



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

**NETWORK VULNERABILITY ASSESSMENTS:
A PROACTIVE APPROACH TO PROTECTING NAVAL
MEDICINE INFORMATION ASSETS**

by

Steven Reinkemeyer

June 2004

Thesis Advisors:

Scott Côté
Dan C. Boger

Approved for public release; distribution unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			<i>Form Approved OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE June 2004	3. REPORT TYPE AND DATES COVERED Master's Thesis	
4. TITLE AND SUBTITLE: Network Vulnerability Assessments: A Proactive Approach to Protecting Naval Medicine Information Assets			5. FUNDING NUMBERS	
6. AUTHOR(S) Steven Reinkemeyer				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			10. SPONSORING/MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution unlimited			12b. DISTRIBUTION CODE	
13. ABSTRACT (maximum 200 words) The purpose of this study was to determine whether Naval Medicine's current Information Assurance Policy and resultant efforts properly address federal requirements or current threats confronting Naval Medicine information technology professionals. The primary research was conducted with a survey instrument detailing thirty questions with various response categories. The findings of the survey questionnaire revealed the existing numbers of previously compromised systems were directly related to the frequency of vulnerability scanning and remediation practices in the current threat environment. This study will provide insight to anyone interested in the future assessment of Naval Medicine's information security posture. These findings have important implications for command personnel charged with the responsibility and accountability of Naval Medicine's networks and data systems, as well as other communities throughout the Navy.				
14. SUBJECT TERMS vulnerability assessment, patch management, information assurance, Naval Medicine, vulnerability statistics			15. NUMBER OF PAGES 121	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL	

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution unlimited

**NETWORK VULNERABILITY ASSESSMENTS:
A PROACTIVE APPROACH TO PROTECTING NAVAL MEDICINE
INFORMATION ASSETS**

Steven Reinkemeyer
Lieutenant, United States Navy
B.A., St. Leo College, 1997
M.A., Management, Webster University, 2000
M.A., Human Resources Development, Webster University, 2000

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

**NAVAL POSTGRADUATE SCHOOL
June 2004**

Author: Steven Reinkemeyer

Approved by: Scott Coté
Thesis Advisor

Dan C. Boger
Co-Advisor

Dan C. Boger
Chairman, Department of Information Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The purpose of this study was to determine whether Naval Medicine's current Information Assurance Policy and resultant efforts properly address federal requirements or current threats confronting Naval Medicine information technology professionals.

The primary research was conducted with a survey instrument detailing thirty questions with various response categories. The findings of the survey questionnaire revealed the existing numbers of previously compromised systems were directly related to the frequency of vulnerability scanning and remediation practices in the current threat environment.

This study will provide insight to anyone interested in the future assessment of Naval Medicine's information security posture. These findings have important implications for command personnel charged with the responsibility and accountability of Naval Medicine's networks and data systems, as well as other communities throughout the Navy.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
A.	SITUATION ANALYSIS.....	1
B.	PREMISE AND HYPOTHESIS.....	3
C.	DEFINITIONS.....	3
	1. Naval Medicine.....	3
	2. Information System	3
	3. System Compromise	3
	4. Vulnerability Patch.....	3
D.	DISCLAIMER AND LIMITATIONS	4
II.	BACKGROUND	5
A.	INTRODUCTION.....	5
B.	CURRENT GLOBAL NETWORK THREATS	5
C.	CULTURE CONTRIBUTORS.....	7
D.	VULNERABILITY STATISTICS	8
E.	THE THREAT PERSPECTIVE	13
F.	THREAT AWARENESS AND RESPONSE RESOURCES	14
G.	WHAT IT MAY TAKE TO COUNTER FUTURE THREATS	16
H.	INFORMATION ASSURANCE POLICY REQUIREMENTS.....	19
	1. Federal Requirements	19
	a. Privacy Act of 1974, P.L. 93-579, 5 U.S.C. 552a (1974).....	19
	b. Computer Security Act of 1987 P.L. 100-235 (1988).....	19
	c. The Clinger-Cohen Act of 1996.....	19
	d. Management of Federal Information Resources (OMB Circular No. A-130, Appendix III, "Security of Federal Automated Information Systems", 1996.....	20
	e. Health Insurance Portability & Accountability Act of 1996, Public Law 104-191 (HIPAA)	20
	f. Presidential Decision Directive-63 (PDD-63), 1998.....	20
	g. The E-Government Act of 2002 (Public Law 107-347).....	21
	h. Federal Information Security Management Act of 2002 (FISMA)	21
	2. DoD Requirements.....	22
	a. DoD 5200.28-STD - Department Of Defense Trusted Computer System Evaluation Criteria.	22
	b. DoD Instruction 8500.2 – Information Assurance (IA) Implementation	22
	3. Command Requirements.....	23
	a. Military Health System (MHS) Information Assurance (IA) Policy/Guidance Manual.....	23
	b. Bureau of Medicine and Surgery (BUMED) Information Assurance Information Systems Security Policy Manual.....	24

	4.	Comparative Summary of Information Assurance Policies	24
I.		DEFENDING YOUR INFORMATION ASSETS	26
	1.	Awareness Training.....	26
	a.	Continuing Education	26
	b.	Annual Training	27
	c.	Professional Training	28
	d.	Experience-based	28
	2.	Vulnerability Assessments.....	29
	a.	Purpose.....	29
	b.	External.....	29
	c.	Internal.....	30
	d.	Network Surveys.....	30
	e.	Limitations of Vulnerability Assessments	30
	f.	Unexpected Consequences Derived From Testing	31
	3.	Automated Tools	31
	a.	DoD Approved.....	31
	b.	Non-DoD Approved.....	32
	c.	Vulnerability Assessment Tools.....	36
		1) Information Gathering Tools:	36
	d.	Tools and Information Available to the General Public	37
	4.	Proactive Measures	42
	a.	Systems Configuration.....	42
J.		POTENTIAL BENEFITS TO NAVAL MEDICINE	45
	1.	Navy Marine Corps Intranet (NMCI) Implications	45
	a.	Maintenance for Non-Qualifying Systems.....	45
	2.	Greater Assurance of Due Diligence in Personal Privacy Issues...	45
	3.	Estimated Savings in Personnel Costs	46
	4.	Significant Reductions in Vulnerabilities	46
III.		RESEARCH METHODS	47
	A.	WORK PLAN.....	47
	B.	SECONDARY	47
	C.	PRIMARY	47
	D.	SURVEY INSTRUMENT DEVELOPMENT	48
IV.		RESEARCH FINDING AND ANALYSIS	51
	A.	INTRODUCTION.....	51
	B.	DEMOGRAPHIC ANALYSIS	51
	C.	SURVEY QUESTIONNAIRE ANALYSIS.....	54
V.		CONCLUSIONS AND RECOMMENDATIONS.....	59
	A.	CORRELATION OF RESULTS IN COMPARISON TO PREMISE	59
	B.	THESIS QUESTIONS REVIEW	59
	C.	RECOMMENDATIONS FOR INCREASING NAVAL MEDICINE INFOSEC POSTURE.....	62
	D.	SUGGESTIONS FOR FURTHER RESEARCH.....	63
		LIST OF REFERENCES	65

BIBLIOGRAPHY	67
APPENDIX A. SAMPLE HTML RESEARCH QUESTIONNAIRE.....	73
APPENDIX B. SURVEY PRE-TEST QUESTIONNAIRES	81
APPENDIX C. ENTIRE POPULATION – RAW DATA SURVEY RESPONSE SPREADSHEET	85
APPENDIX D. ENTIRE POPULATION – END ANCHORED DATA CODING SPREADSHEET FOR QUESTIONS 5 THROUGH 30.....	93
APPENDIX E. ALL RESPONSE STATISTICS SPREADSHEET FOR QUESTIONS 5 THROUGH 30.....	95
APPENDIX F. LESSONS LEARNED DURING RESEARCH	99
INITIAL DISTRIBUTION LIST	101

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1.	Number of Incidents Reported. From <i>CERT/CC Statistics For Incidents</i> (2003).....	9
Figure 2.	Number of Vulnerabilities Reported. From <i>CERT/CC Statistics For Vulnerabilities</i> (2003).....	10
Figure 3.	CERT/CC Statistics for Percent of Annual Increase. From <i>CERT/CC Statistics for Percent of Annual Increase</i> (2003).....	12
Figure 4.	NIST Publications.....	45
Figure 5.	Regional Survey Response	52
Figure 6.	Survey Respondent Titles	52
Figure 7.	Respondent Organization Size (Personnel Strength).....	53
Figure 8.	Respondent Years of Experience	54
Figure 9.	Regional Survey Response	59

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1.	Statistics on all NIST Analyzed Vulnerabilities.	13
Table 2.	Comparative Summary of Information Assurance Policies.....	25
Table 3.	Computer Security Links	26
Table 4.	Vulnerability-Assessment Tools: Vendors at a Glance	33
Table 5.	Vulnerability-Assessment Tool Features.....	34
Table 6.	Vulnerability-Assessment Tools: Report Card.	35
Table 7.	Network Defense and Attack Tools and Links	42
Table 8.	NIST Publications Referenced in NIST SP 800-664.....	44

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I extend many thanks to those of you who assisted me in completing this project. Your willingness to assist me throughout this endeavor will never be forgotten. I am grateful for your patience, understanding, encouragement, and personal efforts afforded to me throughout the development of this thesis. I remain sure that I would not have accomplished this much without each and every one of you.... Thank You!!

Jennifer West
Erika Reinkemeyer
Scott Côté
Dan Boger
Gretchen Fenninger
Maria Horton
Naval Medicine CIOs
NMO site developers
Mohammad Kohistany
Sean Kelley
Richard Foster
Laura Tillery
William Murray
Dorothy Denning
JB Bagby
Margaret Freeman
Paul Clarke
Chris Eagle
Daniel Warren
John Halligan

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

The numbers of well-known software vulnerabilities continue to increase and will likely worsen as even more powerful and complex applications emerge. Traditionally, information technology managers have combated network vulnerabilities with a variety of approaches. The most common involves applying the latest patch (“hot fix”) or service pack to a computer system, while maintaining stringent access control lists (ACLs) on routers and firewalls to filter network traffic. This last method, though somewhat effective, is limited in that even the best effort approaches to separating good and bad network traffic can be circumvented. Unfortunately, technologies such as these are intended to serve primarily as perimeter network defense systems, but have quickly become the panacea of network security. In many cases, a false sense of security has been created and a large number of networks fall prey to well-known exploits because the recommended system patches have not been applied to vulnerable systems. Additionally, 80% of system compromises originate within the local network, leaving the perimeter controls at a significant disadvantage (Konigsberg, 2002). While the most basic tenets of securing computing systems are the application of system patches, fewer patches are being applied as networking environments become more complex.

The proposed research within this thesis evaluated whether automated network vulnerability scanning software solutions would provide a reliable and cost effective means to manage the growing numbers of operating systems and applications vulnerabilities, while providing a greater ability to comply with federal requirements in the area of information security practices for Naval Medicine components. This project also provided an analysis of the total number of systems compromises over the past 12 months and concluded that vulnerability scanning and remediation procedures were not being performed expediently enough to meet the current information assurance threats.

Knowing there will always be differences in the way organizations respond to potential threats, common to them will be maintaining an effective patch management program, becoming even more important as zero-day exploits begin to appear on a more

regular basis. The ability to incorporate this, as well as new and emerging concepts and practices, will ultimately determine the future success of any organization's information security program.

It should be noted that there are other security models that do not depend on patch management, or supplement it, but will not be covered in this work. Managing and patching systems is now a way of life in our industry, and until such time as they are unnecessary, they need to be systematically incorporated into our policies.

I. INTRODUCTION

A. SITUATION ANALYSIS

The number of well-known software vulnerabilities, on average, has doubled every year since 1998 (CERT, 2003) and will likely worsen as even more powerful and complex applications emerge. In 2002, more than 4,000 well known vulnerabilities were listed and over 82,000 incidents were reported to CERT (CERT, 2003). Surprisingly, 99% of reported incidents resulted from not having well-known exploits patches on affected computing systems (Shipley, January 23, 2003).

Traditionally, information technology professionals have thwarted network vulnerabilities using a variety of approaches. One of the most common involves applying the latest patch or service pack to a computer system, while maintaining stringent access control lists (ACLs) on routers and firewalls to filter network traffic. It is well recognized that even the best approaches to separating good and bad network traffic can be circumvented, which has lead to numerous implementations of Intrusion Detection Systems (IDSs) to provide notification of suspected malicious network traffic.

Modern approaches to network security are focused on signature based recognition and access control lists (ACLs), such as are found in firewalls and routers, and Intrusion Detection System (IDS) monitoring. Unfortunately, these technologies are intended to serve primarily as perimeter network defense systems, but have quickly become the perceived panacea of network security. In many cases, because the recommended system patches are not applied to vulnerable systems, a large number of networks fall prey to a false sense of security from the aforementioned perimeter defense, and are victims of well-known exploits. Additionally, 80% of system compromises originate within the local network, leaving the firewall and certain IDS at a significant disadvantage (Konigsberg, 2002). Recent surveys also indicate that the majority of attacks are directed at port 80, which has traditionally not been filtered since it facilitates Web traffic (Burns, 2003). While the most basic tenets of securing computing systems are the application of system patches, it has become a seemingly less practiced task as

networking environments become more complex, and defenses are being thrust to the perimeter.

Maintaining a relatively secure computing network has become a comprehensive task for many information technology managers. Preparing for the next wave of system exploits to approach the Internet remains a mystery to many information managers unable to keep abreast of the trends. Commonly known vulnerabilities and the attacks associated with them are well documented, such as the buffer overflow; however, these vulnerabilities have not been fully addressed and corrected by the vendors for a variety of reasons. For those that even realize the importance of patching systems, many have concerns of system patch incompatibility and fear that the available patches may disrupt or negatively impact the computing system operation. Protecting information systems can equate to ensuring that the most recent software patches have been applied to every known vulnerable system, but knowing of every patch or update, and their possible side-effects, becomes a virtually impossible task. Management of these systems becomes a somewhat daunting task then, as the number of vulnerabilities increases, the number of systems to be managed grows, and information technology staffing remains the same or decreases due to cutbacks.

The proposed research evaluates whether automated network vulnerability scanning software solutions can provide a reliable and cost effective means to manage the growing numbers of operating systems and applications vulnerabilities, while providing a greater ability to comply with federal requirements in the area of information security practices. The research focuses on determining what, if any, formal patch management practices exist and how current actions can be supplemented with automated vulnerability scanning and patching technologies.

This study is of particular importance to the command personnel charged with the responsibility and accountability of Naval Medicine's networks and electronic data systems. The supervisors, educators and trainers of today will develop the leaders of tomorrow, who will become responsible for ensuring that mission essential objectives are completed. To accomplish this, leaders must know what people need or desire to get the best performance from them. This research offers practical information regarding

modern patch management techniques and the technologies available to assist them in that effort.

The Internet has become essential for most organizations and has grown exponentially in the number of private parties obtaining access each year. As more people engage in electronic activity, the potential threat increases at the same rate (Azari, 2003). There will always be differences in the way people and organizations respond to potential threats, but maintaining an effective patch management program will become even more important as zero-day exploits begin to appear. The ability to incorporate this, as well as new and emerging concepts and practices will ultimately determine the future success of any organization's information security program.

B. PREMISE AND HYPOTHESIS

Based on prior experience handling incident reports of subordinate command computer compromises, and following through with mitigation of known vulnerabilities within Naval Medicine, observation suggests at least three out of four compromises resulted from lack of timely patch administration. In conducting the research for this thesis, this observational figure posed a suitable point from which to pursue the following hypothesis: 75 percent of Naval Medicine's known information systems compromises were not protected by the available vulnerability patch(es).

C. DEFINITIONS

1. Naval Medicine

The Department of the Navy healthcare organization, composed of approximately 400 individual units responsible for maintaining the health of all Navy and Marine Corps personnel.

2. Information System

Hardware and software, application programs and devices that input, process, store and/or output electronic data elements.

3. System Compromise

Any unauthorized system events or data theft occurring on an information system.

4. Vulnerability Patch

A software and or hardware vendor remedy that corrects known system vulnerabilities or operating system errors.

D. DISCLAIMER AND LIMITATIONS

The information used to compile research findings is utilized to satisfy the academic reporting requirements needed for completion of a Master of Science degree in Information Systems Technology from the Naval Postgraduate School. Surveys will be limited in distribution to Naval Medicine Chief Information Officers. Additionally, completed survey questionnaires and any other organizational data utilized within this research paper will be held in strict confidence and used solely for the indicated purpose.

Secondary research efforts may be limited by the number of personnel employed within Naval Medicine available, or their willingness to participate in the Information Assurance Management Survey. The total percentage of known information systems compromises that were not protected by the available vulnerability patch will be extracted from the survey results to validate or invalidate the premise. Additionally, the length of the academic term further limits the scope of the study. Lastly, the efforts of this research may not accurately represent the other components of the United States Navy in regards to Chief Information Officers or any other Department of Defense representatives fitting the above mentioned titles.

