 2001).

One of those seven core competencies is *Information Superiority*. AF Vision 2020 defines this as "the ability to control and exploit information to our nation's advantage to ensure decision dominance" (USAF 2001). AF Vision 2020 further states that leveraging information technology is the means by which to continue transforming the Air Force's operational capabilities and command and control (USAF 2001). The Air Force looked internally after gathering information from the industry leaders in the information technology field and formulated *One Air Force; one network.*

The strategy is based on adapting the latest commercially available information technologies. AF Vision 2020, *One Air Force*; *one network*, DOD guidance, and task force concepts of operations all influence the direction and make up of the Air Force Strategic Plan. The outcome of this formulation is the Air Force Information Strategy (See Figure 1).

A shortcoming to the Air Force Information strategy developing process depicted below is that it leaves MAJCOM's and functional supporting plans open to personal interpretation by their respective leaders and commanders. The possibility for plans being developed or implemented differently to satisfy a customer locally instead following the prescribed guidance exists.

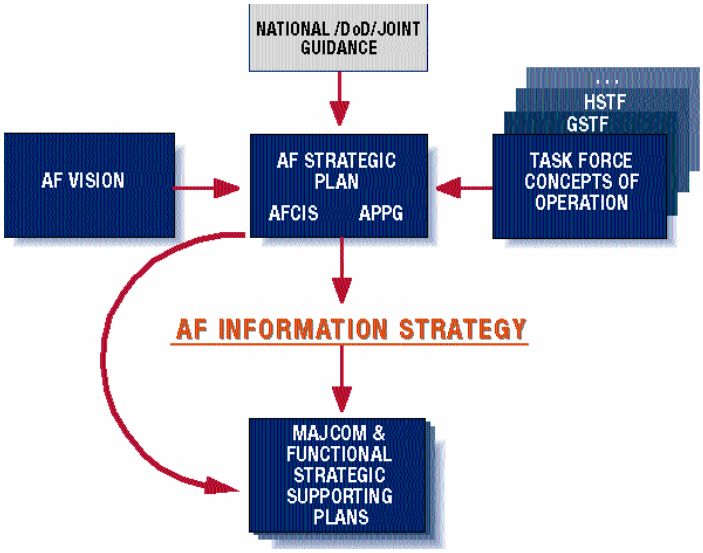

Figure1. Cycle for developing the Air Force Information Strategy (USAF 2001).

The purpose of the Air Force Information Strategy is to bridge the gap between top-level vision and strategy documents, which include the Task Force CONOPS, and the actual planning, decision-making and resourcing activities within the Air Force. The Air Force Information Strategy consists of nine goals through which the Air Force hopes to empower Air force personnel to accomplish the transformation outlined in the Air Force Strategic Plan. The goals are listed in the table on the next page (USAF 2002). The goals form the framework for the development of detailed planning objectives,

implementation projects, and subsequent performance metrics to determine the Air Force's success. For this research we are concerned with only two of them; goals two and three. Goal *# 2* implies that a single global network must be established and it must capable of providing secure data to decision makers at any time. Goal *#3* states the Air Force must be able to successfully protect its information and supporting systems.

To do this the Air Force has employed a "*defense in depth*" approach to simultaneously secure multiple layers of the network, systems, and applications. This tactic requires defining a security architecture that identifies and maps security enforcement policies to employment of protection capabilities. This security design must be executed across all Air Force networks and systems.

Table 1. 9 Goals of Air Force Information Strategy.

Goal	
1	Provide decision-makers and all Air Force personnel with on-demand access to authoritative, relevant and sufficient information to perform their duties efficiently and effectively.
2	Ensure worldwide, real-time and secure access to information via a single integrated global network environment through a robust digital communications infrastructure.
3	Protect Air Force information resources from attack and/or intrusion by both outside forces and internal disruption.
4	Ensure that Air Force integrated information systems are architected to enable modular, platform-independent information management capabilities and are interoperable with Department of Defense and other government information systems.
5	Leverage information technology to support and improve Air Force processes to increase both efficiency and effectiveness.
6	Ensure the Air Force takes advantage of state-of-the-art IT and best commercial practices.
7	Implement knowledge management practices and technologies to assure knowledge is identified, captured, and shared.
8	Empower a focused, well-trained and motivated workforce prepared to continually search out and embrace new information-based capabilities for the Air Force.
9	Ensure responsible stewardship of Air Force financial resources spent on information management and related information technology

Air Force Information Technology Initiatives

Medical Field initiatives

There are several IT initiatives currently underway that directly affect the medical information systems and networks. The main project is the *Medical Information Technology Transition (MITT) Last Mile* Design. Under this program the medical systems and networks at 90 military medical treatment facilities all over the world will be integrated into the Air Force's network. All medical information systems, networks, and networked devices will be connected into the respective location's base network in a standardized design, all placed under base Network Control Center (NCC) and Network Operations and Security Center (NOSC) management (Headquarters Electronics Systems Center 2004).

Several organizations have vital roles in this venture. The Air Force Surgeon General (AF/SG) and the Air Force Medical Support Agency (AFMSA) are responsible for presenting the medical community needs to the Air Force Communications Agency (AFCA). AF/XI and AF/IL provide operational guidance covering the AF network policy. The Combat Information Transport System (CITS) Project Management Offices (PMO) created this design.

The MITT LMD isn't an implementation plan; it's technical in nature. In fact, the document states that. It stipulates that each base's medical facility's integration into the Air Force's network could potentially be different due to the existing medical network. The MITT LMD provides two different designs. It first presents a final end state that according to the CITS PMO "logically meets medical requirements while accommodating AF policy"(Headquarters Electronics Systems Center 2004) (see Figure

2 below). Secondly, the MITT LMD offers an interim state (Figure 3). It accommodates the different access points traffic might take given its source and destination. This interim design is due to the timeliness in which the final end state can be achieved to help mitigate risks in the near term (Headquarters Electronics Systems Center 2004).

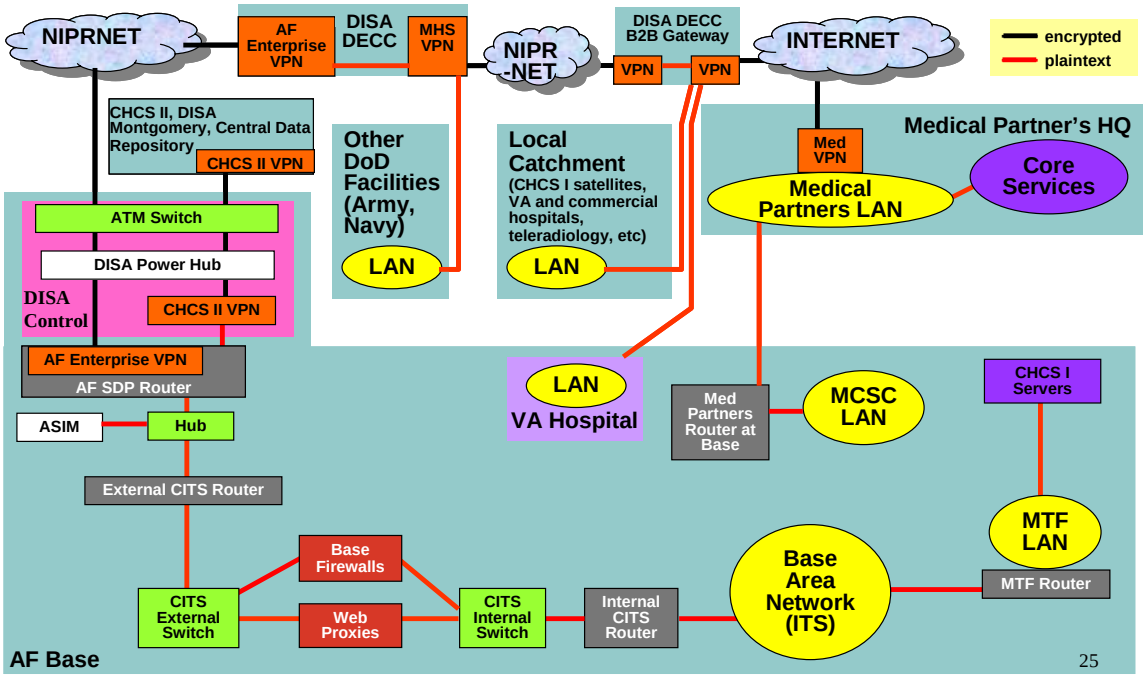

Figure 2- The Last Mile Design - Final Design. (Headquarters Electronics Systems Center 2004)

The design does offer five different options for connecting into the network; weighing the advantages and disadvantages of each. Implementing the standardized MITT LMD includes support for Composite Health Care System (CHCS) II traffic. The CHCS II is a medical and dental clinical information system that will generate and maintain a comprehensive, life-long, computer-based patient record (CPR) for each MHS beneficiary. CHCS II was designed to meet the challenge of making medical and dental records immediately available to providers caring for a highly mobile population that includes 1.4 million active duty Armed Service members around

the world. The system provides authorized users with secure electronic access to a Department of Defense (DoD) beneficiary's comprehensive health record, which includes data on preventative care, illnesses, injuries, and exposures treated at any military treatment facility (MTF). All CHCS II users will have access to any eligible beneficiary's medical/dental record within seconds from any MTF in the world(Office 2004) .

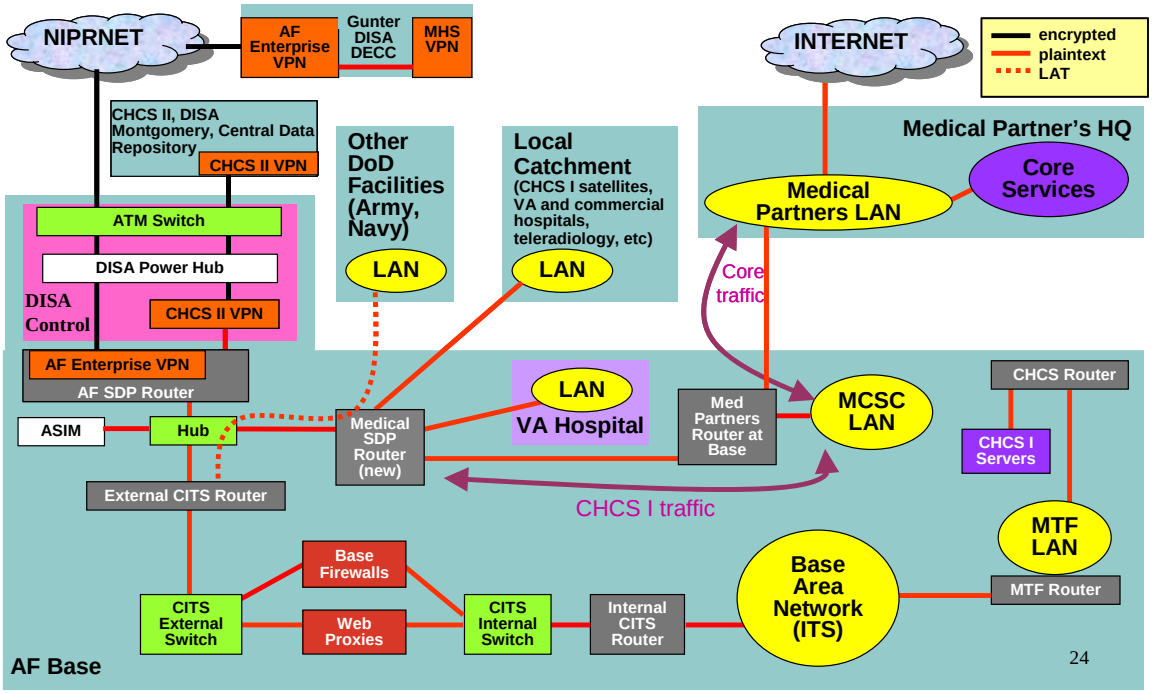

Figure 3- The Last Mile Design- Interim Design.(Headquarters Electronics Systems Center 2004)

Legal Implications

Laws of Armed Conflict (LOAC)

One of the most critical subjects for today's military is the Law of Armed Conflict (LOAC), also known as the Law of War. What is LOAC? According to Joint Publication 1-02; "That part of international law that regulates the conduct of armed hostilities" (Staff 2001).