II. BACKGROUND

A. INTRODUCTION

Today, the only thing that seems certain is change. Business and operational environments have undergone significant transformations over the past decade. The constant stream of differing and more powerful Internet technologies, networked systems, and applications have refined processes and simultaneously created a surfeit of system vulnerabilities. This problem tends to increase each time a new technology or a system with more features is introduced. If the increasing complexity is coupled with other issues associated with expanding enterprises, it is relatively easy to imagine that the proper management and control of such technologies could be difficult at best. A primary concern regarding these technologies is ensuring information security; though it is often one of the most difficult items to justify in annual budgets as it becomes more difficult to assess, prioritize and measure corrective methods to counter the known risks or threats. Personnel, knowledge, funding, tools, and training are therefore seemingly obvious deficiencies in information security environments.

B. CURRENT GLOBAL NETWORK THREATS

A small nation-state now has the ability to cripple a large adversary by compromising unprotected information system controls. Electrical grids, water treatment facilities, airline communications systems, financial systems, and many others are susceptible to compromises by anyone with the appropriate skill levels, equipment, and time. A system can be monitored and maintained to resist or repel known threats, but one sophisticated hacker can wreak havoc in minutes. A well-publicized example of how quickly and successfully an attack can be performed was demonstrated by the Slammer Worm (AKA: Sapphire), which was released on 25 January 2003. The Slammer worm was the fastest-spreading worm in computing history, primarily due to its small total size of 404 bytes, which included the header. Slammer was an exploit of a buffer overflow in Microsoft's SQL server and applications created with the Microsoft Server 2000 Desktop Engine. Within 3 minutes of its release, the total number of infected hosts doubled every 8.5 seconds. Thirty minutes later, the worm and its clones were scanning 55 million IP

addresses per second. Within 40 minutes, approximately 90% of all susceptible hosts had been compromised (McGuirl, 2004).

Although Slammer was not carrying a malicious payload, it did cause significant collateral damage. Twenty-seven million Korean mobile phone and Internet accounts were offline, more than a 100,000 Portuguese cable modems were offline, 13,000 Bank of America ATMS were downed, and emergency service providers in Seattle lost dispatch capabilities for hours while attempting to service a community of 700,000 people. Mi2g Limited, an English security firm, estimated that Slammer costs reached \$1.2B in productivity losses (McGuirl, 2004).

The Slammer incident is one of many examples where a vendor patch was available for a well-known exploit for more than 6 months, but had not been applied to the affected systems. Slammer is not the first, nor the last, to be seen. We must not forget while history repeats itself, in cyberspace it replicates. Two previous worms that caused similar issues were the Code Red IIS ISAPI buffer overflow attack and the Nimda Worm that exploited an IIS Web traversal vulnerability. Again, anyone who experienced these attacks could have prevented them if they had simply applied the patch 3 to 4 weeks after the vulnerabilities had been announced.

Slammer originated with one initial instance of a compromise. If one considered that a number of these exploit attempts and break-ins occur on a daily basis, the concept may impose more concern. To determine just how much malicious activity occurs on the Internet, I-trap Security Services, based in Cleveland, Ohio, monitored and analyzed two weeks of internet traffic from a 10,000 node ISP enterprise that serviced Tel Aviv University, the largest university in Israel. A two-week sampling recorded 180,000 attack events. Those events consisted of scanning and actual break-in attempts. Approximately 96 percent of the recorded scans were followed by attacks from the same source. That is a staggering number in itself, but it is more important to recognize that roughly 90% of those attacks are generated by worm activity. Any organization relying on perimeter controls such as firewalls, router access control lists, intrusion prevention systems or anti-virus tools would not have been protected. The I-trap report indicated that most of the attacks originating from China and the United States were automated;

however, it should be noted that attack totals were supported by 99 differing countries around the globe. Another interesting note from the sample was that more than 139,000 of those attacks (75%) were directed at port 80, the port used for standard Web (HTML) page transfers. (Burns, 2003)

Today's most competitive organizations, whether private, corporate or government-funded, are employing their personnel with the fastest and most efficient computing systems to perform their tasks. The majority of those systems interface with the Internet, and the electronic transactions and/or data stored on those systems is at risk – some more than others, but at risk nonetheless. If these risks are discovered by anyone with malicious intent, the organization's image and livelihood can be damaged in a number of ways. System compromises can result in, but are not limited to, media attention, public embarrassment, financial losses, whether stolen or incurred by penalty, increased maintenance for restoration efforts, and loss of productivity in downed systems. Protecting information system assets in a globally connected world requires a dedicated amount of time and funding to counter the existing threats. A near real time vulnerability scanning and patching process is the last line of defense in protecting information assets once perimeter filters have been breached (Nicolett and Pescatore, 2003).

C. CULTURE CONTRIBUTORS

Computing systems technology has reached approximately 25 percent of homes worldwide in the past decade (Azari, 2003). The world we lived in just ten years ago has been replaced with much more convenient and less expensive methods of performing daily tasks, methods driven by technology that affects nearly everything imaginable in our daily lives. These changes range from daily transactions involving purchases and sales to monetary transfers, safety devices, and communications systems, among many others. Global connections link the majority of markets and institutions around the world and significantly affect the overall economy. Military components tout cyber warfare as the new order for combat operations, and a number of technology-driven weapons systems, often referred to as smart weapons, are fast replacing conventional methods of warfare.

The technological revolution even affects those millions that don't use the Internet or other technological advances. As previously mentioned, anyone relying on electricity, purified water, public transportation or financial systems can be affected by technology because it also drives the majority of those systems. This continued reliance on technology will continue to enforce its utilization and dependence.

D. VULNERABILITY STATISTICS

Although it was not the first, one of the most widely recognized worms was designed by Robert Morris in 1998. The Morris worm introduced many to the reality of cyber threats as it invaded approximately 6000 computers within a couple of hours. In 1998, this figure represented 10% of the entire Internet. The worm was not destructive, but it did prove the powers of a buffer overflow. This event had two beneficial outcomes: the realization that dangers do exist in a connected world, and more importantly, the genesis of the Computer Emergency Response Team (CERT), which was developed as a notification and dissemination point for known vulnerabilities. The CERT Coordination Center (CERT/CC) is supported by federal research funds and is operated by Carnegie Mellon University. Many information assurance practitioners have reviewed their advisories about vulnerabilities, bugs, patches, and where to find the fixes to those known problems (Rubin, 2001). Figures 1 through 3 display the number of reported incidents, vulnerabilities and the percentages of increase from 1988 through 2003, respectively.

The number of incidents reported over the past five years produces a wide range of assumptions. The Internet, and incidence of malicious code, has grown substantially. Reported incidents may not necessarily be the actual number of incidents as many organizational reputations may be at risk for simply admitting they have experienced an incident. What may not be as obvious is the fact that many more organizations are reporting incidents because they are more familiar with the occurrence of system compromises.

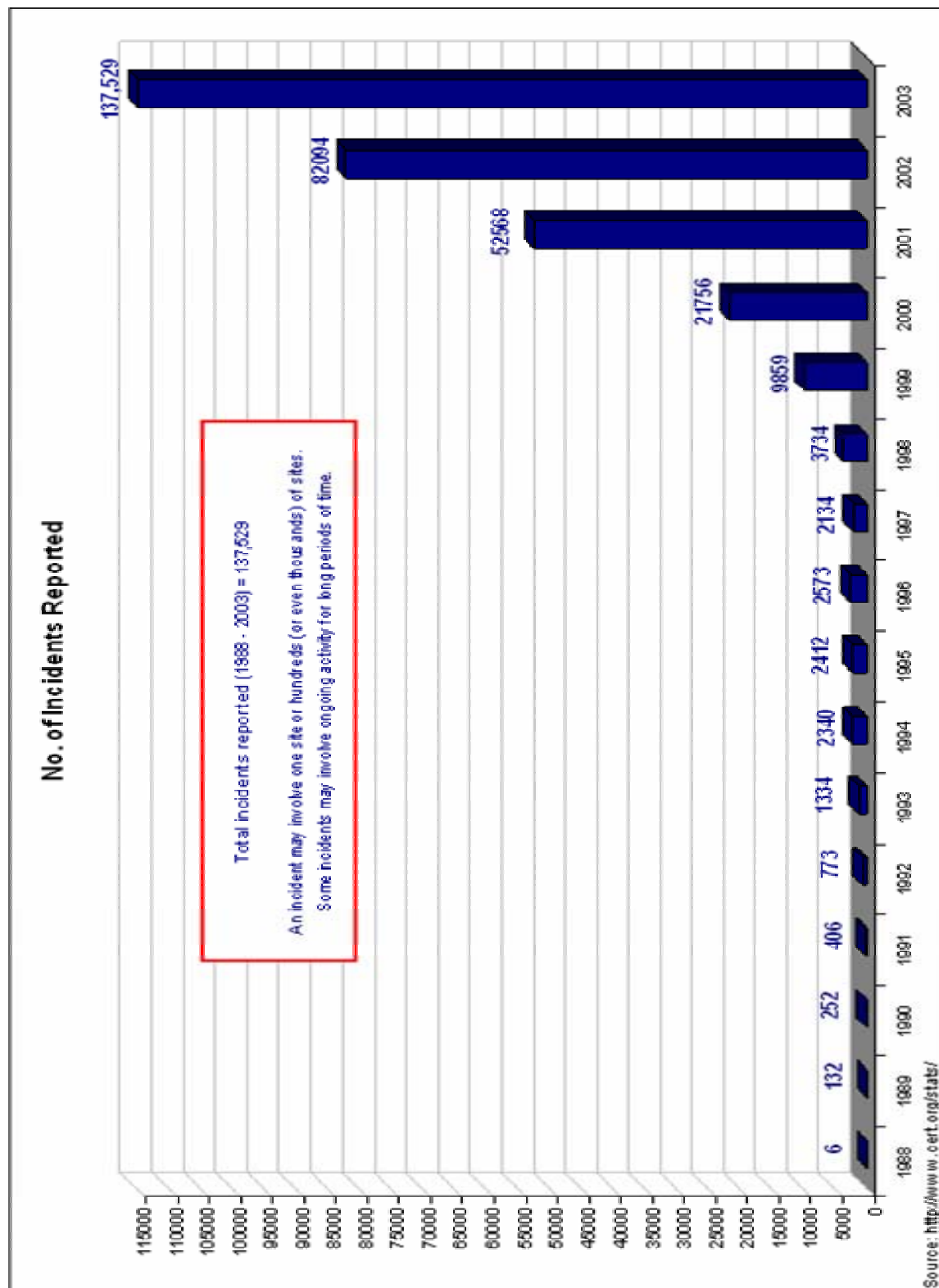


Figure 1. Number of Incidents Reported. From *CERT/CC Statistics For Incidents* (2003).

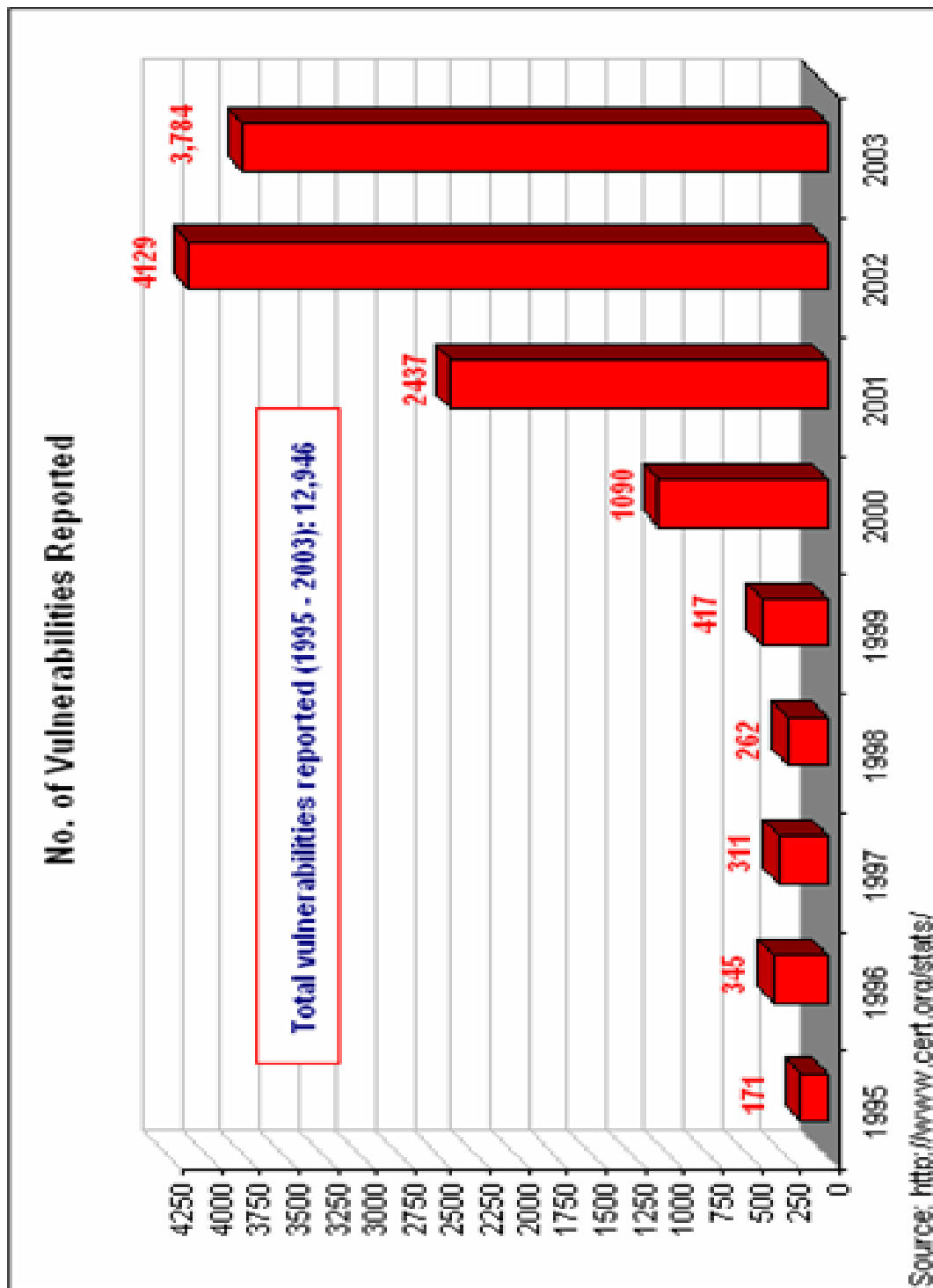


Figure 2. Number of Vulnerabilities Reported. From *CERT/CC Statistics For Vulnerabilities* (2003).

The number of new vulnerabilities specifically indicates those that have not been seen before. Many are reiterations of earlier ones, but they are still different. On 24 February 2004, at the annual RSA panel discussion, Quals reported that “the lifespan of some vulnerabilities is unlimited” and that “50% of the most prevalent and critical vulnerabilities are being replaced on an annual basis”(Eschelbeck, 2004). Quals also presented a differing total number of vulnerabilities based on vulnerability data from December 2003. Their presentation submitted that there have been a total 3,011,000 IP scans, 1,905,000 total critical vulnerabilities, 2,054 different vulnerabilities and 1,175 different critical vulnerabilities. Their definition of critical was defined as “Providing an attacker the ability to gain full control of the system and/or leakage of highly sensitive information. For example, vulnerabilities may enable full read and/or write access to files, remote execution of command, and the presence of backdoors”(Eschelbeck, 2004).

During 2002, the Security Alert Consensus said there were approximately 1000 new operating system and applications vulnerabilities, which equates to roughly 83 new vulnerabilities per month. During 2003, SecurityFocus reported 7,679 vulnerabilities in their database, while NISTS ICAT metabase listed only 5,712 and the Common Vulnerabilities and Exposures Group at mitre.org listed only 2,573 (Shiple, June 26, 2003). It seems rather confusing that such drastic differences are reported, but the important thing to remember is that there are thousands of vulnerabilities that have been identified and there are likely thousands more that have not been discovered. Becoming aware of them and guarding information systems from those threats are the only ways a connected organization will be able survive the onslaught of malicious code floating around in cyberspace. “In short, when it comes to compromise of data confidentiality, what you don’t know can really hurt you” (Rubin, 2001).

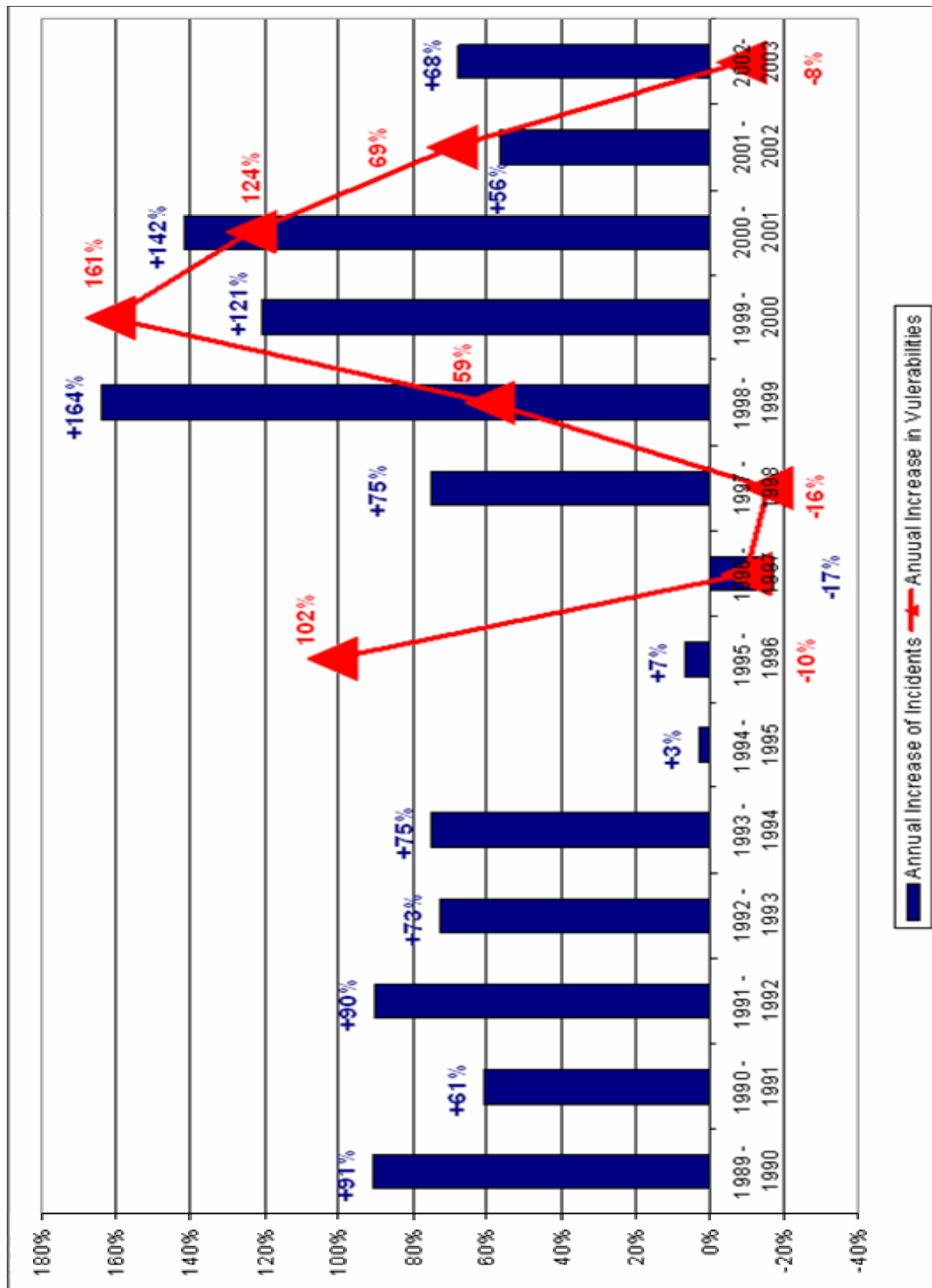


Figure 3. CERT/CC Statistics for Percent of Annual Increase. From *CERT/CC Statistics for Percent of Annual Increase* (2003).

As of 20 May 2004, the past four years of NIST-analyzed vulnerability types were as follows:

Statistics on all NIST Analyzed Vulnerabilities				
Vulnerability Type	2004	2003	2002	2001
Vulnerability Count	264	1007	1307	1506
Remote Attack	193 (73%)	755 (75%)	1052 (80%)	1056 (70%)
Local Attack	75 (28%)	252 (25%)	275 (21%)	524 (35%)
Denial of Service	68 (26%)	281 (28%)	330 (25%)	419 (28%)
OS Vulnerabilities	56 (21%)	163 (16%)	212 (16%)	248 (16%)

Table 1. Statistics on all NIST Analyzed Vulnerabilities.

From http://icat.nist.gov/vt_portal.cfm

Note: This table shows the distribution of various vulnerability characteristics. The raw number in each cell is the number of vulnerabilities that meet that particular characteristic for that year. The percentage to the right of each raw number is the percentage of vulnerabilities having that particular characteristic for that year.

The increases and a select number of decreases in vulnerabilities and incidents can be directly related to the widespread releases of new operating systems software and applications, while additional decreases can be attributed to the investments made in information assurance practices to combat such threats. Some analysts contend that the rise in reports is due to the increased numbers of people that are monitoring the network and the recent expansions of the unsophisticated consumer market obtaining broadband connections such as DSL and cable modems. These types of connections are always on and present immediate dangers to the system owner if not configured or protected by filtering devices such as firewalls. (Goth, 2004)

E. THE THREAT PERSPECTIVE

The United States military services are not excluded from the same vulnerabilities that confront the rest of the free world. To get an idea of just how many times the

military services have faced vulnerability incidents, consider the following links that showcase past hacker activities.

Current attack postings are available at zone-h.org at <http://www.zone-h.org/en/defacements/>. It is disturbing to know that new attacks are posted nearly every minute of every day. At certain times, there are multiple attacks occurring within one minute around the globe. This site clearly displays the operating system that was compromised. A quick review will provide all the proof required to dispel the myth that some operating systems cannot be breached.

The digital attacks archive link on the left column of zone-h.org's web page will redirect a Web browser to the primary archive. If desired, add the filter ".mil" to view what the services have encountered in the past. OSD, SPAWAR, and even some of Navy Medicine's Web pages are easily found within the archive. A visit to the breakout link within the attrition.org site at <http://www.attrition.org/mirror/attrition/> allows one to view even more .mil and other federal agency defacements. According to this mirror site, since July 1999, 186 defacements have occurred on .mil domains, and 42 (approximately 23%) of those were Navy-specific.

F. THREAT AWARENESS AND RESPONSE RESOURCES

A significant number of resources exist to alert and help information systems personnel defend their assets. Many of them are listed on the NIST Vulnerability and Threat Portal http://icat.nist.gov/vt_portal.cfm. Links to other competent vulnerability notification organizations such as The US Computer Emergency Readiness Team (US-CERT), the Carnegie Mellon Software Engineering Institute, the National Institute of Standards and Technology, and the SANS Institute are linked from the NIST portal. Each of them differs slightly, but each is an excellent resource. Users can submit to mailing lists for frequent vulnerability updates.

The US Department of Homeland Security (DHS) employs the US Computer Emergency Readiness Team (US-CERT) and provides the US-CERT Current Activity Web page, which offers an up to date summary of the most frequent and devastating types of information security incidents. This resource is located at: http://www.us-cert.gov/current/current_activity.html. The CERT/CC Incident Notes Web page is

maintained by the Carnegie Mellon Software Engineering Institute and is located at http://www.cert.org/incident_notes/. Another feature page maintained by the Carnegie Mellon CERT® Coordination Center provides Steps for Recovering from a UNIX or NT System Compromise. That resource can be found at http://www.cert.org/tech_tips/win-UNIX-system_compromise.html.

The ICAT Metabase is maintained by the Computer Security Division at the National Institute of Standards and Technology. The ICAT is an index of searchable computer vulnerabilities. It also provides a search capability at a granular level that links users to vulnerability and patch information and can be found at <http://icat.nist.gov/icat.cfm>.

The System Administration, Networking, and Security Institute (SANS) showcases the SANS Top 20 Internet Security Vulnerabilities at <http://www.sans.org/top20/>. The SANS Top 20 is the merger of two top-ten lists. Specifically, it provides the ten most commonly exploited vulnerable services in Windows and the ten most commonly exploited vulnerable services in UNIX and Linux operating systems. There are a great number of security incidents occurring every year that affect these popular operating systems, but the majority of the successful attacks focus on one or more of the twenty identified vulnerabilities. It should be noted that the twenty vulnerabilities are those that are considered by a number of security experts to be the most critical vulnerabilities that warrant immediate attention. The entire process is coordinated by leading security experts that practice security roles in some of the most information security-focused agencies around the world. This is not limited to, but includes information from, security vendors, consulting organizations and a number of the top university-driven security programs. The SANS Institute Internet site also maintains a reading room archive rich in resources pertaining to policy, risk assessment procedures as well as a number of other information security-related topics.

Last, but not least, Bugtraq is considered by many to be the most important Internet information security list. Vulnerabilities announcements are often posted here well in advance of the government-sponsored resources previously referenced. A number of current and previous archives can be found at <http://www.ntbugtraq.com>.

Each of these noted services is a dynamic and ever-changing resource, from step-by-step instructions to additional links regarding information useful for correcting known security flaws. Most generally, each of them provide feedback links for continuous improvement initiatives and encourage participation in fighting the good fight in the continuous battles involved in the information security arena.

G. WHAT IT MAY TAKE TO COUNTER FUTURE THREATS

The future holds many uncertainties, but the experts agree that the cyber universe is a dangerous place to conduct electronic transactions, whether business or personal. There are a number of reasons those dangers exist. The reality of the bits and bytes world is that nothing is bulletproof. NIST recently reported that 36% of vulnerabilities are resultant of configuration or design problems, and the rest are due to programming errors. “Of those errors ‘the basic mistakes’—buffer overflows, directory traversal attacks, format string vulnerabilities, symlink attacks, cross-site scripting vulnerabilities, and shell metacharacter issues—are responsible for 51 to 64 percent of vulnerabilities” (Goth, 2004). Remediating the known vulnerabilities in a timely manner and configuring systems to repel attacks remain the best known defenses.

If these realities are not heeded, they will be costly in terms of lost data, downed systems, or legal penalties. To counter a threat, two basic concepts must be understood: The threat has to be identified; only then can it be responded to. Those two factors will determine your overall effectiveness in thwarting the threat. NIST and other vulnerability summary organizations are now facing the challenges of keeping pace with the outbreaks of vulnerabilities, identifying them so a response can be developed. The decreasing window of time between discovery and remediation has incited the need for even more efficient processes for determining the identifiers for inclusion into the industry standard Common Vulnerabilities and Exposures (CVE) Dictionary. The CVE in and of itself is not a database; it is simply a dictionary of vulnerabilities and exposures (Goth, 2004).

To combat increasingly sophisticated and more aggressive cyber attacks, everyone will be required to entertain new approaches, tools and services to increase their chance of survival. The standard practices of waiting for alerts and patching when

convenient is already becoming ineffective. It is predicted that “soon computers will face ‘Warhol’ threats that spread across the Internet and infect systems worldwide within 15 minutes. In a few years, the Net will be hit by ‘flash threats that can spread in just seconds...’” (Evers, 2003). Leading researchers and security experts further predict that during 2004, the number of remote procedure call (RPC) exploits will continue to appear. The RPC is a primary component required to manage client-server computing. These procedures are not restricted to Microsoft operating systems and Jeff Moss, President and CEO of Black Hat, Inc. reported that hackers are now looking for areas that are not being addressed. “In particular, hackers are exploring ways to attack memory ‘heaps,’ or areas of computer memory that are created dynamically when programs run.” (Roberts, 2003)

The ever-increasing rates of information systems compromises have also gained the immediate attention of the federal government over the past decade. As voters become more dissatisfied with the level of protection their private information is afforded, the requirements and penalties imposed for lack of due diligence will continually increase. The future of information assurance has already been addressed by a federal legislation. Sean Doherty published email poll results regarding the impact of the newest federal initiatives in the July 2003 edition of *Network Computing* magazine. The survey indicated that 72% of survey respondents were directly affected by the legislative mandates. “The Gramm-Leach-Bliley Act (GLBA) and the Health Insurance Portability and Accountability Act (HIPAA) hold affected enterprises accountable to protect private information, meaning IT must assess the risks and implement appropriate safeguards” (Doherty, 2003). Healthcare information losses resultant of ignoring the rules under HIPAA can cost up to \$25,000 per violation. Individual losses of personal information can cost financial institutions \$1,000 per individual or up to \$500,000 for a class of individuals who have not been afforded the appropriate protection mandated for them under the GLBA.

Additionally, the Sarbane-Oxley Act of 2002 (SARBOX) mandates that any company issuing private securities maintain the appropriate controls of their financial reporting systems, as well as perform assessments of their systems’ controls and reporting those findings to the Securities and Exchange Commission (SEC). The

SARBOX legislation can impose fiscal penalties up to \$1 million as well as ten years' imprisonment for a corporate officer that knowingly endorses a false financial report.

As a part of the Federal Information Security Act of 2002 (FISMA), Congress is requiring the National Institute of Standards and Technology (NIST) to develop guidance for IT management safeguards that will adequately address the information assurance security triad of confidentiality, integrity and availability of information systems and their data elements. NIST Special Publication 800-53 is expected to be finalized in the near future to detail required government entity controls by 2005, which will also include requirements for hardware and software maintenance. The 238-page draft version is currently available for comment. This document should be utilized in conjunction with two other NIST publications: the Federal Information Processing Standard Publication 199: Standards for Security Categorization of Federal Information and Information Systems; and the NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems (Chabrow, 2003).

The draft version of the National Strategy to Secure Cyberspace, September 2002, also highlights the changes required to properly address existing deficiencies in information assurance practices. On Tuesday, 3 December 2002 at the Computer System Security and Advisory Board Meeting, Richard Clarke, the Chair of the President's Critical Infrastructure Protection Board "...indicated that the real problem was not the lack of threat analysis but of a vulnerability analysis." (Clarke, 2002). According to the draft, a number of initiatives and practices will have to be adopted to protect information technology assets. Among those items that pertain to this project, section R3-5 in the summary section is most applicable. This section contends that "Federal agencies should continue to expand the use of automated, enterprise-wide security assessment and security policy enforcement tools and actively deploy threat management tools to preempt attacks" (Computer System Security and Privacy Advisory Board, 2002).

If the information assurance initiatives to safeguard information assets can focus more on a holistic approach that addresses the security framework, specifically in the areas of policy, processes, personnel and products, a more recognizable sense of information security will be realized (McGuirl, 2004).

H. INFORMATION ASSURANCE POLICY REQUIREMENTS

This section identifies the source of privacy and security requirements for Federal automated information systems with which DoD and Naval Medicine must comply. Governing Federal privacy and security policy statements express fundamental privacy and security requirements and serve as a framework for developing more specific technical and administrative security specifications, design, and operational requirements.

1. Federal Requirements

a. Privacy Act of 1974, P.L. 93-579, 5 U.S.C. 552a (1974)

The Privacy Act requires federal agencies to safeguard personal data processed by automated information systems. This Act also requires the agencies to allow individuals to find out what personal information is being maintained and to correct inaccurate information. The Act identifies physical security procedures, information management practices, and computer and network controls for systems that process Privacy Act data.

b. Computer Security Act of 1987 P.L. 100-235 (1988)

The Computer Security Act, which went into effect in September 1988, requires every U.S. government computer system that processes sensitive information to have a customized security plan for the system's management and usage. It also requires all U.S. government employees, contractors, and others who directly affect federal programs undergo periodic training in computer security. All users of systems containing sensitive data must also receive computer security training corresponding to the sensitivity of the data to which they have access.

c. The Clinger-Cohen Act of 1996

The Clinger-Cohen Act requires all federal government agency heads to design and implement IT management processes for maximizing the value and assessing and managing the risks of the IT acquisitions. They are also directed to establish goals for improving the efficiency and effectiveness of agency operations through the effective use of IT. With regards to information assurance, they ensure that the information security policies, procedures, and practices of the agency are adequate.

d. Management of Federal Information Resources (OMB Circular No. A-130, Appendix III, "Security of Federal Automated Information Systems", 1996

OMB Circular No. A-130 Appendix III, revised in February 1996, stresses management controls, individual responsibility, accountability, and awareness and training, rather than technical controls. Agencies must ensure that risk-based rules of behavior and operation are established, that employees are trained in them, and that the rules are enforced. Specifically, it requires agencies to implement and maintain a program to ensure adequate security is provided for all agency information collected, processed, transmitted, stored, or disseminated in general support systems and major applications. Appendix III no longer requires a formal risk analysis. Instead, risk-based management is employed to address general risk assessments. Major risk-based management factors include: applications, threats, vulnerabilities, and safeguard effectiveness. Lastly, each agency is required to work with OMB, NIST, and NSA to improve agency computer security.

e. Health Insurance Portability & Accountability Act of 1996, Public Law 104-191 (HIPAA)

The HIPAA Security Rule specifically focuses on the safeguarding of electronic protected health information (EPHI). The main goal of the HIPAA Security Rule is to protect the confidentiality, integrity, and availability of electronic protected health information. The Federal Information Security Management Act (FISMA) applies to all federal agencies and all information types, but the HIPAA requirement further refines the rules for use of EPHI. All Naval Medicine facilities and health care providers must comply with the HIPAA Security Rule, which establishes a set of security standards for securing certain health care information. A health care provider is defined as any provider of medical or other health services, or supplies, which transmits any health information in electronic form in connection with a transaction for which a standard has been adopted.

f. Presidential Decision Directive-63 (PDD-63), 1998

This document recognizes that the United States maintains the world's strongest military as well as the largest national economy and that those aspects of our

power are mutually reinforcing and dependent. It also recognizes that each aspect is increasingly reliant on certain critical infrastructures and cyber-based information systems. It further recognizes that although critical infrastructures had historically been physically and logically separate systems with little interdependence, they were increasingly dependent on information technology, and each other. The increased automation and links between them also created new vulnerabilities to equipment failure, human error, weather and other natural causes, and physical and cyber attacks. The directive contends that addressing these vulnerabilities require flexible and evolutionary approaches for the public and private sectors. Frequent assessments are made of critical infrastructures' reliability, vulnerability and the threat environment because the threats to infrastructures will continue to change and protective measures and responses must be robust and adaptive.