LOAC is based upon two main sources. These are *customary international law* and *treaty law*. *Customary international law* arose out of the conduct of nations during hostilities and binding upon all nations. *Treaty law* (also called conventional law) arose from international treaties and only binds those nations that have ratified a particular treaty. *Treaty law* is generally divided into two overlapping areas: Hague law (named for treaty negotiations held over the years at The Hague, Netherlands) and Geneva law (named for treaty negotiations held over the years at Geneva, Switzerland). The *treaty law* that pertains to this research is Hague law. It is concerned mainly with the means and methods of warfare (e.g., lawful and unlawful weapons, targeting) (Strand 2004).

There are several purposes of LOAC. Some of which include limiting the effects of the conflict, safeguarding the individual rights of and protecting combatants and non-combatants from unnecessary suffering, and preventing the conflict from getting worse. The basic legal principle of LOAC is *military necessity*. This is defined as "the application of only that degree of regulated force, not otherwise prohibited by the laws of war, required for the partial or complete submission of the enemy with the least expenditure of life, time and physical resources." Attacks must be limited to military objectives. This principle imposes a requirement to distinguish between *military* objectives and *civilian* objects (Strand 2004).

Military objectives are objects which by their nature, location, purpose, or use make an effective contribution to military action and whose total or partial destruction, capture, or neutralization, in the circumstances ruling at the time, offers a definite military advantage. Examples of this include troops, bases, supplies, lines of

communications, and headquarters. *Civilian* objects are such things as places of worship, schools, hospitals, and dwellings. These things can lose their protective status if they are used to make a contribution to the military action. An attacker must not intentionally attack civilians or employ methods or means (weapons or tactics) that would cause excessive collateral civilian casualties. However, a defender has an obligation to separate civilians and civilian objects (either in the defender's country or in an occupied area) from military targets.

These guidelines suggest that data of a medical nature be physically segregated as much as possible from information that can invite hostile targeting. *Complete* physical segregation is not currently feasible due to cost, maintenance, and other considerations. Most AF bases do not completely segregate medical and non-medical traffic because an Air Force base is considered to be a trusted network for medical traffic. Also given the make up of the United States adversaries today will it matter if the data isn't separated? Today's enemies either just don't care if collateral damage occurs or they possess the tools to spin control the damage through control of the media.

Healthcare Insurance Portability* and *Accountability Act (HIPAA)

The LMD must protect the privacy of medical traffic according to Health Insurance Portability and Accountability Act (HIPAA) constraints. HIPAA went into effect on April 14, 2003, is intended to improve the efficiency and effectiveness of the health care system by standardizing electronic data interchange. HIPAA has three main parts: (1) Insurance Portability, (2) Fraud Enforcement (accountability), and (3) Administrative Simplification.

HIPAA requires appropriate administrative, technical, and physical safeguards to protect the privacy of health information. The final Security Rule released in February 2003, contains specific standards for implementing physical and technical safeguards of protected healthcare information. Organizations must comply with the security requirements by the April, 2005 deadline. There are five areas of note- *Facility access controls, workstation use, workstation security, Device and media controls,* and *Access controls* (Services and Rights 2003).

In the area of *facility access controls* healthcare organizations must implement policies and procedures to limit physical access to electronic information systems and the facilities in which they are housed, while ensuring that properly authorized access is allowed. The *workstation use* section stipulates that healthcare organizations implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of workstations that can access electronic protected health information(Services and Rights 2003).

The *workstation security section* requires organizations to implement physical safeguards for all workstations that access electronic protected health information in order to restrict access to authorized users. The *device and media controls* section states organizations must implement policies and procedures that control the acquisition, disposal, and movement of hardware and electronic media containing personal health information.

The final section *access controls* requires organizations to implement unique user identification and emergency access procedures. They are to ensure that protected healthcare information is available to authorized individuals. The healthcare institution must utilize technical safeguards to enable secure access to data(Services and Rights 2003). In addition to accomplishing those tasks HIPAA mandates that healthcare organizations implement *security risk management*. Fundamental to an effective security risk management program is a clear understanding of the organization's exposure to infrastructure vulnerability and an ability to detect and assess threats. Developing detection, response, and control processes to address these areas is a priority.

Security and risk management initiatives often fall short because they rely on manual methods to document infrastructures that are vastly complex and constantly changing.

The Air Force has selected ***OCTAVE*** ® (Operationally Critical Threat, Asset, and Vulnerability Evaluation) to prevent that and ensure HIPAA compliance.

OCTAVE

OCTAVE is a risk based strategic assessment and planning technique for security. OCTAVE is self-directed. Air Force personnel will assume responsibility for setting the organization's security strategy. The technique leverages the personnel's knowledge of the medical facility's security-related practices and processes to capture the current state of security practice within the medical facility.

Standards

Attacks and trends- <u>Reasons to rethink standards</u>

Information technology has become embedded in the daily operations of the US government. Valuable government and business assets, along with critical services, are now at

risk over the Internet and other information infrastructures. Disruption or attacks on the computers and the information systems employed could have devastating consequences. The widespread use of databases threatens the privacy of individuals. Increased use of computers in safety-critical applications, including the storage and processing of medical records data, increases the chance that accidents or attacks on computer systems can cost people their lives(Pethia 2002).

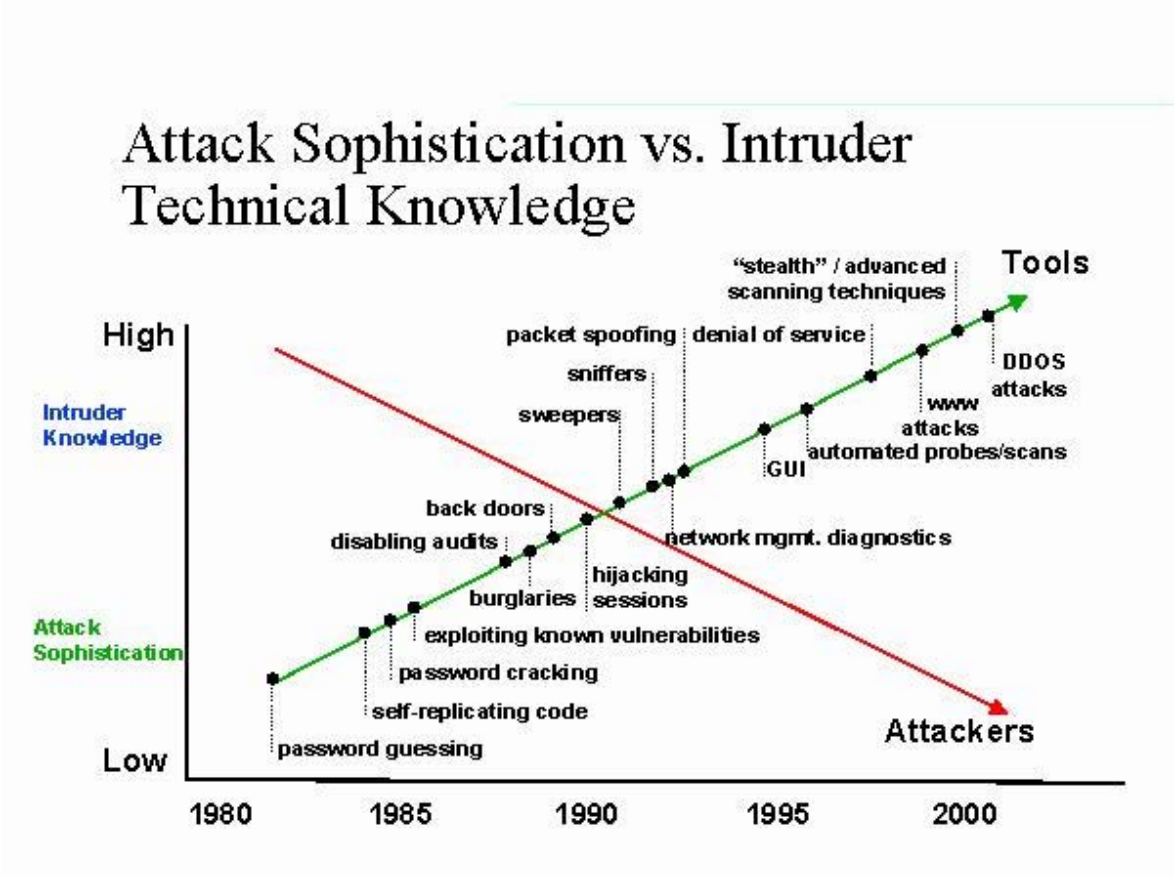

Figure 4- Attack sophistication Vs intruder technical knowledge(Pethia 2001)

"There is little evidence of movement toward improvement in the security of most products; software developers do not devote enough effort to applying lessons learned about the causes of vulnerabilities. We continue to see the same types of vulnerabilities in

newer versions of products that we saw in earlier versions"(Pethia 2002). That is not to say that there isn't new areas intruders find to attack. The Computer Emergency Response Team (CERT) Coordination Center has been tracking intruder activity since1988. CERT has made the following observations over that time. The technical skill and knowledge an intruder needs to possess has diminished (Figure 4). The amount of damage an attack causes has increased dramatically. In addition intruders are gaining leverage through automation and exploiting network interconnections and moving easily through the infrastructure. They are also becoming more skilled at masking their behavior. CERT has also identified the disturbing attack trends noted below in table 2. The trends seen by the CERT/CC indicate that organizations relying on the Internet face significant challenges to ensure that their networks operate safely and that their systems continue to provide critical services even in the face of attack.

Table 2- Attack Trends (Center 2002)

Trends	
Automation	**Level of automation in attack tools continues to increase. Attack tools exploit vulnerabilities as a part of the scanning activity, which increases the speed of propagation**
Increased sophistication of attack tool	**Attack tool signatures are more difficult to discover through analysis and more difficult to detect through signature-based systems such as antivirus software and intrusion detection systems**
Faster Discovery of Vulnerabilities	**Subsequent reviews of existing code for examples of the new vulnerability class often lead, over time, to the discovery of examples in hundreds of different software products. Intruders are often able to discover these exemplars before the vendors are able to correct them.**
Increasing permeability of firewalls	**Technologies are being designed to bypass typical firewall configurations. Some protocols marketed as being "firewall friendly" are, in reality, designed to bypass typical firewall configurations.**
Increasingly asymmetric threat	**With advances in attack technology, a single attacker can relatively easily employ a large number of distributed systems to launch devastating attacks against a single victim. As the automation of deployment and the sophistication of attack tool management both increase, the asymmetric nature of the threat will continue to grow.**
Increasing threat from infrastructure attacks	**They are of increasing concern because of the number of organizations and users on the Internet and their increasing dependency on the Internet to carry out day-to-day business.**

The SANS (SysAdmin, Audit, Network, Security) Institute was established in 1989. It is one of the most valuable sources for information security training and certification in the world. The SANS Institute develops and maintains the largest collection of research documents about various aspects of information security. In addition the institute operates the Internet Storm Center providing alerts to the latest threats and releasing a yearly top 20 list of the most critical internet vulnerabilities. The list contains the ten most commonly exploited vulnerable services in Windows and the ten most commonly exploited elements in UNIX and Linux environments.

Although there are thousands of security incidents each year affecting these operating systems, the overwhelming majority of successful attacks target one or more of these twenty vulnerable services(Institute 2004). Two new additions to the list of particular interest to this research are file sharing and instant messaging (IM). Instant messaging presents a particular challenge to maintaining standards with the Air Force's "Friends and Family Instant Messenger (AFIM)"(Neveu 2005) launched two years ago. AFIM runs through the AF portal and is encrypted. Program content must also adhere to the established messaging guidance presented in AFI 33-119. But is that enough?

According to Richard D. Pethia, former Director of the CERT® Coordination Center (CERT/CC) it isn't. "The second major category of vulnerability includes weaknesses in the management and operational practices of system operators"(Pethia 2003). Factors that can lead to this weakness are lack of, unclear, or poorly enforced organizational security policies and regulations; security roles and responsibilities that are not clearly defined or lack of accountability(Pethia 2003). Poor account management or password management by all users can also aid in developing this vulnerability(Pethia 2003).

The weak operational practices of organizations combined with the advanced technology that attackers now possess resulted in the number of incidents reported to increase to over 137,529 in 2003 and the reported number of vulnerabilities to remain relatively constant over the last three years(see figure 5)(Center 2005). Approximately 90% of all successful intrusions into the Air Force networks come from known vulnerabilities or failure to use sound system protection practices (Butler 2004).

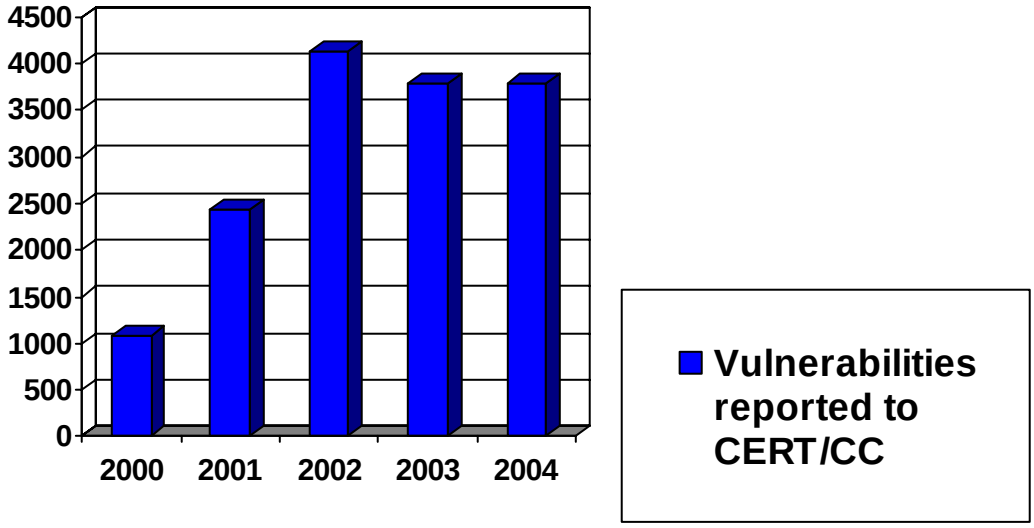

Figure 5- Number of Vulnerabilities reported to CERT/CC.(Center 2005)

Faulty or poor practices as those mentioned above have resulted in the US government computer systems receiving a D + as an overall grade on the 2004 security report card released by the House Government Reform Committee(Vijayan 2005). The report card is issued annually in accordance with the Federal Information Security Management Act (FISMA) of 2002.

The evaluations are compiled by the committee based on criteria established in FISMA (Federal Information Security Management Act) and information provided by each agency's inspector general. The Department of Defense received a overall grade of "D" for the second consecutive year (see table 3)(Vijayan 2005). This doesn't bode well for providing secure, trusted data and the concept of net- centric warfare.

Table 3- FISMA Computer system security grades(Vijayan 2005)

SELECTED AGENCIES	'04	'03
Department of Transportation	A-	D+
Nuclear Regulatory Commission	B+	A
Environmental Protection Agency	B	C
Department of Justice	B-	F
Department of the Interior	C+	F
Department of State	D+	F
Department of the Treasury*	D+	D
Department of Defense*	D	D
NASA	D-	D-
Department of Commerce	F	C-
Department of Energy	F	F
Department of Homeland Security	F	F

*No independent evaluation from the agency's inspector general was submitted in 2003.

Source: House government reform committee

Technology has now advanced to the point where it is easy for attackers to take advantage of vulnerable machines and bind them together to launch high-powered attacks. Intruders can utilize schemes similar to that depicted in figure 6 and focus them onto a single network or system. This could wreck havoc on DoD systems. Secretary Rumsfeld stated: “some adversaries are using those high-tech tools to develop "offensive information operations" that could disrupt military information systems, such as those that enable U.S. troops to engage in "network-centric" warfare with other combat units and foreign allies.

"In a networked environment, information assurance is critical," Rumsfeld said. "Information systems must be protected from attack, and new capabilities for effective information operations must be developed” (Peterson 2002).

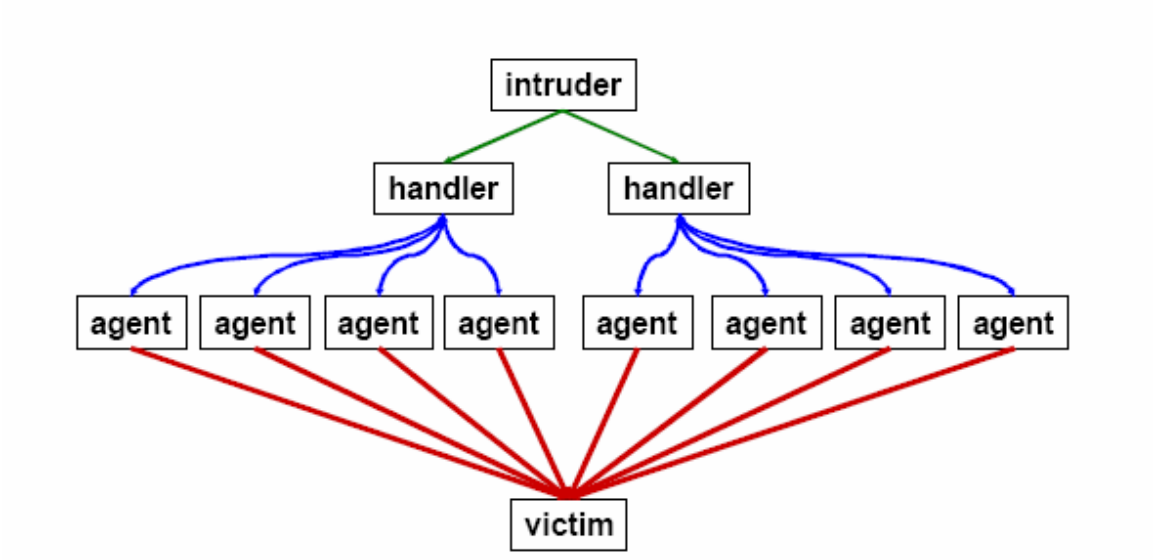

Figure 6 – possible cyber attack scenario.

Software Standardization

The Air Force has reached an agreement with Microsoft to provide enterprise wide software standardization with a single version of its operating system and applications. Mr. John Gilligan, the Air Force CIO stated that “the Air Force endures about one network-based attack per week that successfully exploits new vulnerabilities. There’s some disruption and loss of capability”(Messmer 2004).

To combat this issue security, performance and software feature settings will be designed specifically for the Air Force. They will be based on inputs from the National Security Agency (NSA), Defense Information Systems Agency (DISA) and the Center for Internet Security. Utilizing a single version of the Microsoft products and establishing a centralized distribution for patch management is also expected to lessen the severe associated time delays and costs. Applying software patches is still accomplished manually in the Air Force. Mr. Gilligan advised that “it’s not unusual for patching of vulnerabilities to take months to complete”(Messmer 2004). The agreement with Microsoft is slated to save the Air Force $100 million over the next six years.

Some officials believe that cost savings are often the underlying reason for such agreements. Alan Salisbury, chairman of the Center for National Software Studies, said standardization usually reduces costs. "The name of the game continues to be total cost of operations, which is dominated by maintenance and support," he said. "Fewer configurations equal lower costs (Verton 2004)".

Other analysts believe the agreement with Microsoft is similar to the one the Department of Energy (DoE) reached with Oracle in 2003(Verton 2004). Given the DoE's grade of "F" pertaining to the security of their computer systems (see Table 3) it appears not to be the best model from which the Air Force should follow.

Medical Devices

The Air Force currently operates over 100 medical facilities worldwide. The advances in telemedicine and the medical community's dependency on it greatly increase the possibility for attacks to medical networks. Initiatives such as Composite Health Care System II (CHCS II) and Defense Blood Standard System (DBSS) are guaranteeing that fact(Office 2004). Computerized medical devices are at the forefront of susceptible entry points into the networks. Many of these devices use Off-the-shelf (OTS) software such as Microsoft Windows.

The use of OTS software in a medical device allows the manufacturer to concentrate on the application software needed to run device-specific functions. However, OTS software intended for general purpose computing may not be appropriate for a given specific use in a medical device. The medical device manufacturer using OTS software generally gives up software life cycle control, but still bears the responsibility for the continued safe and effective performance of the medical device(Food and Drug Administration 1999). Mr. Gilligan, the Air Force CIO has acknowledged that medical devices present a unique problem for the Air Force. He is also aware that these devices

face patching issues and are vulnerable to attack left unpatched (Messmer 2004). To address this problem there is currently a separate certification program under which vendors must agree to timely patch updates. The Air Force has started to insist on proper patch management in contracts with device vendors(Messmer 2004).

Currently medical devices fall under the governance of the Food and Drug Administration (FDA). It is the FDA's responsibility to ensure that the vendors complete software updates with their medical devices. The FDA has also issued guidelines to the Air Force that will allow direct installation of software patches in certain circumstances(Messmer 2004).

Summary

This chapter provided background information for the multiple ongoing information technology projects within the Air Force medical community. It discussed the need for *singular direction and a coordinated implementation* to prevent possible shortcomings in information security. After this a discussion concerning the legal implications of integrating the medical networks into the Air Force network was provided. A definition of the Laws of Armed Conflict (LOAC) was given and the possible ramifications of medical data integration were explained. Closing out the chapter was a dialogue covering *standard*s.

This discourse was broken down into three areas. First, the rethinking of the standards currently in place due to cyber attacks and today's trends. Second, the idea of software standardization was covered. Finally, the area of medical devices and the standards used for patch management were discussed.

III. Methodology

Overview

This chapter imparts the approach taken to answer the research and investigative questions, presented in chapter I of this research study. This chapter discusses the qualitative research approach, the case study method and its applicability. Triangulation, designing the case study protocol, conducting the case study, evidence analysis, and research limitations will also be presented. This research project uses a multiple site case study methodology to examine the Air Force's integration of medical information systems and their networks. Focused interviews with medical network support personnel from two Air Force medical facilities provide the data for analysis.

Qualitative Approach

Creswell states that qualitative research is an inquiry process of understanding based on distinct methodological traditions of inquiry that explore a social or human problem. The researcher builds a complex, holistic picture, analyzes words, report detailed views of informants, and conducts the study in a natural setting (Creswell 1998). Simply stated qualitative research may be generally defined as a study, which is conducted in a natural setting where the researcher, uses an instrument of data collection, gathers evidence, analyzes them inductively, focuses on the meaning of participants, and describes a process that is both expressive and persuasive in language.

Qualitative research studies typically serve one or more of the following purposes:

Description - They can reveal the nature of certain situations, settings, processes, relationships, systems or people.

Interpretation - They enable the researcher to (a) gain insights about the nature of particular phenomenon, (b) develop new concepts or theoretical perspectives about the phenomenon, and/or (c) discover that problems exist within the phenomenon.

Verification - They allow a researcher to test the validity of certain assumptions, claims, theories, or generalizations within real-world contexts.

Evaluation - They provide a means through which a researcher can judge the effectiveness of particular policies, practices, or innovations.

Characteristics of good qualitative research

A list of characteristics of a "good" qualitative research is presented below by Creswell(Creswell 1998):

1) Good qualitative research entails rigorous data collection: 2) The researcher collects multiple forms of data, and summarizes them adequately. 3) The study is framed within the assumptions and characteristics of the qualitative approach to research. 4) The researcher identifies studies and employs one or more traditions of inquiry. 5) The researcher starts with a single idea or problem that s/he seeks to understand, not a causal relationship of variables. 6) The study involves detailed methods, a rigorous approach to data collection, data analysis, and report writing. 7) The writing is so persuasive that the reader experiences "being there." 8) Data is analyzed using multiple levels of

abstraction. That is, the researcher's work is presented in a way that moves from particulars to general levels of abstraction. 9) The writing is clear, engaging, and full of unexpected ideas. 10) The story and findings become believable and realistic, accurately reflecting all the complexities that exist in real situation (Creswell 1998).