NSA is charged with the National Manager responsibilities and assesses U.S. Government systems for interception and exploitation, disseminates threat and vulnerability notices, establishes standards, and conducts research and development in areas of security product evaluations.

g. The E-Government Act of 2002 (Public Law 107-347)

The E-Government Act of 2002 recognizes the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, entitled the Federal Information Security Management Act of 2002 (FISMA), tasks NIST with the responsibility for standards and guidelines. This includes development of the standards to be used by all federal agencies to categorize all information and information systems collected or maintained by each agency. This is based on the objectives of providing appropriate levels of information assurance according to a range of risk levels and guidelines to recommend the types of information and information systems that should be included in each category

h. Federal Information Security Management Act of 2002 (FISMA)

FISMA directs federal agency heads and their Chief Information Officers (CIOs) to ensure that there is an information security program in place as well as trained personnel to administer the program. A great emphasis is placed on fully integrating

security into the existing and future business processes. Each management official, typically referred to as the Designated Approval Authority (DAA), is required to authorize each system for operation with a formal certification and accreditation (C&A) process. The certification and accreditation process is required on all federal information systems. This process is intended to ensure that the appropriate security controls are implemented and are operating as intended. FISMA further requires that agency systems be certified and accredited to continue IT operations, which includes those federal systems subject to HIPAA compliance.

Agency heads are responsible for providing information security protections regarding the magnitude and risk of harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of data or information systems. Requirements include periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, performed with a frequency depending on risk, but no less than annually, to ensure that they are effectively implemented. These procedures are required for detecting, reporting, and responding to security incidents, and are consistent with standards and guidelines, including the mitigation of risks associated with such incidents before substantial damage occurs.

2. DoD Requirements

a. DoD 5200.28-STD - Department Of Defense Trusted Computer System Evaluation Criteria.

The DoD 5200.28-STD, paragraph 2.2.3.2.1 directs department heads to test security protection mechanisms to confirm they work as claimed in the system documentation and to search for obvious flaws that would allow the bypass of security mechanisms, permit a violation of resource isolation, and allow unauthorized access to the audit or authentication data

b. DoD Instruction 8500.2 – Information Assurance (IA) Implementation

DoD Instruction 8500.2, paragraph E3.3.10. requires each DoD component's information assurance (IA) program to regularly and systematically assess their IA posture with regard to DoD component-level information systems, and the DoD component-wide IA services and supporting infrastructures via combinations of self-

assessments, independent assessments and audits, formal testing and certification activities, host and network vulnerability testing, as well as IA program reviews.

3. Command Requirements

a. Military Health System (MHS) Information Assurance (IA) Policy/Guidance Manual

The provisions of this policy apply to all MHS components, military personnel, DoD civilians, and contractors, who manage, design, develop, operate, or access DoD information systems, and the TRICARE Management Activity (TMA)–developed and operated information systems, or access DoD data. MHS Components include: Service Medical Departments, TMA Directors, TMA Centrally Managed Systems, and TRICARE contractors.

Risk assessments are to be conducted whenever significant and major changes occur or when new threats are identified to the DoD IS or the IS operating environment. MHS Components are directed to attempt to exploit network security vulnerabilities using penetration testing during the C&A process, or more frequently as required by the MHS IA Program Office. Penetration tests on DOD information systems will be conducted by the MHS IA Program Office, in coordination with the appropriate Service, to verify the adequacy of security countermeasures in place.

Vulnerability Assessments performed on MHS Components will identify system and network vulnerabilities through use of vulnerability assessment tools. Vulnerability assessments are to be conducted on the network and critical servers and systems at least annually. Additionally, the Systems Administrator (SA) and the Information Systems Security Officer (ISSO) obtain and run vulnerability assessment software on automated information systems and networks monthly.

The MHS Components will incorporate a comprehensive process to audit, detect, isolate, and react to intrusions, service disruptions, and incidents that threaten the security of operations. Individual sites are required to review audit records for DOD information systems on a monthly basis or more frequently when deemed necessary. Continuous security monitoring will be performed within each MHS Component. The information system owners will ensure the information systems they are responsible for

are regularly monitored, that system records are reviewed on a weekly basis, and that all DOD information systems are protected by Intrusion Detection Systems (IDS).

b. Bureau of Medicine and Surgery (BUMED) Information Assurance Information Systems Security Policy Manual

A primary function of the Bureau of Medicine and Surgery (BUMED) is to ensure the National Command Authority has a healthy fighting force with a supporting combat-ready health care system. The inherent sensitivity of the BUMED healthcare information systems is ascertained by the concerns for individual privacy and the integrity of the personal and medical information processed, as well as the availability of the information systems that support the Navy's health care programs.

The BUMED Information Systems Security Program was implemented to ensure required protective measures are implemented to protect BUMED information systems against unauthorized modification, disclosure, destruction, and denial of service throughout all system life cycle phases. The document establishes the security policy for protecting the data, services, and resources related to development, maintenance and operations involving the systems and networks in Claimancy 18 activities, which are comprised of approximately 400 commands. Each system's level of security must protect the confidentiality, integrity, and availability of the information. Specifically, the document requires that each system undergoes periodic monitoring to test for known operating system vulnerabilities. It further recommends that every open port should be associated with a known application and that all other should be terminated and that regular monitoring of system logs for suspicious activity should be conducted. Finally, the policy recommends the use of available tools to periodically audit systems, especially servers, to ensure that there have been no unauthorized or unknown changes to the file system, registry, or user account database.

4. Comparative Summary of Information Assurance Policies

Table 4 below shows a comparison of the information assurance policies described above. The Vulnerability Scanning Requirements column indicates how often vulnerability assessments are required, at a minimum. Per the background information reviewed in this chapter, none of the minimum requirements are sufficient in today's networked computing environment, as the window between new threats decreases.

Policy	Vulnerability Scanning Requirement	Valid in Current Operating Environment
<u>Federal</u>		
Computer Act of 1987	None	No
Privacy Act of 1974	None	No
HIPAA	Periodic	No
FISMA	Annually	No
OMB Circular A-130	None	No
PDD 63	Frequently	No
<u>DoD</u>		
DoD 8500.2	Regularly	No
<u>Organizational</u>		
MHS	Monthly	No
BUMED	Periodically	No

Table 2. Comparative Summary of Information Assurance Policies

After a thorough review of the aforementioned policies and directives, it can be concluded that the MHS policy is the most stringent attempt made to require Naval Medicine activities to properly address or meet the current information assurance threats. The overarching policies are vague at best and should be revised as soon as feasible. Retired Vice Admiral Arthur Cebrowski, Director of Force Transformation for the Office of the Secretary of Defense stated that “...trends, which futurists call ‘perfectly predictable surprises’ – when the rate of transactions exceeds the resources, then policy will change – are already showing, and aiming toward networks and networking behavior”(Roosevelt, 2004). As task loads continue to increase, IT managers will have to voice their concerns about the technical issues confronting them. Alerting policy

makers, managers and strategists are parts of the solution (Azari, 2003). Without the awareness of an ever-increasing responsibility, management may never know what is required. MHS and will and can assist in evaluating network security assessments, but coordinating and scheduling full scale network security audits may take some time as the technical experts on staff to perform such task is limited in number.

I. DEFENDING YOUR INFORMATION ASSETS

1. Awareness Training

a. Continuing Education

Continuing education is a must in information technology. New systems hardware, software, user features and enhanced capabilities continue to alter our connected world, and technology continues to push the boundaries of physics and space. Continuing education does not necessarily mean that increases in training budgets are required. There are a number of free vendor seminars and publications that yield significant amounts of information security-related training. John Saunders has provided an excellent Web page at <http://www.johnsaunders.com/security.htm> that maintains a plethora of information security topics. Table 3 displays the key categories found on that page.

Computer Security Links (as of May 2004)					
Antivirus	Attacks & Vulnerabilities	Assessment	Biometrics	Cryptography	Education
Firewalls	Forensics	"Free" Items	Incident Reporting	Intrusion Detection	Laws
Miscellaneous	Network Penetration Testing	Online Publications	Operating System, Web Server & Router Security	Organizations & Certification	Oversight-Federal
Public Key Infrastructure	Research & University	Risk Management	Virtual Private Networks	Wireless Access and Security	Other General Security Links

Table 3. Computer Security Links

Federal Computer Weekly often has current IT news and trends that are relative to the U. S. Federal Government. Although the title is misleading, this resource is a commercial entity. URL: <http://www.fcw.com/links/legislation/techleg.asp>

The U.S. Government also hosts many helpful links. The following are among the more prevalent resource materials available online.

The National Institute of Standards and Technology (URL: <http://www.nist.gov/>) is a repository of laws, statutes, acts, Executive Orders, and multiple policies concerning information technology issues relevant to the federal government.

The Office of Homeland Security, The White House (URL: <http://www.whitehouse.gov/homeland>) is the newest department in the Executive Branch that possesses the teeth to affect information technology components and processes.

The Sixty-Minute Network Security Guide (First Steps Toward a Secure Network Environment) was published by the Systems and Network Attack Center (SNAC) of the National Security Agency. An E-mail request should be sent to SNAC.Guides@nsa.gov for the current URL of this valuable tool.

The Defense Information Systems Agency is another valuable site that should not be overlooked. The Information Support Environment link <http://iase.disa.mil/eta/> provides free video and training/tutorial CDs on some of the hottest topics in information security today. The information assurance videos are great for the required annual information security refresher training.

A number of other informative sites are available for researching vulnerabilities and threats that have been identified for specific systems and services. They can be reviewed at the following sites:

- Security Focus www.securityfocus.com
- Incidents.org www.incidents.org
- InfoSysSec www.infosyssec.com
- Packet Storm www.packetstormsecurity.org

b. Annual Training

Annual training is a reminder to all organizational personnel that security is an individual responsibility. Not all personnel are security engineers, but the basics should always be included in such training. This include, but are not limited to social engineering methods, which remains one of the most effective methods that attackers utilize to gain access to an organization's information assets; password management,

locking system desktops, reporting suspicious activity or system files including unsolicited email attachments.

c. Professional Training

Professional training is not for everyone, but a number of organizations provide information security training programs and certifications. Some are vendor-specific and others operate as a non-profit organization. Most professional certifications require a test and/or practical demonstration of knowledge in a wide range of domain-specific areas of information security. Some of the most recognized security certifications are:

Certified Information Systems Security Professional (CISSP) – Visit <http://www.isc2.org> for additional information.

System Administration, Networking, and Security (SANS) – Visit <http://www.sans.org/> for additional information.

Vendor-specific:

Cisco certifications are organized in 3 major categories; Associate, Professional, and Expert levels of expertise. Visit <http://cisco.netacad.net/public/> for additional information.

Microsoft Certifications are arranged for systems administrators, application developers, solutions developers, systems engineers, and database administrators. Additional details can be found at Microsoft's Web site, located at <http://www.microsoft.com/education/msitacademy/WorldWide/Default.aspx> .

d. Experience-based

Education can only be supplemented by time and experience. Although experienced security personnel have existing certifications, continued training is required to expand their knowledge base current. More experienced personnel should be scheduled for advanced training whenever feasible.

2. Vulnerability Assessments

a. Purpose

Vulnerability assessments are an effective way to identify potential vulnerabilities in a system or network. These exercises of security evaluation usually employ common attack methods that an adversary may use in an attempt to access information systems of interest. These methods may range from a simple IP scan to identifying resources that utilize services with known vulnerabilities or unpatched systems for future exploits. The end goal of vulnerability assessments is to report system weaknesses to the owner for resolution or to the attacker for a future exploit.

Vulnerability assessments are performed for a number of reasons, but they are not considered a simple task and usually require special knowledge to perform. Fears of corrupting or breaking existing systems are generally the reason they are not a standard inter-organizational practice. They are normally composed of multiple rather than one aggressive attack methods and when they are performed, it is done when activity periods are slow as the networked systems or the network as a whole can be disabled during the process. Vulnerability assessments are often performed during certification and accreditation assessments or whenever a test of organizational intrusion detection and response capabilities are desired.

b. External

External vulnerability assessments originate from the platform on which a true adversary would likely attack from. This type of attack tests the abilities of the firewall and router filtering capabilities, all the systems that are accessible from the outside, such as web and mail servers, as well as gateway-specific controls that may assist to block such attempts. These types of tests are seldom performed due to the complexity and legal situations that may arise from such vulnerability assessments, especially in DoD networks, where other entities outside of the organization may be monitoring network activities. External attack scenarios take a considerable amount of coordination by all parties concerned.

c. Internal

Internal vulnerability assessments are better managed within specified boundaries of the network. These attacks can be directed at a network segment more easily and consume less resources in the process. Tests of network segments are less costly, more controlled, and safer to perform in regards to network stability.

d. Network Surveys

Network surveys promote a more comprehensive method of testing the overall security posture of a network. These foot printing and scanning exercises provide an insight to determining which resources are available for testing purposes. Mapping or surveying most generally yields domain names, server names, Internet service provider information, Internet protocol (IP) addresses of individual hosts, and their interconnecting devices. The Nmap tool is very effective for this type of discovery. Nmap can differentiate which operating systems are running on a network as well as the types of packet filters or firewalls are in use. Additional details can be found by visiting the Nmap hyperlink posted in Table 7.

e. Limitations of Vulnerability Assessments

If vulnerability assessments are going to be initiated to simulate a real attack, they should be conducted as "black box" exercises. In a real attack, the attacking agent would not normally possess intimate information about the system being tested. Knowing about the system specifics would actually invalidate the test before it could begin. It is easy to imagine that an attacker already knowing administrator passwords and how your network was configured would not really be testing anything except for their personal skills. A simulated attack will only identify the problems that it is designed to look for. If the tools are not configured to seek a system feature or service, it will not produce any information about its level of security or insecurity. It is also important to remember that vulnerability assessments would seldom, if ever, provide information about vulnerabilities that have not yet been discovered and well documented within the security community (one must know the "signature" of what they are looking for... few, if any, heuristic tools are available in this area). Furthermore, if there are no instances where vulnerabilities are identified after the vulnerability assessment is complete, it does

not necessarily mean that a network is secure. Assessments are a “snap-shot” in time, and can become obsolete within days as new vulnerabilities are discovered by information assurance professionals. If vulnerabilities are discovered, as they often are, it is imperative that the corrective configuration settings and or patches are applied as soon as possible. The effort required to remediate vulnerabilities can be quite substantial. More often than not, a vulnerability report collects dust before corrective actions are implemented, which often means that more vulnerabilities have likely been reported and the system will not be any more secure after the earlier noted changes are applied. It must be remembered that one vulnerable platform is all that an attacker needs to influence a network operating environment.

f. Unexpected Consequences Derived From Testing

Vulnerability assessments can have serious consequences for the network on which they are run. If badly conducted it can cause congestion and systems crashing. It is, therefore, vital to have consent from the management of an organization before conducting vulnerability assessments on its systems or network. If the issue of timing is not resolved properly, it could be catastrophic to an organization. Imagine conducting a denial-of-service ‘test’ on a university on the day its students take their online examinations. This is an example of poor timing as well as lack of communication between the vulnerability assessors and the university. Good planning and preparation will help avoid such bad practices.

3. Automated Tools

a. DoD Approved

Government off-the-shelf (GOTS) vulnerability scanning software is available from the Defense Information Systems Agency (DISA) at no cost to all government agencies. There are two versions of Security Profile Inspector (SPI), for Windows NT (SPI-NT) operating systems and for Unix Networks (SPI-NET). Both versions can be retrieved from: http://www.cert.mil/resources/security_tools.htm

The Department of Homeland Security (DHS) offers another no-cost service to federal agencies. Patch Authentication and Dissemination Capability (PADC) is a service that allows agencies to retrieve information on trusted and authenticated

patches for their specific operating systems. Subscriptions must be requested from the DHS's Federal Computer Incident Response Center (FedCIRC). Of the 2000 accounts available, only 47 agencies had active subscriptions as of 10 September 2003. Other patch management solutions may offer expanded capabilities, but they are not free of charge.

b. Non-DoD Approved

A recent study published on 26 June 2003 by Kevin Novak provides a great level of detail in regards to vulnerability assessment scanners. The study examined 11 of the most prevalent vulnerability assessment scanners on the market. The features, capabilities, company information, and costs associated with those systems are listed in Tables 4 through 6.