Case Study Method

Case study is an ideal methodology when a holistic, in-depth investigation is needed (Feagin 1991). It is the best suited research approach for the topic under study. The case study is preferred in examining contemporary events, but only when the relevant behaviors cannot be influenced (Yin 1994).

Case studies are designed to bring out the details from the viewpoint of the participants by using multiple sources of data (Tellis 1997). The literature review for this research provided only some insight into the current status regarding integration of the medical networks in the Air Force. This gives credence to Leedy's assertion that utilizing the case study method may be especially suitable for learning more about a little known or poorly understood situation (Leedy 2001).

Research Design

The decision of which strategy or method to use depends upon three conditions: 1) the type of research question posed, 2) the extent of control an investigator has over the events under study, and 3) the degree of focus on contemporary as opposed to historical events (Yin 1994). Table 4 displays each condition and how they relate to the five major research methods.

Table 4, Strategy for Research Design (Yin, 1994)

Strategy	Form of Research Question	Requires Control of Behavioral Events?	Focuses on Contemporary Events
Experiment	How, why?	Yes	Yes
Survey	Who, what, where, how many, how much?	No	Yes
Archival analysis	Who, what, where, how many, how much?	No	Yes/No
History	How, why?	No	No
Case Study	How, why?	No	Yes

Research Design Components

Yin identified five components of research design that are important for case studies: 1) a study's questions, 2) its propositions, if any, 3) its unit(s) of analysis, 4) the logic linking the data to the propositions, and 5) the criteria for interpreting the findings (Yin 1994). The most important condition for choosing your research strategy is identifying the type of research question. "How" and "why" questions are likely to favor the use of case studies, experiments, or histories. Table 5 lists the four widely used tests and tactics to maintain research design quality throughout the study. How each is performed during this research endeavor is the table.

Design Tests

Construct Validity

Construct validity is especially problematic in case study research. It has been a source of criticism because of potential investigator subjectivity. Yin proposed three remedies to counteract this: using multiple sources of evidence, establishing a chain of

evidence, and having a draft case study report reviewed by key informants (Yin 1994). All three devices are employed in this research. Multiple sources of evidence include multiple cases and focused interview transcripts. A chain of evidence is established through the investigator's receipt of Air Force implementation plans and documentation from the Air Force Surgeon General's office. Key informants working in network support positions at the medical facilities reviewed the case study report and interviewees validated interview transcripts for content and context.

Internal Validity

Internal validity is the degree to which the design of a study allows you to accurately attribute an observation to a specific cause rather than alternative causes. It can be a problem of "inferences". This is only a concern in *causal* (explanatory) case studies (Yin 1994). Internal validity can be strengthened through pattern-matching. Pattern- matching compares an empirical pattern with a predicted one. In explanatory case studies internal validity is enhanced if the patterns are related to the dependent or independent variables. In this research study it will be used to see if there are identifiable areas of concern.

External Validity

External validity deals with knowing whether the results are pertinent beyond the immediate case (Yin, 1994). Can the findings be replicated? Theory in single case studies is one way to address this issue. Another approach to increase external validity is replication logic in multiple case studies. This research examines multiple cases by delving into the integration of medical networks and systems at two Air Force medical facilities. Consequently, replication logic is used to increase external validity.

Reliability

The goal of reliability is to minimize the errors and biases in a study. Reliability deals with demonstrating the operations of a study are repeatable and will provide the same results and conclusions if a succeeding investigator follows the procedures a preceding investigator did in conducting the same case study (Yin 2003) . As it is alluded to in Table 4 the use of a case study protocol and development of a case study database are two strategies for increasing reliability. In this study, a *case study protocol* is used to increase reliability.

Table 5. Case Study Tactics for Four Design Tests (Yin, 1994:33)

Tests	Case Study Tactic	Phase of research in which tactic occurs
Construct validity	• Use multiple sources of evidence	data collection
	• Establish chain of evidence	data collection
	• Have key informants review draft case study report	
Internal validity	• Do pattern-matching	data analysis
	• Do explanation-building	data analysis
	• Address rival explanations	data analysis
	• Use logic models	data analysis
External validity	• Use theory in single-case studies	research design
	• Use replication logic in multiple-case studies	research design
Reliability	• Use case study protocol	data collection
	• Develop case study database	data collection

Triangulation

Stake states that the protocols that are used to ensure accuracy and alternative explanations are called triangulation (Stake 1995). Triangulation is the rationale for using multiple sources of evidence. The Case study approach is known as a triangulated research strategy. Snow and Anderson asserted that triangulation can occur with data, investigators, theories, and even methodologies(Feagin 1991). Denzin identified four types of triangulation: *Data source triangulation*, when the researcher looks for the data to remain the same in different contexts; *Investigator triangulation*, when several investigators examine the same phenomenon; *Theory triangulation*, when investigators with different view points interpret the same results; and *Methodological triangulation*, when one approach is followed by another, to increase confidence in the interpretation (Denzin 1984).

The need for triangulation arises from the ethical need to confirm the validity of the processes. In case studies, this could be done by using multiple sources of data; consideration must be given to construct validity, internal validity, external validity, and reliability (Yin 1989). This research study will use multiple data sources to ensure accuracy and identify possible alternate explanations.

Research Questions

Chapter I introduced the following main research question and investigative questions:

Main Research Question

How is the Air Force addressing the integration of the medical systems and networks under the policy of "One Air Force, One Network" (Ryan 2001)?

Investigative Questions

1. How are medical devices integrated into the medical facilities networks?
2. How does the plan address adherence to HIPPA?
3. Does the integration of the medical information systems into the base networks change the classification of the system under the Laws of Armed Conflict (LOAC)? If so, does this make them more susceptible to attack?
4. Is the implementation of several projects/initiatives increasing the possibility for security vulnerabilities?
5. Is direction being given from a single point or multiple agencies/ commands?
6. Are there other issues that are not addressed under the current plan?

Logic Linking of Data to Propositions

Each proportion directs attention to something that should be examined within the scope of the research. However, not all studies need to have propositions. An exploratory study, rather than having propositions, would have a stated purpose or criteria on which the success will be judged.

Research Propositions and Model

1. Research will identify the issues that the Air Force needs to be concerned with when integrating the medical networks and systems

2. Research will identify sources of concern with integrating the medical networks and systems.

3. Research will show advantages and disadvantages of integrating the medical systems and networks into the *one Air force, one network*

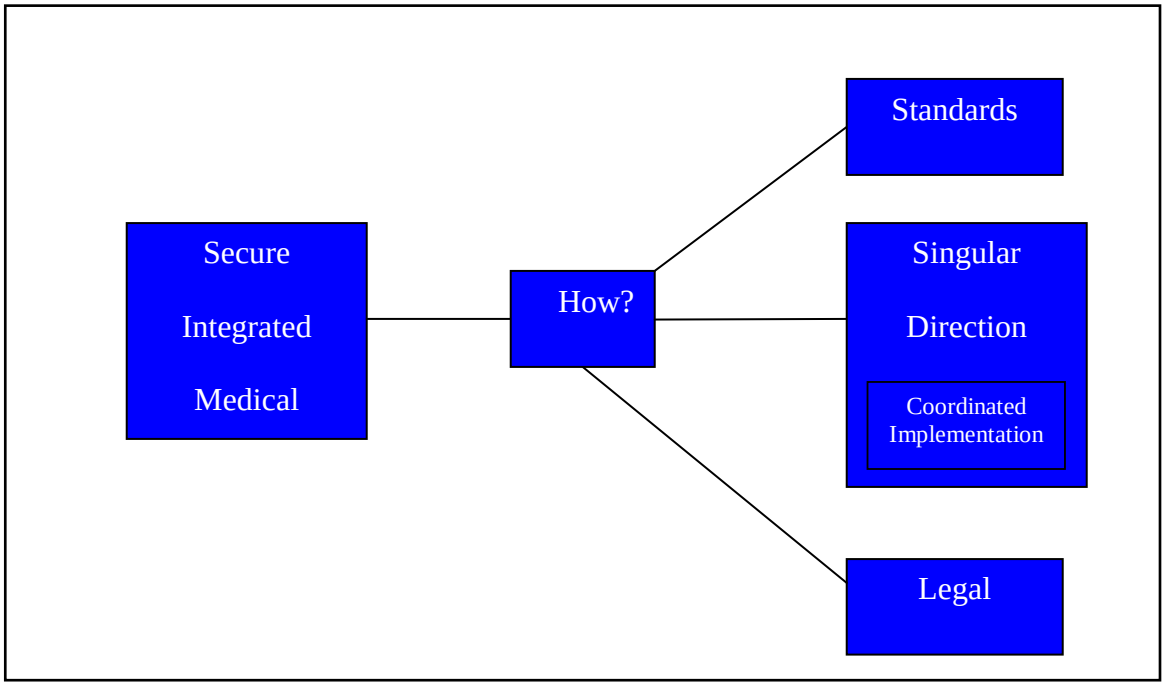

Figure 7- Research model

Research Procedures

This section illustrates the procedures used to answer each research question. The answer to the main research question is inferred by reviewing answers to each of the investigative questions and the literature review.

The table below identifies how each research question is addressed. Interview questions are listed later in this chapter under the Data Collection section.

Table 6- Research question addressing.

Investigative Question	Method Addressed
1	Answered by interview questions 3,4,5,6,7
2	Answered by interview question 6 & Literature review
3	Answered by interview question 4 & Literature review
4	Answered by interview questions 8 -14
5	Answered by interview questions 2, 8-10,12
6	Answered by interview questions 1, 15

Unit of Analysis

The unit of analysis defines what the case is. It is a critical factor in the case study. Case studies tend to be selective, focusing on one or two issues that are fundamental to understanding the system being examined. Linking the data to propositions and the criteria for interpreting the findings are the least developed aspects in case studies (Yin 1994). The unit of analysis for this research study is the medical Networks, Systems, and devices at each site.

Criteria for Interpreting Results

"Data analysis consists of examining, categorizing, tabulating, or otherwise recombining the evidence to address the initial propositions of a study" (Yin 1994). The

analysis of case study is one of the least developed aspects of the case study methodology (Yin 2003). Yin stated that every investigation should have a general analytic strategy, so as to guide the decision regarding what will be analyzed and for what reason (Yin 1994).

The strategy will help you to treat the evidence fairly, produce compelling analytic conclusions, and rule out alternative interpretations (Yin 2003). In general, the analysis will rely on the theoretical propositions that led to the case study. The specific analytic techniques that will be employed for this research are: *pattern-matching*, theoretic propositions, and *cross-case synthesis*.

The theoretic propositions: issues that the Air Force needs to be concerned with when integrating the medical networks and systems, sources of concern, advantages and disadvantages of integrating the medical systems and networks into the *one Air force, one network* make up the general analytic strategy. If theoretical propositions are not present, then the researcher could consider developing a descriptive framework around which the case study is organized (Tellis 1997).

Conducting the Case Study

According to Yin *preparing for data collection* is just as important as the *data collection* (Yin 2003). Both areas are detailed below.

Preparing for Data Collection

Preparing for data collection includes the skills of the investigator, the training and preparation for the specific case study, the case study protocol development, the

screening of candidate case studies, and the conduct of a pilot case study (Yin 2003). Each subsection is discussed in further detail below.

Skills of the Investigator

Many people choose to use the case study method because they believe it is easy. This is completely inaccurate. Due to the lack of an established routine (unlike most of the methodologies) the case study is actually much more tasking on your person (Yin 2003). There aren't any tests that will distinguish whether or not a person will make a good case study investigator, but the table below contains commonly required skills that will greatly aid in their endeavor.

Table 7, Core Case Study Investigator skills (Yin 2003)

Question Asking	Case studies require the ability to ask good questions *during* data collection, not just before and after.
Listening	The investigator should be completely open and not trapped by ideologies or preconceptions.
Adaptiveness and Flexibility	Remember the original purpose of the study, but be willing to adapt procedures or plans if unanticipated events occur.
Grasp of Issues being studied	Understand the purpose of the case. Without that the investigator could miss important clues and would not know when a deviation was acceptable or desirable.
Lack of Bias	Investigators must guard against substantiating a preconceived position.

Case Study training

The goal of the training is to have all participants understand the fundamental ideas, language, and issues germane to the study (Yin 2003). Each investigator should

know why the study is being undertaken, what evidence is being sought, what variations can be anticipated, and what would constitute supportive or contrary evidence for any given proposition (Yin 2003).

Designing the Case Study Protocol

A case study protocol contains procedures and general rules that should be followed in using the data collection instrument. It is to be created prior to the data collection phase. It is essential in a multiple-case study, and desirable in a single-case study. Yin presented the design protocol as a major component in asserting the reliability of the case study research. A typical protocol should have the following sections:

- An overview of the case study project -objectives, issues, topics being investigated
- Field procedures -credentials and access to sites, sources of information, and procedural reminders
- Case study questions -specific questions that the investigator must keep in mind during data collection
- A guide for case study report (outline, format for the narrative) (Yin 2003).

Each element as it pertains to the case under study is specified in greater detail below.

Overview of the Case Study Project

The overview contains background information and issues being investigated as outlined earlier in this chapter and chapter 1. It should also contain relevant readings covering those issues.

Field Procedures

As mentioned above these items need to emphasize the major tasks in collecting data for the case study(Yin 2003). Access to Site 1 medical network support personnel was dictated by their work schedule and the Operational Readiness Inspection (ORI) under way. Interview sessions had to be rescheduled on one occassion. Interview sessions with Site 2 network support staff was put onhold until personnel returned from leave. The session times were also dictated by the availabilty of a conference room in which to conduct them.

The case study protocol is important for two reasons. First, it keeps the investigator targeted on the subject of the case study. Second, preparing the protocol forces the researcher to anticipate some problems (Yin 2003).

Case Study Questions

Case study questions are posed to the investigator, and must serve to remind that person of the data to be collected and its possible sources. They are the heart of this protocol. The set consists of level 1 – questions asked of specific interviewees and level 2 – questions asked of the individual case (Yin 2003). The interview questions are listed later in this chapter in the Data Collection.

Case Study Report Guide

The guide for the case study report is often omitted from case study plans, since investigators view the reporting phase as being far in the future (Tellis 1997). Yin proposed that the report be planned at the start (Yin 1994). The reason for the absence of a fixed reporting format is that each case study is unique. The data collection, research questions and indeed the unit of analysis cannot be placed into a fixed mold as in experimental research (Tellis 1997). Since case studies do not have a widely accepted reporting format - the experience of the investigator is a key factor in determining the format of the final product.

Screening Case Study Nominations

Two factors played a major role in determining which locations of those 90 slated for integration would serve as the case study. These were geographical location and size of the Air Force installation and the medical facility that supported the base community. Site 1 was chosen due to its proximity and classification as a large medical facility supporting a large active duty and retired personnel community. Site 2 was selected due its classification as medium sized medical facility and also supporting a large active duty and retired personnel population.

Pilot Case Study

Although the researcher was located at one of the selected sites no pilot study was performed due to time constraints. Therefore, this research is meant to be exploratory

and further research will be warranted. This study is meant to be the basis from which further research can springboard from.

Data Collection

Once the protocol has been developed and tested, it puts the research project into the second phase – its execution. In this phase the primary activity is that of data collection. The protocol described above addresses the types of evidence that are available in the case organization. In this case study, data collection is treated as a design issue that will enhance the construct and internal validity of the study, as well as the external validity and reliability(Yin 1994). Table 8 contains six sources of evidence with both strengths and weaknesses. No single source has a complete advantage over the others; rather, they might be complementary and could be used in tandem. Thus a case study should use as many sources as are relevant to the study (Yin 2003). This research will deal the first three- documents, archival documents, and interviews.

Documents could be letters, memoranda, agendas, administrative documents, newspaper articles, or any document that is germane to the investigation. In the interest of triangulation of evidence, the documents serve to corroborate the evidence from other sources. Documents are also useful for making inferences about events, but this can produce false leads. This has resulted in criticism of case study research. *Archival documents* can be service records, organizational records, survey data, and other such records. They often take the form of computer files and records.

The investigator has to be careful in evaluating the accuracy of the records before using them. Even if the records are quantitative, they might still not be accurate. Large

quantities don't mean the source evidence is necessarily accurate (Yin 2003). *Interviews* are one of the most important sources of case study information. There are several forms of interviews that are possible: open-ended, focused, and structured or survey.

In an open-ended interview, key respondents are asked to comment about certain events. They may propose solutions or provide insight into events. They may also corroborate evidence obtained from other sources. The researcher must avoid becoming dependent on a single informant, and seek the same data from other sources to verify its authenticity. Key informants are often critical to the success of the case study (Yin 2003).

The focused interview is used in a situation where the respondent is interviewed for a short period of time, usually answering set questions developed from the case study protocol. This technique is often used to confirm data collected from another source (Yin 2003). The structured interview is similar to a survey. The questions are detailed and developed in advance, much as they are in a survey.

Direct observation in a case study occurs when the investigator makes a site visit to gather data. The observations could be formal or casual activities, but the reliability of the observation is the main concern. Using multiple observers is one way to increase reliability. Participant observation is a unique mode of observation in which the researcher may actually participate in the events being studied (Tellis 1997).

Table 8. Six Sources of Evidence: Strengths and Weaknesses (Yin 2003)

Source of Evidence	Strengths	Weaknesses
Documentation	• stable - repeated review • unobtrusive - exist prior to case study • exact - names etc. • broad coverage - extended time span	• retrievability - difficult • biased selectivity • reporting bias - reflects author bias • access - may be blocked
Archival Records	• Same as above • precise and quantitative	• Same as above • privacy might inhibit access
Interviews	• targeted - focuses on case study topic • insightful - provides perceived causal inferences	• bias due to poor questions • response bias • incomplete recollection • reflexivity - interviewee expresses what interviewer wants to hear
Direct Observation	• reality - covers events in real time • contextual - covers event context	• time-consuming • selectivity - might miss facts • reflexivity - observer's presence might cause change • cost - observers need time
Participant Observation	• Same as above • insightful into interpersonal behavior	• Same as above • bias due to investigator's actions
Physical Artifacts	• insightful into cultural features • insightful into technical operations	• selectivity • availability

The main concern is the potential bias of the researcher as an active participant. While the information may not be available in any other way, the drawbacks should be carefully

considered by the researcher. Physical artifacts could be any physical evidence that might be gathered during a site visit. That might include tools, art works, notebooks, computer output, and other such physical evidence**.** This exploratory case study uses documentation exclusively pertaining to the integration of medical information networks and systems. A hybrid of focused and open ended interviews was conducted with medical network support personnel. Subjects had an average of six years of practical experience in the telecommunication field.

The following interview questions address the research questions and propositions:

1. How is your shop set up?
2. Where do you take direction from?
3. How are the networks in the hospital configured?
4. Are computerized devices currently logically separated from the rest of the network?

5. Are there plans to do that?

6. Are imaging, billing, and patient records integrated?

7. Are there currently any back door connections outside the network?

8. Are you aware of any AF initiatives?

9. Timeline for completion?

10. Are the systems /circuits currently accredited?

11. If so, what does the process entail?

12. Are medical devices still under the mgt of vendors and fall subject to existing FDA guidelines & policies?

13. How are security patches implemented?

14. How are security incidents/updates reported?

15. Other issues?

Question Development

Table 9- Question development analysis

Interview Question	Supporting Investigative Question	Proposition Supported
1	6	1
2	5	1
3	1	3,1
4	1	3,1
5	1	3,1
6	1,2	3,1,2
7	1	3,1,2
8	4,5	1,2
9	4,5	2
10	4,5	1,2,3
11	4	1,2,3
12	4,5	3,1
13	4	1,2
14	4	1,2
15	6	1,2

Pre-interview Procedures

The nature of the topic restricted the pool of potential interviewees to individuals working in the either medical network support field. Candidates also had to have knowledge of ongoing projects pertaining to the integration of the medical information systems. Medical network support leadership aided in identifying qualified individuals for this study. In qualitative research, purposeful selection of participants or sites provides the best opportunity for the researcher to address the research questions (Creswell, 2003).

To reduce any bias, interviewees were informed of the study's goal to merely assess, not judge the integration of medical information systems, organizations, or personnel involved. Participation in this study is voluntary and anonymous. Interview questions were provided to participants at least 24 hours in advance. Each participant provided an email address to facilitate review and approval of their responses. Any requested modifications received via the email feedback loop were accomplished before any answers were analyzed. Participants were offered a copy of the final report.

Data Analysis

The data analysis can be either a *holistic analysis* of the entire case or an *embedded analysis* of a specific aspect of the case (Creswell 1998). As stated earlier in this chapter this research study utilizes theoretical propositions for the general analytic strategy and pattern matching and cross-case synthesis as the specific analytical techniques.

Theoretical Propositions

This is the first and most preferred strategy (Yin 2003). The propositions introduced in Chapter 1 and earlier in this chapter were based on the original objectives and design of the case study protocol. They shaped the data collection plan and would have given priorities to relevant analytic strategies. This study's purpose is to assess the Air Force' integration plan for the medical information networks and systems. The theoretical propositions directed the exploration of this endeavor with a focus on key issues and sources of concern.

Pattern Matching

Pattern-matching is considered as one of the most desirable strategies for analysis. This technique compares an empirically based pattern with a predicted one. If the patterns match, the internal reliability of the study is enhanced (Trochim 1989). This study compares patterns from multiple cases, open-ended interviews, and focused interviews. The details of the comparison are included in chapter IV.

Research Limitations

As mentioned in chapter I there are several limiting factors for this research study. First, the number of medical facilities scheduled for integration. The Air Force's Medical Information Technology Transition (MITT) plan has directed this work to be completed at 90 Air Force locations worldwide. This research studies medical facilities at only two locations in detail to assess the Air Force initiative and draw a correlation to the rest of medical facilities. . Second, little research exists on the current Air Force projects. As a result, there is not much to build upon. Third, people tend not to speak negatively. Even

if the facts and conditions warrant it. Time represents the final major limitation for study. The importance and difficulty of this study command more time than this effort can provide. This study aims to establish the basis for additional research.

Chapter Summary

This chapter presented the process used to answer the research questions presented in Chapter I of this research study. This chapter discussed the qualitative research approach, characteristics of good qualitative research, and the case study method, case study research design, conducting the case study, preparing for data collection, data collection, data analysis, and research limitations.

IV. Results

Overview

This chapter provides the results of the research methodology outlined in chapter III and the model shown here in Figure 8.