Vulnerability-Assessment Tools VENDORS AT A GLANCE

PUBLIC COMPANIES

Company name (stock symbol)	Year founded	Product name	Product launched	Market capitalization as of June 3 \$000	Current assets \$000	Current liabilities \$000	Revenue most recent quarter \$000	Revenue year earlier \$000	Net income (loss) \$000	R&D spending \$000	Key customers
BINDVIEW DEVELOPMENT CORP. (BVEW)	1990	by-Control for Internet Security 7.2	1999	59,200	46,319	21,654	13,047	16,805	(2,701)	4,235	City of St. Petersburg, Fla., EMC
HARRIS CORP. (HRS)	1895	STAT Scanner Professional Edition 5	1998	2,024,000	1,325,600	457,800	538,900	483,300	22,600	N/A	Navy/Marine Corps Intranet (NMCI), U.S. Army, U.S. Veterans Administration

Sources: SEC filings, company reports, Yahoo, Hoovers.com

PRIVATE COMPANIES

Company name	Year founded	Product name	Product launched	Employees	Key customers
BEYOND SECURITY	1999	Automated Scanning Server 1.5	2001	30	Aladdin Knowledge Systems, EAI, IBM, ICQ, MSN (Microsoft Network), Smartteam solutions
eEYE DIGITAL SECURITY	1999	Retina Network Security Scanner 4.9	1999	80	Bank of Montreal, Precision Computer Systems, SI International, Watson Wyatt Worldwide
FOUNDSTONE	1999	Foundstone Enterprise Software 2.6	2002	123	Ingram Micro, Motorola, U.S. Department of Transportation
NCIRCLE NETWORK SECURITY	1998	IP360 Vulnerability Management System 5.3	2001	60	Archer Daniels Midland, Bechtel, Patenco Credit Union, Visa
QUALYS	1999	QualysGuard	2000	100	ABN AMRO, Adobe Systems, Apple Computer, AXA, Bank of the West, BASF, BlueCross BlueShield, Cartier, Cedars-Sinai Medical Center, Fireman's Fund, Hewlett-Packard, RR Donnelley, The Thomson Corp., TIAA-CREF
RAPID7	2000	NeXpose 3.0	2001	10	Not disclosed
SAINT CORP.	1998	SAINT 4.3	1998	50	ATI Technologies, Oregon State University, U.S. Naval War College
TENABLE NETWORK SECURITY	2002	Tenable Nessus Appliance 1.0	2003	8	Not disclosed
VIGILANTE.COM	1997	SecureScan NX 2.6.50	2001	55	Not disclosed

Source: Company reports

Table 4. Vulnerability-Assessment Tools: Vendors at a Glance

From <http://www.nwc.com/1412/1412f2.html>

Vulnerability-Assessment Tool Features											
	Beyond Security Automated Scanning Server 1.4	BindView by-Control for Internet Security 7.2	eEye Digital Security Retina Network Security Scanner	Foundstone Enterprise with FoundScan Engine 2.6	Harris STAT Scanner Professional Edition 5	nCircle Network Security Vulnerability Management System 3.3	Qualys QualysGuard and Intrastat Scanner 1.9	Replix NoXpose 3.0	SAINT 4.3	Tenable Network Security Tenable Nessus Appliance 1.0 with Tenable Lightning 1.1	Vigilante.com SecureScan NX 2.6.50
Management											
Sets company policy	N	Y	N	N	Y	Limited	N	Limited	N	N	N
Remediation ability	N	Partial	Y	N	Partial	N	N	N	N	N	N
Runs safe/immediate scans	Y/Y	Y/Y	Y/Y	Y/Y	Y/Y	Y/N	Y/Y	Y/Y	Y/Y	Y/Y	Y/Y
Secure remote interface	Y	Y (MMC)	Y	Y	Y	Y	Y	Y	Y (HTTPS)	Y	N
Creates users and sets privileges	N	Y	Y	Y	N	Y	Y	Y	Y	Y	N
Issues tickets/displays scan status	N/partially	N/Y	Y/Y	Y/Y	N/Y	Y	N/partially	N/Y	N/Y	Partially/partially	N/Y
Scans can be scheduled	Y	Y	Y	Y	Y (CLI)	N	Y	Y	Y	Y	Y
Definable time window for scans	N	N	N	Y	Partial	N	Y	N	N	Y	N
Can interact with system during scans	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Can pause scans	N	Y	N	Y	N	N	N	N	N	Y	N
Runs multiple concurrent sessions	Y	Y	Y	Y	N	Y	Y	Y	N	Y	N
Notification methods	E-mail	None	None	E-mail, Ticket system	E-mail	SMTP, SNMP	E-mail	E-mail, SNMP, Syslog	None	E-mail	E-mail
Secure notification	Y	N/A	N/A	N	N	Y	Y	N	N/A	Through e-mail daemon	N
Tunes performance settings	N	N	Y	Y	Y	Y	Y	Y	Y	Y	N
Supports multiple organizations/divisions	N	N	Y	Y	N	Y	Y	Partially	N	Y	N
Reporting											
Numerical representation of vulnerability	N	N	N	Y	N	Y	Y	Y	N	Partial	N
Assets can be assigned a risk level	N	N	N	N	N	N	N	N	N	N	N
Asset information can be added	N	N	N	Y	N	N	Y	N	N	Y	N
Trending	Y	N	Y	Y	Y	N	Y	Y	Y	Y	Y
Exportable formats	XML, e-mail	None	HTML	HTML, XML	CSV, PDF, XML, TML, Excel, Word, RTF, text	CSV, PDF, XML	HTML, XML, MHT	HTML, XML, database export, RTF	HTML text, tab/comm separated	PDF	HTML, PDF
Auto vulnerability database update	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	N
Alerting/customizable reporting	N/N	N/N	Y/Y	Y/Y	N/Y	Y/N	Y/Y	Y/Y	None/Y	N/N	N/N
Views can be adjusted/re-sorted	N	N	N	Y	Y	Y	Y	Y	N	N	N
Vulnerabilities											
References common vulnerability databases	Minimally	Minimally	Y	Y	Y	Y	Y	Y	Y	Y	Y
Includes scans for wireless vulnerabilities	N	N	Y	Y	N	Y	Y	N	N	Y	N
Authenticates to target	Y	Y	Y	N	Y	N	N	Y	Y	Windows Auth.	N
Customizable vulnerabilities	N	N	Y	Y	N	Y	N	N	Y	Y	N
SANS top 20 check	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
General											
Platforms	Appliance only	Windows	Windows	Windows	Windows	Appliance	Appliance only	Windows, Linux, Solaris	Linux	Linux	Windows
Manages multiple scanners	Y	N	N	Y	N	Y	Y	N	N	Y	Y
Integrates with other security tools	N	Y (by-Control products)	Y (eEye product line)	Arcsight, Citadei	Y	Check Point and other nCircle products	Multiple	N	Riskwatch	IDS, Snort, Dragon, RealSecure, Bro using Lightning	N
Yes, No											

Table 5. Vulnerability-Assessment Tool Features.

From <http://www.nwc.com/1412/1412f22.html>

REPORT CARD

Vulnerability-Assessment Tools

	Foundstone Enterprise with FoundScan Engine 2.6	QualysGuard Intranet and Scanner 1.9	Harris STAT Scanner Professional Edition 5	eEye Digital Security Retina Network Security Scanner 4.9	Vigilante.com SecureScan NX 2.6.50	SAINT 4.3	nCircle Network Security IP360 Vulnerability Management System 5.3	Tenable Network Security Tenable Nessus Appliance 1.0 with Tenable Lightning 1.1	BlindView hv-Control for Internet Security 7.2	Rapid7 Nexpose 3.0	Beyond Security Automated Scanning Server 1.4
REPORTING (3%)											
FINDINGS EASILY SORTABLE (12%)	3.5	4	3	3	3	2	3	2	3	2	1
DOCUMENTATION ON FIXES (12%)	4	3	4	3	3	3	3	3	3	3	2
EXPORT CAPABILITIES (4%)	3	2	2	2	3	2	3	1	2.5	5	1
TRENDING CAPABILITIES (3%)	4	4	3	4	3	3	4	3	3	3	0
PERFORMANCE AND SCALABILITY (30%)											
RELIABILITY (10%)	3.5	4	4	3	2	3	3	4	4	2	1
DETECTION ACCURACY (8%)	4	4	4	4	4	4	4	4	4	4	4
NONINTRUSIVENESS (8%)	3	2	3	3	2	3	3	2	3	3	3
SPEED (4%)	4	4	3.5	4	3	3	2	4	3	2	1
COVERAGE/SCOPE (17%)											
CRITICAL CHECK COVERAGE (12%)	3	3.5	4.5	3.5	4	4.5	3	4	1	2	2
TOTAL COVERAGE (5%)	3	3.5	4.5	3.5	4	4.5	3	4	1	2	2
MANAGEMENT (12%)											
AUToupdate CAPABLE (3%)	4	5	1	5	3	2	3	5	2	2	5
CONFIGURATION (3%)	5	4	3	3	5	3	4	3	5	5	2
INSTALLATION AND CONFIGURATION (3%)	5	5	0	4	0	0	4	2	2	3	0
TIERED USER AUTHENTICATION (3%)	4	5	4	3	4	3	3	3	3	4	3
PRICE (10%)	4	3	4	4	4	4	3	2.5*	4	2	1
TOTAL SCORE (100%)	3.66	3.55	3.52	3.39	3.17	3.16	3.13	3.09	2.92	2.69	1.84
A>4.3, B>3.5, C>2.5, D>1.5, F<1.5 A-C GRADES INCLUDE + OR - IN THEIR RANGES. TOTAL SCORES AND WEIGHTED SCORES ARE BASED ON A SCALE OF 0-5.											
*TENABLE'S NISSUS APPLIANCE 1.0 IS NOT REQUIRED TO RUN TENABLE LIGHTNING 1.1.											
Customize the results of this report card using the Interactive Report Card [®] , a Java applet at www.nwc.com .											

Table 6. Vulnerability-Assessment Tools: Report Card.

<http://www.nwc.com/1412/1412f213.html>

c. Vulnerability Assessment Tools

There are a great number of other tools available that are designed to automatically discover vulnerabilities. Nessus is a scanning utility that remains a favorite among attackers and can be found at <http://www.nessus.org>. Nessus possesses the capability of remotely auditing a network and reporting the existing vulnerabilities. A short abbreviated list of other commonly used tools with a brief description of their capabilities is provided below.

1) Information Gathering Tools:

- Nmap – Network and port scanner with operating system discover
- Hping – Port scanning tool
- Netcat – Obtains service banners and versions
- Firewalk – Useful for determining a firewall access control list (ACL)
- Ethereal – Useful for monitoring and logging traffic returning from maps and scans
- Icmpquery – Used to determine target systems time and network mask used to hide real addresses
- Strobe – A useful port scanning utility
- Superscan – A Windows port scanning tool
- RPCDump- Command line tool that performs queries on Remote Procedure Call (RPC) endpoints
- Netstat – Shows active TCP connections, open ports, Ethernet statistics, and the IP routing table

The Foundstone Company is another free defense resource site that also offers a comprehensive list of tools for security risk management and vulnerability assessments. The tools offered freely to the public are the ones used in the field by its consultants. Visit them at <http://www.foundstone.com/> and click the resources link to view the available tools.

Another type or method of vulnerability assessment involves password breaking, also referred to as password cracking. Again, these are automated tools that are simple to use and are limited only by processing power. Even on standard use personal computers, a password cracking utility can process more than 100,000 guesses per second. One of these utilities is especially effective against passwords required for remote access systems allowing Telnet and FTP transfers, since it does not require the

password file off a computer, as do the first three mentioned below. The following lists a few of the password cracking methods and tools used today.

- Dictionary Attack – Uses a word list or dictionary file and can be modified to incorporate multiple languages. One standard dictionary attack takes a few minutes to test every word. It is a fast method that is often very effective where password policies are not enforced.
- Hybrid Crack - Tests for passwords that are variations of the words in a dictionary file. It consumes more time, but yields more results.
- Brute Force – This method uses a variety of tests for passwords that are made up of characters and numbers by performing every combination possible. This method is most effective and will break anything given enough time, time being the key ingredient. A password of eight characters or more could take from days to millions of years to crack.
- Brutus- This tool is used to automatically crack telnet and ftp accounts. Fast, effective method to demonstrate to management why those types of remote access are not a novel idea any longer. Brutus is not included in Table 4, but is available at <http://www.hoobie.net/brutus>

Please refer to Table 7 for additional tools that grant access and escalation of privilege. L0phtcrack and John the Ripper are two of the most appropriate tools for password cracking.

d. Tools and Information Available to the General Public

Table 7 is a brief compilation of tools available to network defenders and attackers to determine where an organization's strength and weaknesses are, created by the authors of the "*Hacking Exposed*" series of books.

General Security Tool Sites

Hackersclub	http://www.hackersclub.com
NewOrder	http://neworder.box.sk
Security-Focus	http://www.securityfocus.com
Technotronic	http://www.technotronic.com

Countermeasure Tools

BlackICE by NetworkICE	http://www.networkice.com
CyberCop Monitor by Network	http://www.nai.com

Associates Inc.	
Hidden Object Locator	http://www.netwarefiles.com/utils/hobjloc.zip
Ippl	http://www.via.ecp.fr/~hugo/ippl/
ITA from Axent	http://www.axent.com
Kane Security Monitor	http://www.intrusion.com
Netguard	http://www.Genocide2600.com/~tattooman/unix-loggers/netguard-1.0.0.tar.gz
Network Flight Recorder	http://www.nfr.net
Perro (formerly Protolog)	http://www.grigna.com/diego/linux/protolog/index.html
Psionic Portsentry from the Abacus project	http://www.psionic.com/abacus/
RealSecure by Internet Security Systems (ISS)	http://www.iss.net
Scanlogd	http://www.openwall.com/scanlogd/
Secured by Memco	http://www.memco.com
Secure Shell (SSH)	http://www.ssh.fi http://www.f-secure.com
SessionWall-3 by Abirnet/Platinum Technology	http://www.abirnet.com

Denial of Service

Land and Latierra	http://www.rootshell.com/archive-j457nxiqi3gg59dv/199711/land.c.html http://www.rootshell.com/archive-j457nxiqi3gg59dv/199711/latierra.c.html
Portfuck	http://www.stargazer.net/~flatline/filez/portfuck.zip
Smurf & Fraggle	http://www.rootshell.com/archive-j457nxiqi3gg59dv/199710/smurf.c.html http://www.rootshell.com/archive-j457nxiqi3gg59dv/199803/fraggle.c.html
Synk4	http://www.jabukie.com/Unix_Sourcez/synk4.c

Teardrop, newtear, bonk, syndrop	http://www.rootshell.com/archive-j457nxiqi3gg59dv/199711/teardrop.c.html http://www.rootshell.com/archive-j457nxiqi3gg59dv/199801/newtear.c.html http://www.rootshell.com/archive-j457nxiqi3gg59dv/199801/bonk.c.html http://www.rootshell.com/archive-j457nxiqi3gg59dv/199804/syndrop.c.html
--	--

Enumeration Tools

Bindery	http://www.nmrc.org/files/netware/bindery.zip
Bindin	ftp://ftp.edv-himmelbauer.co.at/Novell.3x/TESTPROG/BINDIN.EXE
Epdump	http://www.ntshop.net/security/tools/def.htm
Finger	ftp://ftp.cdrom.com/.1/novell/finger.zip
Legion	ftp://ftp.technotronic.com/rhino9-products/legion.zip
NDSsnoop	ftp://ftp.iae.univ-poitiers.fr/pc/netware/UTIL/ndsnoop.exe
NetBios Auditing Tool (NAT)	ftp://ftp.technotronic.com/microsoft/nat10bin.zip
Netcat by Hobbit	http://www.l0pht.com/~weld/netcat/
Netviewx	http://www.ibt.ku.dk/jesper/NTtools/
Nslist	http://www.nmrc.org/files/snetware/nut18.zip
On-Site Admin	ftp://ftp.cdrom.com/.1/novell/onsite.zip
Snlist	ftp://ftp.it.ru/pub/netware/util/NetWare4.Toos/snlist.exe
Somarsoft (dumpacl, dumpreg, etc.)	http://38.15.19.115/
user2sid and sid2user	http://www.chem.msu.su:8080/~rudnyi/NT/sid.txt
Userdump	ftp://ftp.cdrom.com/.1/novell/userdump.zip
Userinfo	ftp://ftp.cdrom.com/.1/novell/userinfo.zip

Footprinting Tools

ARIN database	http://www.arin.net/whois/
Cyberarmy	http://www.cyberarmy.com
Dogpile (meta search engine)	http://www.dogpile.com
DomTools (axfr)	http://www.domtools.com/pub/domtools1.4.0.tar.gz

Ferretsoft	http://www.ferretsoft.com
Sam Spade	http://www.samspace.org
Securities and Exchange Commission (SEC)	http://www.sec.gov/
USENET Searching	http://www.deja.com http://www.dogpile.com
VisualRoute	http://www.visualroute.com
WHOIS database	http://www.networksolutions.com
WS_ Ping Pack Pro	http://www.ipswitch.com

Gaining Access

L0phtcrack's Readsmb	http://www.l0pht.com/
Legion	http://www.rhino9.com
NetBios Auditing Tool (NAT)	ftp://ftp.technotronic.com/microsoft/nat10bin.zip
Nwpcrack	http://www.nmrc.org/files/netware/nwpcrack.zip
SMBgrind by NAI	Included with CyberCop Scanner from Network Associates (http://www.nai.com)
Sniffit	http://newdata.box.sk/neworder/a/sniffit.0.3.2.tar.gz
SNMPsniff	http://www.AntiCode.com/archives/network-sniffers/snmpsniff-1_0.tgz
THC login/telnet	http://thc.pimmel.com/files/thc/thc-lh11.zip

Privilege Escalation and Back Door Tools

Elitewrap	http://www.multimania.com/trojanbuster/elite.zip
Getadmin	http://www.ntsecurity.net/security/getadmin.htm
Hunt	http://www.cri.cz/kra/index.html#HUNT
Imp	http://www.wastelands.gen.nz/
Invisible Keystroke Logger	http://www.amecisco.com/iksnt.htm
Jcmd	http://www.jrbsoftware.com

John the Ripper	http://www.openwall.com/john/
Netbus	http://www.netbus.org
Netcat	http://www.l0pht.com/netcat
NTFSDOS	http://www.sysinternals.com
NTuser	http://www.pedestalsoftware.com
Pandora by NMRC	http://www.nmrc.org/pandora/download.html
Pwdump2	http://www.Webspan.net/~tas/pwdump2/
Revelation by Snadboy	http://www.snadboy.com
Sechole	http://www.ntsecurity.net/security/sechole.htm
SNMPsniff	http://packetstorm.harvard.edu/sniffers/snmpsniff-1.0.tar.gz
Unhide	http://www.Webdon.com
Virtual Network Computing (VNC)	http://www.uk.research.att.com/vnc

Pilfering

File Wrangler	http://www.tucows.com
PowerDesk's ExplorerPlus	http://www.mijenix.com/powerdesk98.asp
Revelation	http://www.snadboy.com

Rootkits and Cover Tracks

Cygwin Win32 (cp and touch commands)	http://www.cygnus.com
Wipe	ftp://ftp.technotronic.com/unix/log-tools/wipe-1.00.tgz
Zap	ftp://ftp.technotronic.com/unix/log-tools/zap.c

Scanning Tools

BindView	http://www.bindview.com
Chknull	http://www.nmrc.org/files/netware/chknull.zip
CyberCop Scanner by NAI	http://www.nai.com

Firewalk	http://www.packetfactory.net/firewalk/
Fping	http://packetstorm.harvard.edu/
HackerShield by Bindview	http://www.bindview.com/netect
Hping	http://www.kyuzz.org/antirez/
InspectorScan by Shavlik	http://www.shavlik.com
Internet Scanner by ISS	http://www.iss.net
Kane Security Analyst	http://www.intrusion.com
Network Mapper (Nmap)	http://www.insecure.org/nmap
NTInfoscan	http://www.infowar.co.uk/mnemonix/
Pinger	ftp://ftp.technotronic.com/rhino9-products/pinger.zip
Scan	http://www.prosolve.com
Solarwinds	http://www.solarwinds.net
Strobe	http://www.hack-net.com/cgi-bin/download.cgi?strobe-1_03.tgz
Udpscan	ftp://ftp.technotronic.com/unix/network-scanners/udpscan.c
WebTrends Security Analyzer by WebTrends	http://www.Webtrends.com
WS_Ping Pack Pro	http://www.ipswitch.com

War Dialing Tools

PhoneSweep by Sandstorm	http://www.sandstorm.net
THC	http://www.infowar.co.uk/thc/
ToneLoc	http://www.hackersclub.com/km/files/pfiles/Tl110.zip

Table 7. Network Defense and Attack Tools and Links

From <http://www.hackingexposed.com/tools/tools.html>.

4. Proactive Measures

a. Systems Configuration

Vulnerability scanners will alert system owners of potential weaknesses within their information system, but maintaining the appropriate systems configuration

alleviates many of the vulnerabilities found in unmanaged systems. Applications and services required to operate the system should be evaluated to determine which ports and protocols are required for functionality. All unused ports and services should be terminated. Many of the findings that are derived from vulnerability assessments address unnecessary open port and service issues. The majority of applications and operating systems on the market today are loaded with default settings focused on providing the customer with all available services included in the software. Many of those services installed by default are never required and place the system at a higher level of risk as soon as it is connected to the Internet.

NIST has produced a number of Special Publications to assist in information assurance tasks. The following table is referenced in the draft version of NIST SP 800-66, An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. This is a great resource in its entirety. Appendix E has an extensive HIPAA Security Rule/FISMA requirements crosswalk table that breaks down every element required for compliance with the federal mandates. See Table 8 for a quick review of what NIST has to offer.

NIST Publication	Title
FIPS 140-2	<i>Security Requirements for Cryptographic Modules</i>
FIPS 199	<i>Standards for Security Categorization of Federal Information and Information Systems</i>
NIST SP 800-12	<i>An Introduction to Computer Security: The NIST Handbook</i>
NIST SP 800-14	<i>Generally Accepted Principles and Practices for Securing Information Technology Systems</i>
NIST SP 800-16	<i>Information Technology Security Training Requirements: A Role- And Performance-Based Model</i>
NIST SP 800-18	<i>Guide for Developing Security Plans for Information Technology Systems</i>
NIST SP 800-26	<i>Security Self-Assessment Guide for Information Technology Systems</i>
NIST SP 800-27	<i>Engineering Principles for Information Technology Security (A Baseline for Achieving Security)</i>
NIST SP 800-30	<i>Risk Management Guide for Information Technology Systems</i>

NIST SP 800-34	<i>Contingency Planning Guide for Information Technology Systems.</i>
NIST SP 800-35	<i>Guide to Information Technology Security Services</i>
NIST SP 800-36	<i>Guide to Selecting Information Security Products</i>
NIST SP 800-37	<i>Guide for the Security Certification and Accreditation of Federal Information Systems</i>
NIST SP 800-42	<i>Guideline on Network Security Testing</i>
NIST SP 800-44	<i>Guidelines on Securing Public Web Servers</i>
NIST SP 800-47	<i>Security Guide for Interconnecting Information Technology Systems</i>
NIST SP 800-50	<i>Building Information Technology Security Awareness and Training Program</i>
NIST SP 800-53	<i>Recommended Security Controls for Federal Information Systems</i>
NIST SP 800-55	<i>Security Metrics Guide for Information Technology Systems</i>
NIST SP 800-56	<i>Recommendation on Key Establishment Schemes</i>
NIST SP 800-57	<i>Recommendation on Key Management</i>
NIST SP 800-59	<i>Guideline for Identifying an Information System as a National Security System</i>
NIST SP 800-60	<i>Guide for Mapping Types of Information and Information Systems to Security Categories</i>
NIST SP 800-61	<i>Computer Security Incident Handling Guide</i>
NIST SP 800-63	<i>Recommendation for Electronic Authentication</i>
NIST SP 800-64	<i>Security Considerations in the Information System Development Life Cycle</i>

Table 8. NIST Publications Referenced in NIST SP 800-66₄

Figure 4 illustrates how the NIST publications relate to the essential elements for creating and managing an information assurance security program.

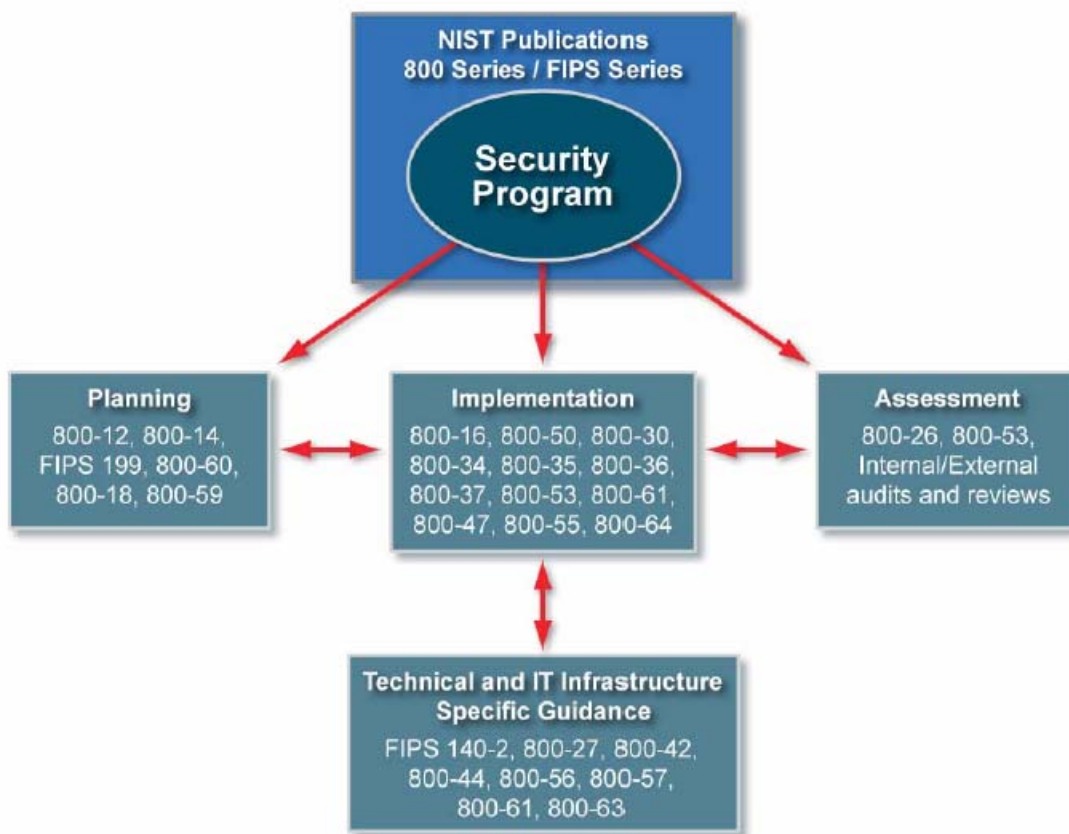


Figure 4. NIST Publications

J. POTENTIAL BENEFITS TO NAVAL MEDICINE

1. Navy Marine Corps Intranet (NMCI) Implications

a. *Maintenance for Non-Qualifying Systems*

Although the NMCI initiative will assume operations for the majority of systems with the Navy and Marine Corps, and therefore the security associated with them, some exceptions to the assumption of individual networks will occur. Many of the legacy programs will not meet the required certification and accreditation status needed to operate on the NMCI network. Until they are replaced or incorporated into other qualifying systems, the need to manage those systems vulnerabilities will remain a requirement.

2. Greater Assurance of Due Diligence in Personal Privacy Issues

Federal legislation has recently mandated that executive staff members, especially the Commanding officers of those organizations, are responsible for the safekeeping of personal data stored on information systems. Ignoring that responsibility may require that their negligence be penalized with significant fines and/or imprisonment. An effective patch management program will more likely demonstrate due diligence should a compromise occur than would having none at all.

3. Estimated Savings in Personnel Costs

Gartner group estimates that a 1000-unit server farm costs \$300,000 per year to perform patch management tasks. The same server population would cost \$50,000 to implement an automated solution (Schroder et al, 2003). This question will be covered in greater detail in Chapter V, Conclusions and Recommendations.

4. Significant Reductions in Vulnerabilities

The overall benefit derived from performing continuous vulnerability assessments across the entire network will not only alert administrators of existing weaknesses, but will save them numerous hours in reconfiguration efforts required to recover from compromised systems. When considering the legal responsibilities facing organizations in today's network-centric environment, can anyone really afford to leave their systems unprotected? According to Security Alert Consensus www.sans.org/newsletters/sac, there are approximately 1000 new operating systems and applications vulnerabilities reported each year, which is roughly 83 new vulnerabilities per month (Shipley, 2003).

III. RESEARCH METHODS

A. WORK PLAN

This project utilizes an applied research methodology, including both primary and secondary research. This research is limited to Naval Medicine personnel who are directly responsible for information systems operations.

B. SECONDARY

Secondary research was obtained from online sources, including the World Wide Web and the Dudley Knox Library archives at Naval Postgraduate School. These efforts confirm the current technologies utilized by other information-centric organizations and seek the most effective employment techniques (scheduling, automation, etc.). Interviews with industry and government information assurance professionals aid in determining a return on investment, should the recommended policies and practices be accepted.

C. PRIMARY

The primary research begins with an evaluation of the current Naval Medicine network vulnerability management policy and practices. A comparison to Federal Information Security Management Act (FISMA) and other federal/service policies is reviewed to confirm or recommend current policy modification. In addition to policy review, the information assurance (IA) methodologies suggested by NSA will be recommended, if applicable, to enhance existing IA practices. A Web-based survey seeking general information in regards to IA policy, known systems compromises, current vulnerability scanning methods, and patching practices will be posted on the Naval Medicine Intranet portal referred to as Naval Medicine Online (NMO). The results provide insight into the effects of current policy, tools and techniques used by information technology managers utilized to protect information system assets. Submitted survey responses are anonymous and solely intended to survey current policy practices, overarching policy adherence and current vulnerability assessment practices.

D. SURVEY INSTRUMENT DEVELOPMENT

The survey instrument is designed for comprehensibility to all participants while capturing the information necessary to validate or invalidate the premise: Seventy-five percent of Naval Medicine's known information systems compromises were not protected by the available vulnerability patch(es). The survey is compiled with an All-Points-Anchored response option for each of 30 questions. Response options for Questions 5 through 30 will be coded as 1 through 4 for statistical analysis. The survey development tool within the Naval Medicine Online portal will be utilized to create an HTML-based survey. A survey key, generated and delivered to each Naval Medicine CIO, ensured that only one survey was submitted by each organization. An emphasis in creating a short, easy-to-understand instrument was utilized to encourage participation and to facilitate ease in completion. Each of the 30 questions has supplemental descriptors for clarification. Additionally, each question was placed in a logical progression, while a best effort approach was made to keep response categories as close as possible to similar response categories. Respondents were instructed to select one response for each applicable question.

The survey instrument displayed four response sections in a linear table format. The first portion of the survey, Questions 1 through 4, was used for demographic analysis that included title, years of experience, size of organization and generalized geographic location.

The second area, Questions 9 through 14, inquire about information system certification and accreditation concerns, vulnerability scanning, and patch management practices. Similar surveys regarding these topics were sought during secondary research efforts, but were not available. Therefore, the survey questions were developed from a review of the literature available regarding information security, current technological advances, and interviews with Information Security professors at the Naval Postgraduate School. The response options vary somewhat, but the selection of responses are limited to four choices ranging from Yes, No, Planned, and Don't Know throughout this section.

The third section consisted of Questions 15 through 24, which seeks information regarding known system compromises, number of personnel available to perform

maintenance, and average number of hours spent performing maintenance and/ or restoration efforts. The response options vary somewhat with numerical response options that are ranges of approximation. It was perceived that an exact accounting of previous incidents may have deterred survey participation survey.

Section Four is reserved for Questions 25 through 30, separated because they yield a wide variety of response options. Further, survey respondents were cautioned regarding the dissimilarities in response options. This section seeks information regarding information asset totals, personnel strengths, and personal opinions.

Fellow students enrolled in the information security track within the Information Systems Technology curriculum at the Naval Postgraduate School were selected to edit the survey instrument before pre-testing. Afterwards, the survey was submitted for pre-testing to the Naval Postgraduate School Chief Information Officer (CIO), Chief Technology Officer (CTO), Information Systems Security Officer (ISSO), and Information Systems Security Manager (ISSM) to average the total survey participation time and to solicit any noted discrepancies or potential conflicts within the survey. Their input had a two-fold benefit: a test of the survey instrument for readability and allowance for editing without eliminating potential respondents from the pool of professionals within Naval Medicine.

Prior to distributing the survey, the NMO portal manager at Naval Medical Information Management Center, Bethesda, Maryland, was contacted to request permission to distribute the survey instrument. Once permission was received, potential respondents were contacted via the global address book on the Naval Medicine domain and asked to volunteer for the study.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. RESEARCH FINDING AND ANALYSIS

A. INTRODUCTION

The small number of Naval Medicine CIOs available for this study required utilization of a similar group to pre-test the survey questionnaire. The survey questionnaire for this study was pre-tested by fellow students enrolled in the information security track within the Information Systems Technology curriculum at the Naval Postgraduate School. Afterwards, the survey was submitted for pre-testing to the Naval Postgraduate School CIO, CTO, ISSO, and ISSM to average the total survey participation time and to solicit any noted discrepancies or potential conflicts within the survey. The average time to complete the 30-question survey was approximately 12 minutes. Pre-test questionnaires are located in Appendix B. Following the pre-test, questionnaires were transformed to an HTML-based survey and were activated on the Naval Medicine Online portal. Finally, each of the 51 identified Naval Medicine CIOs was sent a survey key via email with an accompanying message to explain the purpose of the survey.