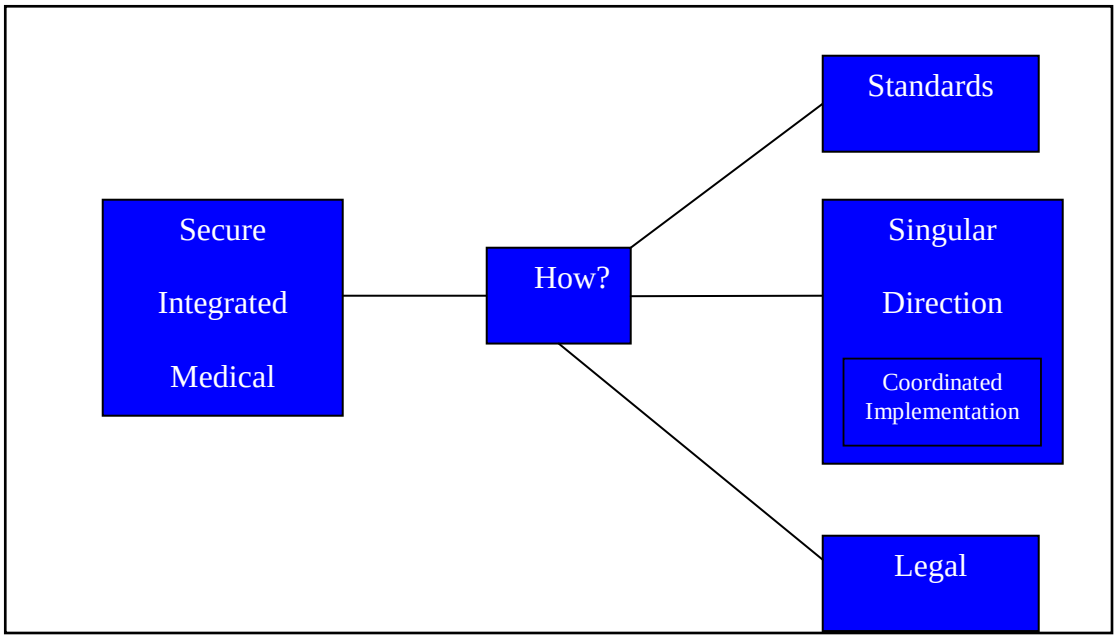

Figure 8, research Model

Figure 8 depicts the proposed model for how a secure integration of the medical networks can be achieved. The resultant data from this study supports the claims of the model. The results are based on focused interviews of medical network support personnel and a detailed literature review. This chapter is arranged into four sections. First, a description of the sites used in this research is provided. Two sites were used in this study to address the six investigative questions and answer the main research question. Second, an overview of the interview data is presented. Third, each

investigative question is answered and summarized. Lastly, the main research question is addressed.

Site Descriptions

This section provides a description of the two sites chosen for this research project. The locations were selected due to their designation in the Medical Information Technology Transition (MITT Last mile Design (LMD) System Design Document (SDD)(Headquarters Electronics Systems Center 2004). Both sites are located within the continental United States, but operationally support different Air Force major commands. Another factor in their selection was how they are representative of the entire Air Force medical community. Site 1 was chosen due its being a large medical facility and supporting network. Site 2 is representative of a medium sized medical facility and supporting network. Information reflected in this section is based on focused interviews with network support personnel. All but one Site 1 interviews were completed face to face. Data from site 2 was gathered via telephone interviews.

Site 1

Site 1 has a Gigabit uplink to the base LAN via vendor *C* switch. Site 1 has redundant connectivity from vendor *A* core switches to their server farm (file/print/application/ database). Both switches have a 100 MB Ethernet connection to each server. Multimode fiber, CAT 5 cable, a 100 Megabit FFDI ring, and an Asynchronous Transfer Mode (ATM) connection to vendor *B* switches form the backbone within the medical facility. There are 100 MB connections to the CHCS core nodes, clinical information servers, and vendor *D* Picture Archiving and Communications

System (PACS). In addition Site 1 has 10MB Ethernet links to the legacy PACS and CHCS network.

Site 1 also has a partnership with a local hospital. The partnership allows Site 1 to utilize the hospital's staff to read digital images. To facilitate this ability there is a Gigabit connection from Site 1's PAC across the base Metropolitan Area Network (MAN) and through the firewall to a workstation at the local hospital. Four personnel from Site 1 were interviewed for this research project.

Site 2

Site 2 also has a Gigabit uplink to the base LAN via vendor *X* switch. Site 2 has redundant connectivity from vendor *Y* core switches to their server farm (file/print/application/ database). The switches have multiple fiber connections for redundancy. Fiber optic connections to vendor *B* switches form the backbone within the medical facility. The CHCS network is completely separate and maintained by contractors. Site 2 also has teamed with local hospitals to provide reading of digital imagery after hours. Three personnel from Site 2 were interviewed via telephone for this research study.

Interview Data

Site 1network support management identified personnel that would provide the necessary insight and knowledge for this research study. The personnel identified by the superintendent have been supporting the medical facility and its network for an average of five years. The interviews were conducted on an individual basis. All but one was accomplished face to face. Face to face interviews were not possible due to work loads at

Site 2. Two interviews were accomplished with Site 2 personnel. All key informants possessed at least 4 years experience supporting the medical community.

Investigative Questions

This section addresses each of the six investigative questions separately. Evidence in the form of interview data, supporting literature, and a summary of the convergent information is presented. Refer back to table six in chapter III for mapping of Investigative questions and interview questions.

Investigative Question one

- How are medical devices integrated into the medical facilities networks?

The results of this study indicate the manner in which medical devices are handled is different throughout the Air Force. Factors that determine this include the services the medical facility offer and the physical make up of the network itself. Although Collmann(Collmann 2003) suggests that logically separating the devices will aid in mitigating the risk of their vulnerabilities it was not accomplished at either location.

Interview question three

- How are the networks in the hospital configured?

The responses to this question indicate that there isn't any standard configuration. The network configuration is primarily based upon the medical facility's mission. The Site 1 personnel stated that there is an additional connection to a local hospital. This connection was due to the personnel constraints at Site 1. In addition, Site 1 interviewees

responded that there are often occasions in which medical personnel connect to the network from home. This connection permits medical staff to access digital imagery. The staff then can make a determination if the situation warrants them driving to the facility to treat the patient. After a further discussion of their responses, two of the interviewees indicated that initially the doctors were buying *business cla*ss internet service to obtain static IP addresses and establishing & maintaining the remote connections through the use of a Remote Access Servers (RAS). However, this changed after the base communication squadron forced them to change to a Virtual Private Network (VPN). This attempt was unsuccessful due to the PAC not working properly when using a Proxy. The communication squadron was forced to allow the connection to "punch through" the firewall to get it to work.

The initial Site 2 personnel responses also indicated that there wasn't a standard configuration at that location. The difference at Site 2 was that the Combined HealthCare System (CHCS) is separate. It doesn't connect into the medical facility's network. Site 2 also has an established partnership with local hospitals to provide after hours care. Site 2 has two T-1 connections to local university medical centers.

Interview questions four & five

- Are computerized devices currently logically separated from the rest of the network?
- If not, are there plans to do that?

The responses to these questions indicate that there is no uniformity in which medical devices are connected. Two interviewees at Site 1 indicated that although the devices are physically connected to the network; the devices are logically separated. The other

interviewee stated that “all DITSCAP approved or grandfathered medical equipment is currently connected to the network similar to any PC on the network. New un-approved medical equipment that we are testing has been placed in a separate or *private* segment of the network while it’s being evaluated. This is done on a case by case basis. This *private* segment of the network is created by placing the medical devices behind a router, and then applying Access Control Lists (ACL) preventing traffic flow to essential traffic in and out of the separated network”.

The interviewee further added that “they hope to develop a better enterprise solution for this issue by placing a true firewall inside the medical center that we can put all of the medical devices we control behind, and create a separate "medical network" which would not have the same requirements when it comes to security patching”. The interviewee also stated that “patching is something they have a very hard time staying current with”.

The initial Site 2 personnel responded that they didn’t work with the medical devices, nor did they have any knowledge of how they were connected. The interviewees’ responses indicated that the devices were treated more like ordinary hospital equipment. The devices were maintained by a different flight within the hospital. Results from a subsequent interview with personnel from that flight indicate that Site 2 has limited medical devices within the facility and that they are both logically and physically separate from the facility’s main network. The individual stated that only laboratory equipment connected into the Composite Health Care System (CHCS).

Interview question six

- Are imaging, billing, and patient records integrated?

Site 1 interviewees advised that yes imaging, billing, and patient information is integrated in the CHCS system. One interviewee further added that information is intended for demographics only. The information isn't transmitted outside the facility. Site 2 personnel responded that the data is also integrated at their location. However, it is stored in servers used strictly for clinical information within the facility. It doesn't enter the CHCS network.

Interview question seven

- Are there currently any back door connections outside the network?

Site 1 personnel advised the Combat Information Transport System (CITS) team had performed a network analysis and assessment approximately six to eight months ago and terminated the two "back door" connections that had previously existed. This was done in preparation for implementing the Medical Information Technology Transition (MITT) Last mile Design (LMD).

Site two personnel disagreed amongst themselves. One interviewee stated that there are no back door connections. That individual didn't mention the remote connectivity to the local hospitals either. The other two interviewees responded that there were direct connections to the local hospitals. These connections didn't transverse the base firewall or LAN. One interviewee added further that there were "1 or 2" dial up

connections to companies in support of other functions of the Medical Treatment Facility (MTF) and its daily operations.

Investigative question one results summary

Convergent evidence is provided to support the belief that the integration of medical devices in Air Force facilities is not standardized. The devices are integrated based upon the facilities own mission and the services they provide. There is also evidence to suggest that although the medical devices are physically or logically separated they are still vulnerable to possible attacks due to remote connections and patch management.

Investigative Question two

- How does the plan address adherence to HIPPA?

With the exception of two individuals at Site 1 none of the other interviewees were aware of the Air Force's plan to integrate the medical information networks. The initiatives under way at both locations to adhere to Health Insurance Portability and Accountability Act (HIPAA) were separate from the MITT design. Positions were created at both locations to ensure compliance.

Interview question six

- Are imaging, billing, and patient records integrated?

Site 1and Site 2 interviewees advised that imaging, billing, and patient information is integrated. The information isn't transmitted outside the medical facilities.

A Site 1 interviewee responded that DoD has mandated that all services implement some sort of risk assessment and analysis system to ensure laws mandated in the security portion of HIPAA are met. The interviewee stated that the Air Force has chosen OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) (Dorofee 2001) to strategically assess and plan security techniques for HIPAA compliance. The interviewee further stated that the OCTAVE was implemented in June 2004 and that "Site 1 was now completing the baseline security and gap analysis".

Literature Review

HIPAA mandates that healthcare facilities implement physical safeguards for systems and workstations that access electronic protected health information (PHI) in order to restrict access to authorized users. In addition the medical treatment facility (MTF) must also utilize technical safeguards to enable secure access to data(Services and Rights 2003). As stated in chapter II MTFs must implement security risk management to develop threat control, detection, and response processes.

Investigative question two results summary

Convergent evidence is provided to suggest that the MITT (Medical Information Technology Transition) Last mile Design (LMD) doesn't take HIPAA into account. The MITT design document does state HIPAA as being a constraint, but doesn't offer any plans or methods to deal with the issue. The MITT LMD doesn't mention the required implementation of security risk management at MTFs either. The interviewee Responses to this question do provide insight on how the Air Force is attempting to comply with

HIPAA. The creation of HIPAA positions at both sites is a start. The data does suggest that theses the personnel deal more with HIPAA complaints rather than HIPAA compliance. The absence of security risk management and remote connections at both sites do provide a means in which the integrity of the PHI is at jeopardy.

Investigative Question three

- Does the integration of the medical information systems into the base networks change the classification of the system under the Laws of Armed Conflict (LOAC)? If so, does this make them more susceptible to attack?

The interviewee responses from both locations were clouded with uncertainty. All personnel weren't sure of just how the medical systems were being integrated into the base networks. Most of the interviewees also believed that the vulnerability for attack existed whether or not the medical systems were connected to the base.

Interview question four

- Are computerized devices currently logically separated from the rest of the network?

The data suggests that there is no standardization for medical device connectivity. Interviewees were divergent in their answers. Believes differed as to if the devices were physically and or logically separated from the rest of the network. The data further suggests that there is no segregation of medical information from the rest of daily operational data at Site 1 or Site 2.

Literature Review

Chapter II identified that the LOAC are broken down into two types of law- customary *international law* and *treaty law*. Treaty law is concerned mainly with the means and methods of warfare (e.g., lawful and unlawful weapons, targeting) (Strand 2004). LOAC also stipulates that attacks must be limited to military objectives (Strand 2004).