B. DEMOGRAPHIC ANALYSIS

Naval Medicine employs approximately 60,000 military, civilian and contract personnel to support medical and dental facilities, health care support offices, research and development activities and training commands around the world. The information technology components of approximately 300 facilities are currently managed by 51 CIOs. A total of 51 survey invitations were sent out for participation in this research effort and 31 anonymously completed surveys were posted to the database. The anonymous respondent survey data is located in Appendix D. Twenty-six (84 percent) of the survey respondents were located in the continental United States (Inconus) and five (16 percent) of the survey respondents were located outside of the continental United States. See Figure 5. This sample size represents approximately 61 percent of the CIOs in Naval Medicine.

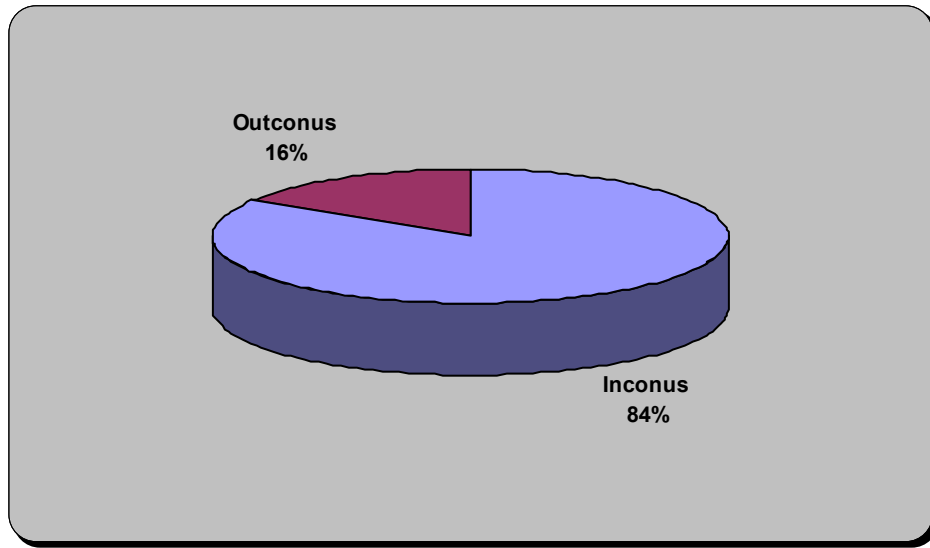


Figure 5. Regional Survey Response

There were 27 CIOs, three ISSMs, and one respondent categorized as “Other” that made up the representative sample of survey respondents. See Figure 6. The CIOs made up approximately 88 percent of the sample, the ISSMs made up another 9 percent of the population and one survey respondent was listed as “Other” for a job title that accounted for approximately 3 percent of the survey sample.

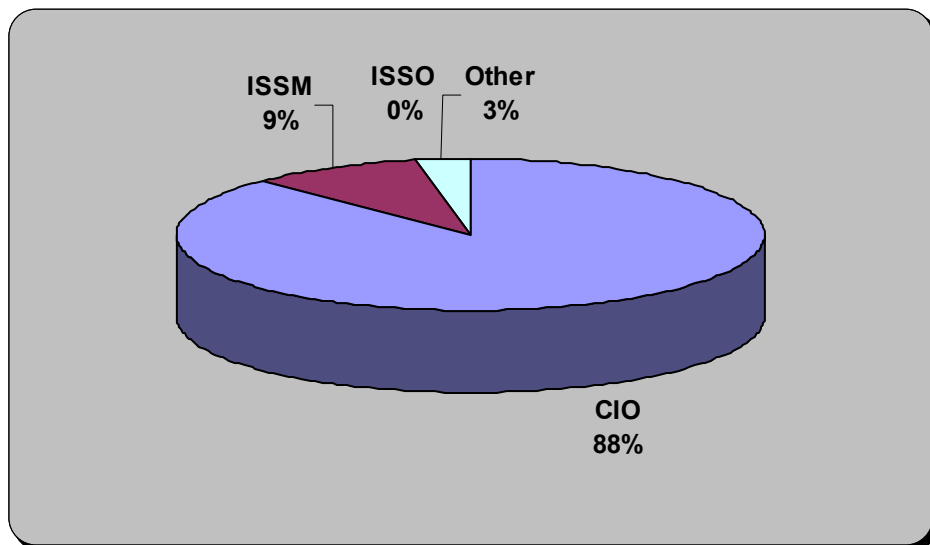


Figure 6. Survey Respondent Titles

This researcher attempted to make a distinction in facility size by incorporating ranges of total personnel strength per facility to classify each as a small, medium, or large facility. Thirteen percent of the respondents were responsible for facilities with more than 1000 personnel within their organization. Fifty-five percent of the respondents were responsible for medium-sized facilities ranging from 201 to 1000 personnel. The other 32 percent were responsible for smaller facilities with less than 200 personnel on board.

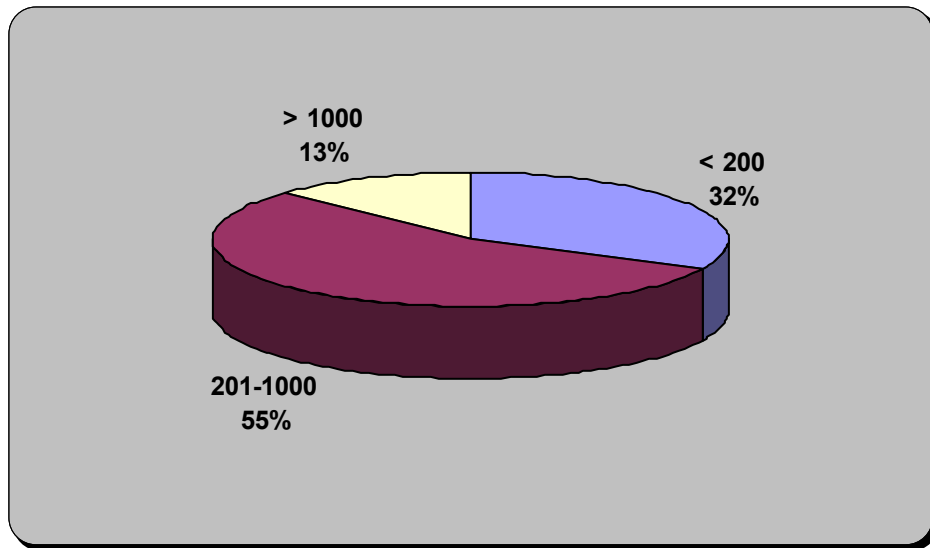


Figure 7. Respondent Organization Size (Personnel Strength)

Seventy-one percent of the sample had eight or more years of IT experience. There were no respondents with less than 2 years of experience. See Figure 8. Only 10 percent of the sample population had between 2 and 4 years of experience in IT operations.

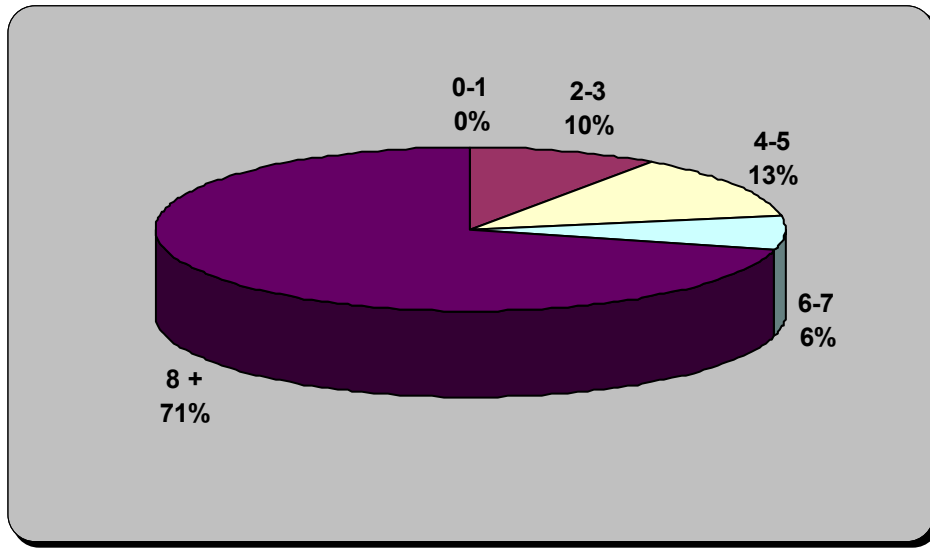


Figure 8. Respondent Years of Experience

C. SURVEY QUESTIONNAIRE ANALYSIS

The standard deviation and confidence levels at 95% were computed for all questions. See Appendix F. Standard deviation remains one of the most commonly used statistical tools in the sciences and social sciences. It provides a precise measure of the amount of variation in any group of numbers. A standard deviation is the plus or minus variance from the mean score needed to capture 68 percent of the population. More generally, it is a number that distinguishes how far a particular field of data varies from the overall average of all respondents that answered a particular question. The smaller the deviation, the more confidence one can have in the computed value for the mean. An extreme deviation was not noted in this survey. Question 26 (“How many months pass between each systems vulnerability/penetration test?”) had the highest standard deviation at 1.362890, and Question 16 (How many system compromises were considered as serious?) had the lowest standard deviation at 0.358568. Those figures are represented in Appendix G.

A comparison of survey questions 15 (“How many known systems compromises, including e-mail and Web-based deliveries of malware, have occurred within your organization in the past year?”) and 17 (“How many of the compromises may have been prevented if the available patches had been installed?”) revealed that of the 14 commands reporting known compromises, seven of them reported that the available vulnerability

patches had not been applied. Fifty percent of the attacks occurred on unpatched systems. The survey did not request specific numbers of known attacks; however, it requested a general range of known attacks (See Appendix A, Question 15). On the conservative side, that total equates to as little as 31 known attacks and at the other end of the response category spectrum, it equates to as many as 72 known attacks in the past 12 months. Along with this data, it should also be noted that 77 percent of those compromised systems were at commands within the continental United States (Inconus), while the remaining 23 percent were outside the continental United States (Outconus). This finding correlates to the findings in Burns (2003), whereas the majority of attacks are directed at the United States.

One would tend to believe that years of experience would make a difference in the frequency of attacks. The demographics portion of the survey inquired about the respondent's years of IT experience. Once again, this area of the survey did not request specific numbers of years; however, it requested a general range of years of experience. (See Appendix A, Question 4). An across-the-board conservative approach, awarding no more than 8 years of IT experience to any one person, revealed that the average IT experience level for those compromised commands is 6.76 years. This average could indicate that some of the CIOs in the field are short on either personnel or resources given that they have an adequate amount of IT experience.

Question 25 inquired about the number of personnel resources employed specifically to perform system configuration and patch management tasks. Question 28 asked if enough resources were available to meet the current security threat. Eight (57%) of the 14 sites reporting compromises reported they had the appropriate resources. Of those 14 sites that experienced system compromises, nine (64%) of them had one or more personnel performing that duty. The other five sites that were compromised did not have personnel assigned specifically to perform patch management tasks, but five (83%) had someone performing those tasks as a part of their responsibility. Since 13 of the 14 (93%) of the compromised sites have someone performing the tasks in some capacity, this could indicate that the current patch management tasks are not being performed as quickly, or as thoroughly, as necessary to prevent the compromises as other tasks may be taking precedence.

Question 26 asked how many months pass between each systems vulnerability test. The cumulative average of all compromised commands is 6.3 months between systems scans, while those that were not compromised average 4.6 months between vulnerability scans. This supports Nicolett and Pescatore's theory (2003) that although malware and bugs may take 6 months to become a problem, more frequent scanning will have an important effect on network management. At a minimum, Military Health System Information Assurance Policy (2003) recommends system vulnerability scans at least once per month. Gartner research predicts that by the year 2005, just 6 months from now, "... the due diligence level of vulnerability assessment will require that full system scans be done at least once per month (.07 probability)." Naval Medicine, as indicated by the IA survey results, is far behind the requirement for monthly scans, which if performed as prescribed, would have eliminated a significant amount of intrusions. Depending on the size of the organization, automated methods of scanning may increase effectiveness, while simultaneously decreasing the overall risk.

An insight to scanning and patching practices was discovered in Questions 10 through 13. Question 10 asked if automated vulnerability scans were performed. Eighteen (58%) commands reported that automated scans are done, while the remaining 13 (42%) reported that they did not perform them. Question 11 was the follow-on to Question 10, as it inquired about how many commands are utilizing automated patching technologies. Twenty-five (81%) reported that they did, and only six (19%) reported that they did not. This is interesting, to say the least if when considering the number of know compromises over the past 12 months. Those reporting automated patching may be indicating that their servers are only performing automated vendor downloads and updates, as are available now on many of the Microsoft and Unix operating systems. Question 12 asked if manual vulnerability scans were performed. Nineteen (61%) commands reported that manual scans are done and the remaining 12 (39%) reported that they did not perform them. Of all respondents surveyed, 14 (45%) of them are performing scans within the 1-3 month timeframe, and it becomes evident at this point that frequency of scans and remediation has the greatest impact in regards to compromise prevention. Only 4 (29%) of the 14 respondents have reported having systems compromises within the past year. Question 13 was the follow-on to Question 12,

inquiring as to how many commands are utilizing manual patching technologies. Twenty-two (71%) reported that they did and nine (29%) reported that they did not. Seventeen (55%) respondents reported that automated patching and scanning was being performed, but collectively, they were compromised eight times. One might question the length of time between detection and remediation of known vulnerabilities. A closer look at the responses regarding automated scanning and automated patching revealed that the average length of time between scans is 5.3 months. Three (37.5%) of those organizations scan and patch every 1-3 months, 2 (25%) others scan every 4 -6 months, and 3 (37.5%) others scan every 10-12 months. Of those eight compromises, one (13%) was serious, and 3 (37.5%) were reported to be lacking the appropriate patch. Furthermore, 6 (75%) of those compromises originated from email and 2 (25%) were compromised via the Web. Another discovery was that the other 14 respondents that did not perform both automatic scanning and patching were collectively compromised seven times. The responses for both Questions 10 and 11 revealed that 50 percent of those commands not performing automated scanning and patching on a continual basis maintain 50 percent of the systems compromised over the past 12 months. The review of Questions 12 and 13, regarding manual scanning and patching, revealed that of the 16 (52%) commands that utilize manual methods, collectively they contributed to approximately 44% of the past year's compromised systems, as seven (44%) of the 16 sites experienced a compromise. Interestingly, six of those compromises stemmed from email and one was due to an outdated anti-virus signature. The 15 (48%) respondents that do not utilize manual scan patching methods collectively contributed to eight systems compromises, which is approximately 53% of the total. Questions 10 through 13, which cover both automated and manual scanning and patching practices revealed that 11 (35%) of all survey respondents were utilizing both methods and 20 (65%) were not. The average time between scans for those that were utilizing both methods was 5.2 months. Of the 11 (35%) that were performing both, 5 (45%) had been compromised. As one may easily recognize, automation does not provide a significant advantage over manual methods if the tools are not being employed on a monthly basis as required by the Military Health Systems (MHS) Information Assurance Policy. This survey should

highlight the speed in which the new threats are approaching and that automation must be utilized on a more frequent basis.

V. CONCLUSIONS AND RECOMMENDATIONS

A. CORRELATION OF RESULTS IN COMPARISON TO PREMISE

The premise that 75 percent of Naval Medicine's known information systems compromises were not protected by the available vulnerability patch(s) was not confirmed. The findings and consolidated view of this study are depicted below in Figure 9 as it relates to significantly disproving the premise of this project.

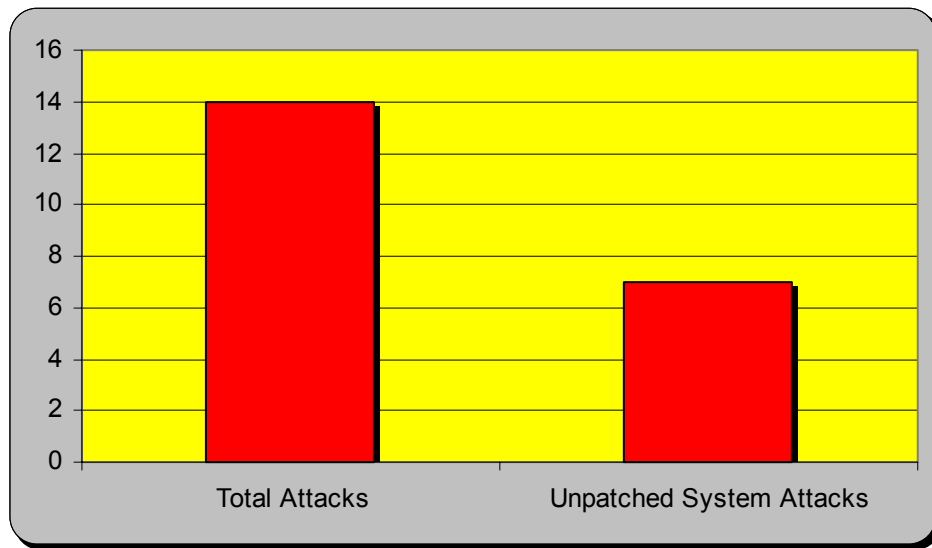


Figure 9. Regional Survey Response

Survey respondents from 14 (45%) commands reported known systems compromises within the past year. Seven (50%) of those respondents reported that the available vulnerability patches had not been applied. In essence, 50 percent of the known attacks were due to the tardiness in application of the appropriate protection. It bears repeating that the average length of time between automated vulnerability scans combined with automated patching is 5.3 months. If this average detection and response time is not corrected, the next 12 months may show a marked increase in system compromises.