LOAC defines *military* objectives are objects which by their nature, location, purpose, or use make an effective contribution to military action and whose total or partial destruction, capture, or neutralization, in the circumstances ruling at the time, offers a definite military advantage(Strand 2004). Examples of this include troops, bases, supplies, lines of communications, and headquarters.

Hospitals are *civilian* objects. Civilian objects are awarded special protection. However, they can lose their protective status if they are used to make a contribution to the military action. This interpretation of LOAC suggests that medical data be physically and logically separated to prevent a hospital's loss of *civilian* object status.

These guidelines suggest that data of a medical nature be physically segregated as much as possible from information that can invite hostile targeting. *Complete* physical segregation is not currently feasible due to cost, maintenance, and other considerations. Most AF bases do not completely segregate medical and non-medical traffic because an Air Force base is considered to be a trusted network for medical traffic. Also given the make up of the United States adversaries today will it matter if the data isn't separated? Today's enemies either just don't care if collateral damage occurs or they possess the tools to spin control the damage through control of the media.

Investigative question three results summary

Complete physical segregation is not currently feasible due to cost, maintenance, and other considerations. Most AF bases do not completely segregate medical and non-medical traffic because Air Force leadership is under the belief that Air Force bases are a trusted network. MITT will logically integrate medical data and physically connect medical systems into the Air Force network. Air Force leadership believes that the integration of the medical networks won't matter. They believe that the hospitals will still be afforded the status of civilian object under the LOAC. The LOAC only apply to nations that wish to abide by them and have signed treaties to state they will. Today's enemies of the United States don't recognize LOAC nor do they abide by them. They either just don't care if collateral damage occurs or they possess the tools to spin control the damage through control of the media.

Investigative Question four

- Is the implementation of several projects/initiatives increasing the possibility for security vulnerabilities?

During the course of this research multiple initiatives were discovered by the researcher to be underway. The interviewees were aware of only one or two and they weren't the same ones.

Interview question eight & nine

- Are you aware of any AF initiatives?
- Timeline for completion?

Table 10 depicts the responses the interviewees gave when asked interview questions eight and nine. Interviewees 1-4 are from Site 1. Interviewees 5-7 are from Site 2. Interviewee 1 stated that MITT had been completed, where as interviewees 2 & 3 stated that they had been informed that project had slipped six months. They were informed that MITT wouldn't be implemented at Site1 until sometime in 2005.

Table 10- Initiative awareness of Site personnel

Initiative	Interviewee 1	Interviewee 2	Interviewee 3	Interviewee 4	Interviewee 5	Interviewee 6	Interviewee 7
MITT	**X***	**X**	**X**		**X***		
Block 30	**X**						
CHCS II	**X**		**X***	**X**	**X***		**X**
Local project					**X**		
Majcom project							**X**
OCTAVE				**X**			

They were informed that MITT wouldn't be implemented at Site1 until sometime in 2005. Interviewees 6 & 7 responded that they were unaware of the MITT

implementation at Site 2. Interviewee 5 was aware of MITT and stated the service level agreement (SLA) had yet to be signed. Only interviewee 1 was aware of the CITS (Combat Information Transport System) Block 30 initiative. He responded that he didn't know the timeline for completion though. Only four interviewees were aware of the CHCS II upgrade. Interview 3 thought it had been halted due to performance issues. Interviewee 5 just knew it was ongoing, but no status as he didn't have anything to do with it. Personnel from site 2 also advised of other initiatives. One was a base undertaking. The interviewee (number 5) stated "that commander wanted this (the project) and it was their responsibility to implement it". Interviewee 7 stated that the major command was possibly implementing a PACS system within the year.

Interview questions ten & eleven

- Are the systems /circuits currently accredited?
- If so, what does the process entail?

Responses from both Site 1& 2 indicated that the medical systems and networks were accredited. One interviewee from Site 1 responded that if the device wasn't accredited or had a waiver it wasn't connected to the network.

Interviewees included the individuals who are responsible for ensuring the accreditation process is completed. One interviewee stated that the systems were accredited in conformance with the DoD Information Technology Security Certification & Accreditation Process (DITSCAP). DITSCAP covers the physical, personnel, administrative, information, and information systems areas of the system under question.

The security personnel gather all pertinent information and submit it to the proper authorities.

Interview question twelve

- Are medical devices still under the mgt of vendors and fall subject to existing FDA guidelines & policies?

Personnel responses from both locations indicate the FDA is still regulating the patch management and software updates for medical devices. Site 1 interviewees responded that they were aware of an initiative by the Air force to ask the FDA to allow Air Force personnel to implement patch updates in certain situations.

Interview question thirteen

- How are security patches implemented?

Site 2 personnel responded that they only had responsibility for a limited number of devices; mainly laboratory equipment. These devices are patched in accordance with FDA and Air Force guidelines. Site 1 personnel indicated that there were devices connected to the network which currently have approved waivers permitting the devices not to have the latest patches installed on them. They also stated that there are devices which have the latest patches and are updated in accordance with FDA and Air Force guidelines.

Interview question fourteen

- How are security incidents/updates reported?

Site 1and 2 interviewees responded that incidents or updates were reported as follows: operator/analyst to security manager to supporting Communication squadron

personnel to major command Network Operations Center (NOC) to Air force Network Operations center (AFNOC).

Investigative question four results summary

The responses indicate that there are holes in the approaches taken at both Site 1 and Site 2. This suggests that multiple project or initiatives increase the possibility for security vulnerabilities. It was suggested by interviewees from both sites that often multiple projects, either occurring simultaneously or in concurrence tend to leave out important aspects (such as information security). They believed this was due to time constraints or more often lack of funding.

Investigative Question five

- Is direction being given from a single point or multiple agencies/ commands?

Interview question two

- Where do you take direction from?

Site 1 personnel all responded that they received direction from a singular point; however they pointed out that the medical facility received funding from another organization. Interviewees from site 2 indicated that they also receive direction from a single point- on the surface. A Site 2 interviewee responded that they still have to support the local commander and sometimes that is a different direction from the normal chain of command

Interview questions eight & nine

- Are you aware of any AF initiatives?
- Timeline for completion?

As shown in table 10 above interviewee responses were diverse. Responses indicate that there is conflicting direction due to multiple sources.

Interview question ten

- Are the systems /circuits currently accredited?

Their initial configuration(s) has been verified and approved by the Designated Approving Authority (DAA). This is part of the DITSCAP accreditation process.

Interview question twelve

- Are medical devices still under the mgt of vendors and fall subject to existing FDA guidelines & policies?

Responses from interviewees indicate that medical device patch management is still the responsibility of the equipment manufacturer. The Food and Drug Administration (FDA) provides guidance for patch updates of these devices. Site 1 personnel responded that there devices which have been granted waivers present on the network.

Investigative question five results summary

There is convergent evidence that suggests there are often multiple lines of authority and direction provided from them. Implementation for today's projects and

instruction is sometimes being left open for personal interpretation or agendas. Evidence suggests that there is conflicting direction from multiple sources.

Investigative Question six

- Are there other issues that are not addressed under the current plan?

The interviewee's responses to the other investigative questions have identified the areas that are lacking. There are issues such as HIPAA and LOAC that are mentioned, but not thought through as to how they are going to be dealt with. There is no mention of how these issues affect implementation of the medical networks or operationally the medical community.

Interview question fifteen

- Other issues?

Investigative question six results summary

The interviewees did not provide any other issues than those already identified by the previous interview questions.

Main Research Question

- How is the Air Force addressing the integration of the medical systems and networks under the policy of "One Air Force, One Network?

The Air Force is attempting to integrate the medical systems and networks mainly by looking at the technical aspects of the undertaking. The results of the six investigative questions support this submission. Existing literature shows that the other

aspects mentioned in this research need to be addressed. The main research question is answered by the results of the six investigative questions.

To address investigative question one, interview data established the manner in which medical devices are handled is different throughout the Air Force. There is no standardization. It was also identified that although the medical devices are physically or logically separated they are still vulnerable to possible attacks due to remote connections and patch management.

To address investigative question two, interview data and existing literature identified the MITT (Medical Information Technology Transition) Last mile Design (LMD) doesn't take HIPAA into account. Although mentioned it doesn't provide direction or even alternate plans or methods to deal with HIPAA compliance. Interview data did identify how the Air Force is attempting to comply with HIPAA, however the absence of security risk management and remote connections at both sites do provide a means in which the integrity of the Protected Health Information (PHI) is at jeopardy.

To address investigative question three, interview data and existing literature identified that Air Force leadership believes that the integration of the medical networks won't change the classification of the systems. They believe that the hospitals will still be afforded the status they previously held under the Laws of Armed Conflict (LOAC). To address investigative question four, interview data identified that there often are holes in the approaches taken. This supports the premise of multiple projects or initiatives increase the possibility for security vulnerabilities. Multiple responses further identified that often multiple projects tend to leave out important aspects (such as information

security and LOAC classification). Factors that were identified to affect this issue are time constraints or lack of funding.

To address investigative question five, interview data identified there are often multiple lines of authority and direction provided from them. Evidence suggests that there is conflicting direction from multiple sources. To address investigative question six, interview data identified there weren't any other issues than those already identified by the previous interview questions.

Table 11, Factors affecting Main Research Question Summary.

Issue	Sound Plan	Multiple Plans	No Plan
Legal Guidance HIPPA			?
Legal Guidance LOAC			X
Standards		X	
Singular Direction		X	

Chapter Summary

This chapter presented the results of the research methodology outlined in Chapter III. Focused interviews of medical network support personnel and a detailed literature review were used to provide convergent sources of information for reaching the presented results. Two sites were used in this study to address the six investigative questions and in due course answer the main research question. Table 11 above depicts the factors identified in the research model presented in Chapter III. The table shows the results of the completed assessment as to whether the Air Force has reliable guidance in place to address these issues.

Table 11 shows that not only is there conflicting guidance in the areas of standards and singular direction, but that there is no direction in legal guidance.

V. Conclusions & Recommendations

Overview

The purpose of this exploratory research dealing with the Air Force's integration of medical networks and systems into the Air Force network was to provide an understanding of issues involved and afford a basis for further investigation. Interview transcripts and existing literature provided evidence that the Air Force is concentrating on the technology under the current plan. This chapter covers a discussion of the research, implications, and recommendation; suggestions for future research; and a summary.

Implications

Given the lack of previous research and newness of the subject matter, the results can provide many contributions. The most significant being the basis from which a survey can be developed. The survey can consist of close ended questions. Close-ended questions list answers, and respondents select either one or multiple responses. These questions produce more uniform answers than open-ended questions, but depend upon your knowing and including all relevant responses in the list. Responses to close-ended questions must be exhaustive and also mutually exclusive in providing for the selection of a single response (Sawer 1984). The survey could be distributed Air Force wide providing a clearer picture of project implementation and coordination, status of HIPAA compliance, and the other issued addressed in this research.

Suggested Future Research

This section outlines opportunities for future research. The first opportunity consists of duplicating this study using locations with similar sized medical facilities,

networks, and services offered to determine if the results are complimentary. A comparison of similar sized medical networks will determine if identified differences and results are unique to this study. Another research prospect would be to study the combination of HIPAA and the Laws of Armed Conflict (LOAC) more in depth. The research could aid in determining the growing legal ramifications facing information systems.

A third research opportunity would be to study the current standards in place governing such things as information assurance (IA), system security, and information classification. New technologies such as WIFI, cell phones, and Blackberries introduce new vulnerabilities not seen before (Gray 2005). In addition the new concept of software standardization could be looked at in greater detail. This could help in ascertaining if the program works in limiting the vulnerabilities and intruder attacks or if it just a way to save the Air Force money. A fourth research opportunity would be the conducting of the survey mentioned above. This survey could aid greatly in identifying inadequate processes and procedures affecting the whole Air Force network.

Summary

The far-reaching, ever-expanding, and ever more rapid advances in technology and the tactics employed by would be intruders over the last five years demand that the Air Force scrutinize all facets of integration. Singular direction, well defined standards, safe guarding information, and sound engineered and implemented technical capabilities are vital if the Air Force is to be successful in their transformation to Net -centric warfare and meeting the goals outlined in Air Force vision 2020.

The goal of this research was to assess the Air Force's implementation of the transition (MITT) of medical information systems into the Air Force Network. From this assessment a survey could be conducted to further evaluate the policies, procedures, and standards in place across the Air Force concerning information system integration. Deficiencies in any of these areas could potentially have devastating effects. The following quote from Deputy Attorney General Eric Holder displays the importance of protecting our networks: "For a real-world terrorist to blow up a dam, he would need tons of explosives, a delivery system, and a surreptitious means of evading armed security guards. For a cyber terrorist, the same devastating result could be achieved by hacking into the control network and commanding the computer to open the floodgates"(Holder 2000).

Bibliography

Butler, B. (2004). Scope Eagle 2004B.

Center, C. E. R. T. C. C. (2002). Attack Trends, the CERT Coordination Center**:** 1-5.

Center, C. E. R. T. C. C. (2005). CERT/CC Statistics 1988-2004.

Collmann, J. P. D. P., Robert (2003). Minimizing Risk to the Air force Network from Medical device Vulnerabilities.

Creswell, J. W. (1998). Qualitative inquiry and research design: Choosing among five traditions. Thousand Oaks, Ca, Sage Publishing.

Denzin, N. K. (1984). The research act. Englewood Cliffs, NJ, Prentice Hall.

Dorofee, C. J. A. a. A. J.(2001). OCTAVESM Criteria, Version 2.0.

Feagin, J., Orum, A., & Sjoberg, G (1991). A case for case study. Chapel Hill, NC, University of North Carolina Press.

Food and Drug Administration, F. (1999). Guidance for Industry, FDA Reviewers and Compliance on Off-The-Shelf Software Use in Medical Devices.

Gilligan, J. (2002). HEARING ON INFORMATION ASSURANCE. SUBCOMMITTEE ON MILITARY READINESS COMMITTEE ON ARMED SERVICES. Washington, D.C.

Gray, T. (2005). Cabir Hits U.S.

Headquarters Electronics Systems Center, E. N. (2004). "Medical Information Technology Transition (MITT) Last mile Design (LMD) System Design Document (SDD)."

Holder, E. (2000). INTERNET DENIAL OF SERVICE ATTACKS AND THE FEDERAL RESPONSE. SUBCOMMITTEE ON CRIME OF THE HOUSE COMMITTEE ON THE JUDICIARY AND THE SUBCOMMITTEE ON CRIMINAL OVERSIGHT OF THE SENATE COMMITTEE ON THE JUDICIARY. Washington, D.C.

Institute, S. (2004). The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts Consensus.

Leedy, P. D., and Ormrod, Jeanne E. (2001). Practical Research: Planning and Design,(7th Ed.). Upper Saddle River, NJ, Merrill Prentice Hall.

Messmer, E. (2004). Air Force to standardize Microsoft configurations, Network World Fusion.

Neveu, L. S. (2005). AF Instant Messenger offers Airmen real-time conversation, U.S. Air Forces in Europe News Service. 2005.

Office, C. I. T. P. (2004). Composite Health Care System II (CHCS II).

Peterson, M. M. (2002). Defense chief outlines challenges of information age warfare, GovExec.com.

Pethia, R. D. (2001). Internet Security Trends. Pittsburgh, Pa, Software Engineering Institute, Carnegie Mellon University**:** 15.

Pethia, R. D. (2002). Information Technology-Essential But Vulnerable: Internet Security Trend: Testimony of Richard D. Pethia, Director, CERT® Centers Software Engineering Institute, Carnegie Mellon University. House Committee on Government Reform, Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations.

Pethia, R. D. (2003). Cyber Security - Growing Risk from Growing Vulnerability: Testimony of Richard D. Pethia
Director, CERT® Centers, Software Engineering Institute, Carnegie Mellon University.
House Select Committee on Homeland Security
Subcommittee on Cyber security, Science, and Research and Development.

Ryan, M. E. (2001). SAF Memorandum, AF IT Initiatives.

Sawer, B. J.(1984). "Evaluating for Accountability."

Services, U. S. D. o. H. a. H. and O. f. C. Rights (2003). Standards for Privacy of Individually Identifiable Health Information Regulation Text; Security Standards for the Protection of Electronic
Protected Health Information; General Administrative Requirements Including, Civil Money Penalties: Procedures for Investigations, Imposition of Penalties, and Hearings.

Staff, T. J. (2001). Joint Publication 1-02, "Department of Defense Dictionary of Military and Associated Terms". Washington, DC.

Stake, R. (1995). The art of case research. Newbury Park, CA, Sage Publications.

Strand, T. L., Colonel, USAF (2004). THE MILITARY COMMANDER AND THE LAW. Maxwell AFB, AL, AFJAGS Press.

Tellis, W. (1997). "Application of a Case Study Methodology." The Qualitative Report **3**(3).

Trochim, W. (1989). "Outcome pattern matching and program theory." Evaluation and Program Planning **12**(4): 355.

USAF (2001). Global Vigilance, Research & Power: Air Force Vision 2020.

USAF (2002). "Air Force Information Strategy." AF CIO Newsletter(September 2002).

Verton, D. (2004). Air Force Consolidates Contracts, Software, Computerworld.

Vijayan, J. (2005). Fed Agencies Get a D+ In Computer Security, WWW.Computerworld.com.

Yin, R. (1989). Case study research: Design and methods (Rev. ed.). Newbury Park, CA, Sage Publishing.

Yin, R. (1994). Case study research: Design and methods (2nd ed.). Thousand Oaks, CA, Sage Publishing.

Yin, R. (2003). Case study research: Design and methods (3rd ed.). Thousand Oaks, CA, Sage Publishing.

Appendix A: Human Research Exception Letter

11 Aug 04

MEMORANDUM FOR AFIT/ENV
AFIT/ENR
AFRL/HEH
IN TURN

FROM: AFIT/ENV

SUBJECT: Request for Exemption from Human Experimentation Requirements (AFI 40-402): Thesis Research, AFIT/ENV, Vulnerabilities inherent to Medical Information Systems.

1. Request exemption from Human Experimentation Requirements of AFI 40-402 for the proposed study of medical information systems and the vulnerabilities they introduce into networks in conjunction with thesis research at the Air Force Institute of Technology. Purpose of this study is to investigate if the AF's proposed plan covers all possible contingences when adding the medical systems to the base network architectures. The results of this study may provide additional areas that need to be addressed for successful implementation of the Air Force's plan.

2. This request is based on the Code of Federal Regulations, title 32, part 219, section 101, paragraph (b)(2), which states "research activities in which the only involvement of human subjects will be in one or more of the following categories are exempt from this policy: (2) Research involving the use of educational tests (cognitive, diagnostic, aptitude, achievement), survey procedures, interview procedures or observation of public behavior". Information obtained will not be recorded in such a manner that human subjects can be identified, directly or through identifiers linked to the subjects nor will any disclosure of the human subjects' responses outside the research reasonably place the subjects at risk of criminal or civil liability or be damaging to the subjects' financial standing, employability, or reputation. Methodology used to collect information for research is based on case study and expert interview procedures and involves less than minimal risk. The following information is provided to show cause for such an exemption:

2.1. Equipment and facilities: No special equipment or facilities will be used.

2.2. Subjects: Subjects will be military and civilian leaders/managers in the communications or information technology career field, selected to participate in the study.

2.3. Timeframe: Data will be collected between Nov 04 and Dec 04.

2.4. Data collected: No identifying information obtained through interviews will be retained or reported in the final thesis. In order to complete the research effort, data collected on individual subjects may include duty title and duration in current position, which will facilitate analysis and follow up for the duration of this study only. Data gathering will be focused on organizational information specific to medical information systems, networks, and base level computer network architectures.

2.5. Informed consent: All subjects are self-selected to volunteer to participate in the interview process. No adverse action is taken against those who choose not to participate. Subjects are made aware of the nature and purpose of the research, sponsors of the research, and disposition of the survey results. A copy of the Privacy Act Statement of 1974 is presented for their review.

2.6. Risks to Subjects: Individual responses of the subjects will not be disclosed. This eliminates any risks to the subjects as noted in paragraph 2. There are no anticipated medical risks associated with this study.

3. If you have any questions about this request, please contact Master Sergeant Paul G. Oleksiak. at paul.oleksiak@afit.edu.

KEVIN L. ELDER
Associate Professor, Information Resource Mgt
Primary Investigator

Paul G. Oleksiak, MSgt, USAF
Student, Information Resource Mgt
Associate Investigator

Attachment:

Interview Questions

Appendix B: Interview questions

1. How is your work center configured?
2. Where do you take operational direction from?
3. How are the networks in the hospital configured?
4. Are computerized devices currently logically separated from the rest of the network?
5. Are there plans to do that?
6. Are imaging, billing, and patient records integrated?
7. Are there currently any back door connections outside the network?
8. Are you aware of any AF initiatives?
9. Timeline for completion?
10. Are the systems /circuits currently accredited?
11. If so, what does the process entail?
12. Are medical devices still under the mgt of vendors and fall subject to existing FDA guidelines & policies?
13. How are security patches implemented?
14. How are security incidents/updates reported?

Vita

Master Sergeant Oleksiak graduated from Notre Dame Bishop Gibbons High School in 1979. He earned an Associate of Science Degree in Electronics System Technology from the Community College of the Air Force in 1994, and a Bachelors of Science Degree in Electronics Management from Southern Illinois University in 1995.

MSgt Oleksiak reported for active duty in the United States Air Force in Aug 1986. From 1995 until Aug 2003 he held positions in two Special Duty Assignments. While with Defense Information Systems Agency Europe (DISA-E) he developed the IP networking plan for EUCOM's Op Plan 1003V and directed the implementation of numerous circuits and trunks in direct support of Operation IRAQI Freedom.

During his career MSgt Oleksiak has been selected for early promotion to Senior Airman under the Below the Zone Program, promoted from Staff Sergeant to Technical Sergeant under the Stripes for Exceptional Performance Program (STEP), and earned the John Levitow award while attending Airman Leadership School. In Aug 2003, he entered the Graduate School of Engineering and Management, Air Force Institute of Technology. Upon graduation, he will be assigned to Langley AFB.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From – To)*
21-03-2005	**Master's Thesis**	Sep 2003 – Mar 2005

4. TITLE AND SUBTITLE

Medical Devices, Supporting Networks, and Their Vulnerabilities: A Case Study Of the Integration of Medical Networks into the Air Force Information Network

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Oleksiak, Paul, G. MSgt, USAF

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)
Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way, Building 641
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/GIR/ENV/05M-13

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

With the implementation of "one Air Force, one network" under way it is important to look at how the Air Force plans to incorporate the medical field and its unique systems, networks, and mission. The medical field presents distinctive problems not seen in other areas. Open network vulnerabilities in the medical information systems not only pose a problem for the individual, but to the military service also. Possible security holes provide both access to vital military & personal information (end strength numbers, current status of personnel, social security), and a door way into the "network". Intruders now can possibly access command & control systems and other weapon systems. This research provides insight into the current & future information initiatives dealing with the Air Force's medical field and the Department of Defense's approach to system security. This research additionally looks at the laws and regulations dealing with privacy and ethical issues. This purview starts with the recently enacted Healthcare Insurance Portability and Accountability ACT (HIPPA), and concludes with the Laws of Armed Conflict. The research questions were answered through the use of a Case Study and a comprehensive literature review. The medical and network support teams from two Air Force medical facilities were the basis of this study.

15. SUBJECT TERMS

Biomedical networks, Computer Networks, Information systems, Information Assurance, Information Technology, Risk, Risk Management, Vulnerability

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Kevin L. Elder, PhD, USAF (ENV)
U	**U**	**U**	**UU**	93	**19b. TELEPHONE NUMBER** *(Include area code)* (937) 255-6565, ext ; e-mail: Kevin.Elder@afit.edu

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39-18