B. THESIS QUESTIONS REVIEW

1. *Are existing Naval Medicine Information Assurance policies in alignment with current Navy policy and federal government requirements?* The existing policies

are all vague and general with regard to vulnerability assessments and patching requirements. MHS has the most up-to-date information, but the requirements within that document still fall short of best-business practices. Nearly every published document pertaining to information assurance within the past year highlights the current threats, reports that the patch management industry is a spiraling market, and that near real time scanning and patching are the only real options left to safeguard connected information assets.

2. *Would the implementation of automated vulnerability scanning and patching technology benefit Naval Medicine?* As previously mentioned in Question 1, automated scanning and patching solutions as close to real time as possible are the most effective means to securing information assets to protect them from the current threat environment. The continued occasional use will not provide the true ROI associated with more aggressive automated vulnerability assessment practices.

3. *Would automated vulnerability scanning and patching be a cost-effective means to address the current information assurance threats?* Gartner group estimates that a 1000 unit server farm costs \$300,000 per year to perform patch management tasks. The same server population would cost \$50,000 to implement an automated solution. Since this researcher does not have access to the actual number of systems within Naval Medicine, the following subjective estimate is submitted.

BUMED estimates personnel strength to be approximately 60,000. If only 25 percent of those personnel utilized information systems to perform their tasks, that would mean that Naval Medicine maintains about 15,000 systems. The sample population for this IA survey reports that the aggregate of respondents currently have 27 dedicated personnel to perform patch management within their organization. The sample size only represented approximately 61 percent of the CIOs in Naval Medicine. If all had responded, the results may have approached a total of approximately 50 personnel that performed patch management as their primary duty. If each of them maintains a salary of \$40,000 per year, Naval Medicine spends approximately \$2M per year in maintenance costs to protect their information assets, while 50 percent of manually scanned and patched systems are compromised within a one-year time frame. If these figures are

somewhat close to the truth, a commercial vendor's automated scanning and patching solution would cost approximately \$750,000 per year.

In addition, one must consider that the conservative approach of 31 known reported system compromises as reported by the survey respondents occurred within the past year. It is unknown which systems were compromised, but if personal privacy data was compromised on any of them, the fiscal penalties from the HIPAA violations alone could easily go beyond \$750K.

Outside of the HIPAA requirements, the reported costs to rebuild compromised systems takes approximately 2-4 hours depending on the operating system and data files required. Currently 17 of the respondents report that they spend 10 + hours per system per month to keep each system patched and configured to meet the current information assurance threats. Considering that a system administrator's salary is approximately \$40,000 per year, each month's maintenance per system is approximately \$3,300 dollars. If that figure is divided in half, the cost remains approximately \$1,500 per month per system for the required maintenance. If the vendor solution is \$50 per year per system, recurring maintenance fees based on \$1,500 per month cost approximately \$18,000 per year. That fee of \$18,000 divided by \$50.00 represents a 180 percent savings in maintenance costs if only half of the administrators were utilized. This automation would not replace the administrative staff, but it would free up their valuable time to work on other significant maintenance issues. The automated technology is well worth what it provides, but Naval Medicine personnel may not have the funding to invest in these technologies right away; however, options for automated solutions are free of charge from DISA and the Department of Homeland Security. "An effective vulnerability-assessment/patch management effort will reduce operational risks for everyone" (Shipley, 2003).

4. *Would a consolidated and centrally managed vulnerability database increase the current security posture?*

Centrally managed vulnerability databases are already maintained by federally funded organizations such as NIST. In the case of a centrally managed database that maintains tested patches, it may be helpful to have a secure source to pull from, but many

are opting out of patch testing as they would rather take one of their own systems offline as opposed to having their entire network, in many cases, exposed to the malware practitioners and hackers looking for free spam relays (Roberts, 2003).

C. RECOMMENDATIONS FOR INCREASING NAVAL MEDICINE INFOSEC POSTURE

The IA survey revealed that approximately 42% of the respondents are not utilizing automated vulnerability assessment tools. This translates to increased risk, increased costs and a lower confidence level for those personnel charged with the responsibility of safeguarding the organizations information assets. Automation has faced much criticism in the past, as has any new technology. According to the IA survey, 45% of the respondents have concerns regarding reliability and another 32% are concerned about the effectiveness of automated assessment and patching solutions. This researcher submits that nothing will ever be bulletproof, but proactively utilizing the best tools available to offset the threat will always remain the best defense (Shipley, January 2003).

The perceived benefit derived from the utilization of automated vulnerability assessment solutions can only promote a healthier and more secure networking environment for Naval Medicine professionals, while significantly decreasing the overall risk (Shipley, January 2003). The continued increases of malware distribution, in conjunction with the increased reliance on networked information systems, create an overwhelming need to maintain confidentiality, integrity, and availability of information assets. The personnel hours required in typical monthly maintenance procedures alone will produce an immediate return on investment if funding is unavailable for an enterprise-wide solution (Schroder, 2003). If funding is not available, an immediate effort should be made by those commands not using automated solutions to obtain the free GOTS vulnerability scanning solution from DISA.

Security experts around the globe concur that today's networked environment is more dangerous than it has ever been and those that do not utilize automated solutions in conjunction with layered defenses are at a much greater risk than those that are taking more proactive and aggressive approaches to securing their information assets.

D. SUGGESTIONS FOR FURTHER RESEARCH

A comparison of blocked attacks per organization in comparison to vulnerability scanning and mitigation practices may yield even more evidence regarding the probability of enhanced security based on speed in detection and mitigation of risk. It would also be interesting to know how many compromises have been avoided within Naval Medicine due to the use of automated or manual vulnerability assessment methods and which tools were considered the best across the boards (i.e., ease of use, licensing expenses, etc.). In addition, a comparison of formal policies and practices among those commands and regions may also provide for interesting research. If BUMED began keeping track of compromises, over time, deviations in command practices and policy adherence may become more evident. This survey only asked for the past 12 months of history. Another year or two of analysis would have been highly beneficial to this research project.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

- Azari, R. (2003). *Current security management and ethical issues of information technology*. Hershey, Penn.: IRM Press.
- Burns, C. (2003, August 25). The Internet danger zone. *Network World*, 20, 34, 48-52.
- CERT/CC statistics for incidents (2003). Retrieved April 5, 2004 from <http://www.cert.org/stats>
- CERT/CC statistics for vulnerabilities (2003). Retrieved April 5, 2004 from <http://www.cert.org/stats>
- CERT/CC statistics for percent of annual increase (2003). Retrieved April 5, 2004 from <http://www.cert.org/stats>
- Chabrow, E. (2003, November 3). NIST drafts security controls for computer systems. *Information Week*. Retrieved April 5, 2004 from <http://www.informationweek.com/story/showArticle.jhtml?articleID=15800643>
- Clarke, R. A. (2002, September 18). *The National Strategy to Secure Cyberspace*. The White House: President's Critical Infrastructure Protection Board.
- Computer System Security and Privacy Advisory Board (2002). Summary of Meeting, December 3-5, 2002, Gaithersburg, Maryland.
- Doherty, S. (2003, July 10). Feds reach out and touch IT. *Network Computing*, 14, 13, 36-56.
- Eschelbeck, G. (2004, February 24). *The laws of vulnerabilities*. RSA Panel Discussion.
- Evers, J. (2003, November 24). *Symantec CEO: new threats need new security tack*. Retrieved April 5, 2004 from <http://enterprisesecurity.symantec.com>
- Goth, G. (2004, March/April). How useful are attack trend resources? *IEEE Security and Privacy*, 2, 2, 9.
- Konigsberg, B. (2002). *Auditing inside the enterprise via port scanning and related tools*. SANS Institute. Retrieved January 11, 2004 from <http://www.sans.org>.
- McGuirl, M. (2004, April). Castles were once a great idea, too. *CyberDefense Magazine*, 2, 4, 24-27.
- Military Health System Information Assurance Program Office (2003, December). *Military Health System Information Assurance policy/guidance manual*.
- Nicolett, M. and Pescatore, J. (2003, November 19). *Security demands shift to vulnerability management*. Retrieved January 11, 2004 from <http://www.gartner.com>
- Roosevelt, A. (2004, January 22). Network-centric warfare emerging, industry must help, officials say. *Defense Daily*, 8.
- Roberts, P. (2003, December 15). *More, worse cyberattacks seen coming in 2004*. Retrieved April 5, 2004 from <http://enterprisesecurity.symantec.com>

Rubin, A. (2001). *White-hat security arsenal: tackling the threats*. Upper Saddle River, N.J.: Pearson Education.

Schroder, N., Colville, R. & Nicolett, M. (2003, May 30). *Patch management is a fast growing market*. Retrieved April 5, 2004 from <http://www.gartner.com>

Shiple, G. (2003, January 23). Tactical security 101. *Network Computing*, p. 44-57.

Shiple, G. (2003, June 26). Are you vulnerable? *Network Computing*, 14, 12, 42-60.

BIBLIOGRAPHY

- Andrews, A. D. (2003, March 23). *Security program management and risk*. SANS Institute. Retrieved January 11, 2004 from <http://www.sans.org>
- Arbaugh, W., Shankar, N. and Wan, Y. C. (2001, March 30). *Your 802.11 wireless network has no clothes*. University of Maryland. Retrieved January 7, 2004 from <http://www.cs.umd.edu/~waa/wireless.pdf>
- Authorized temporary exemptions to baseline settings (2004, January 31). *Navy-Marine Corps Unclassified Trusted Network Policy*. Section 4.3.
- Bahadur, G. (2004). *Developing security risk metrics*. Presentation by Global Knowledge. Retrieved April 5, 2004 from www.globalknowledge.com
- Bailey, C. F. (2003). *Analysis of security solutions in large enterprises*. Master's Thesis, Naval Postgraduate School, Monterey, California.
- Bayne, J. (2002). *An overview of threat and risk assessment*. SANS Institute. Retrieved January 11, 2004 from <http://www.sans.org>
- Berger, B. (2003, August 20). *Data-centric quantitative computer security risk assessment*. SANS Institute. Retrieved January 11, 2004 from <http://www.sans.org>
- Berinato, S. (2004, February 13). *Courts make users liable for security glitches*. Retrieved April 5, 2004 from <http://enterprisesecurity.symantec.com>
- Bogen, J. (2001). *HIPAA challenges for information security: are you prepared?* Retrieved January 11, 2004 from <http://www.HealthCIO.com>
- Bong, K. M. (2003). *Conducting an electronic information risk assessment for Gramm-Leach-Bliley Act compliance*. SANS Institute. Retrieved January 11, 2004 from <http://www.sans.org>
- Bowen, P. et al (2004, May). *An introductory resource guide for implementing the Health Insurance Portability and Accountability Act (HIPAA) security rule*. NIST Special Publication 800-66. Gaithersburg, Maryland: National Institute of Standards and Technology.
- Bridis, T. (2003, October 15). *Microsoft warns of four new Windows flaws*. Retrieved April 5, 2004 from <http://msnbc.msn.com>
- Buffer overflow in Windows Workstation service* (2003, November 11). CERT Advisory CA-2003-28.
- CERT Summary CS-2003-04* (2003, November 25).
- CERT/CC incident and vulnerability statistics through 2003* (2004). Retrieved January 23, 2004 from <http://www.cert.org/stats>
- CERT/CC statistics 1988-2003*. Retrieved September 2, 2003 from <http://www.cert.org/stats/>

Chapman, S. H. (2002, March 1). *Seeking security: the new paradigm for government agencies*. SANS Institute. Retrieved January 11, 2004 from <http://www.sans.org>

Colville, R. and Nicolett, M. (2003, March 18). *Patch management: identifying the vendor landscape*. Retrieved January 11, 2004 from <http://www.gartner.com>

Computer security links (2004, February 12). Retrieved April 5, 2004 from <http://www.johnsaunders.com/security.htm>

Cross, K. (2000, January). *Application of the NSA INFOSEC assessment methodology for GIAC International Schools, Incorporated, Washington, D.C.* SANS Institute. Retrieved January 11, 2004 from <http://www.sans.org>

Dacey, R. (2003, October 17). *Posthearing questions from the September 10, 2003, hearing on worm and virus defense: how can we protect our nation's computers from these serious threats?* United States General Accounting Office: GAO-04-173R. . Retrieved March 31, 2004 from <http://purl.access.gpo.gov/GPO/LPS43210>

Distributed scan model for enterprise-wide network vulnerability assessment (2002). SANS Institute. Retrieved January 11, 2004 from <http://www.sans.org>

Donner, M. (2004, March/April). Hacking the best-seller list. *IEEE Security and Privacy*, 2, 2, 51-53.

Email-borne viruses (2004, January 27). CERT Advisory CA-2004-02.

Evers, J. (2003, November 10). *Office 2003 gets first "critical" update*. Retrieved April 5, 2004 from <http://enterprisesecurity.symantec.com>

Evers, J. (2003, November 11). *New worm steals user information*. Retrieved April 5, 2004 from <http://enterprisesecurity.symantec.com>

Free, D., Wagner, T. and McKibben, D. (2003, April 29). *First steps to enterprise risk management implementation*. Retrieved January 11, 2004 from <http://www.gartner.com>

Garbars, K. (2002). *Implementing an effective IT security program*. SANS Institute. Retrieved January 11, 2004 from <http://www.sans.org>

Grance, T., Kent, K. and Kim, B. (2004, January). *Computer security incident handling guide*. Gaithersburg, Maryland: National Institute of Standards and Technology. Retrieved March 31, 2004 from <http://purl.access.gpo.gov/GPO/LPS43017>

Guirguis, R. (2003, June 14). *Network- and host-based vulnerability assessments: an introduction to a cost effective and easy to use strategy*. SANS Institute. Retrieved January 11, 2004 from <http://www.sans.org>

Hallawell, A. (2003, February 19). *SQL Slammer lessons: traditional antivirus is not enough*. Retrieved January 11, 2004 from <http://www.gartner.com>

Harris, M. C. (2002). *System identification for vulnerability assessment*. SANS Institute. Retrieved January 11, 2004 from <http://www.sans.org>

Hofmeyr, S. (2002). *Primary Response Technical White Paper*. Sana Security. Retrieved March 1, 2004 from <http://www.sanasecurity.com>

Huber, R. (2003, April 20). *Strategies for improving vulnerability assessment effectiveness in large organizations*. SANS Institute. Retrieved January 11, 2004 from <http://www.sans.org>

Hurley, E. (2004, February). *Shocking precedent*. Retrieved April 5, 2004 from http://infosecuritymag.techtarget.com/ss/0,295796,sid6_iss326_art604,00.html

King, J. (2003). *Ten vulnerabilities a scanner might not find*. SANS Institute. Retrieved January 11, 2004 from <http://www.sans.org>

Lankhorst, D. A. (1996). *Using expert systems to conduct vulnerability assessments*. Master's Thesis, Naval Postgraduate School, Monterey, California.

Levy, E. (2004, March/April). Criminals become tech-savvy. *IEEE Security and Privacy*, 2, 2, 65-68.

Lim, W. P. (2003). *Vulnerability of wireless point-to-point systems to interception*. Master's Thesis, Naval Postgraduate School, Monterey, California.

McGraw, G. (2004, March/April). Software security. *IEEE Security and Privacy*, 2, 2, 80-83.

McMillan, R. (2003, November 18). *Linux kernel attack thwarted*. Retrieved April 5, 2004 from <http://enterprisesecurity.symantec.com>

Military Health System Information Assurance Program Office (2003, February 12). *Military Health System Information Assurance policy/guidance manual*.

Military Health System Information Assurance Program Office (2003, July 12). *Military Health System Information Assurance policy/guidance manual*.

Mina, T. (2002). *Application security, information assurance's neglected stepchild – a blueprint for risk assessment*. Paper presented at the GIAC Security Essentials Conference, Baltimore, Maryland, May 18-20, 2001. Retrieved January 11, 2004 from <http://www.sans.org>

Mitchell, J. (2002, April 26). *Proactive vulnerability assessments with Nessus*. SANS Institute. Retrieved January 11, 2004 from <http://www.sans.org>

MyDoom.B rapidly spreading (2004, January 28). CERT Technical Alert TA04-028A.

Naval Medical Information Management Center (2002, January 23). *Bureau of Medicine and Surgery Information Systems Security policy manual*

Navy Bureau of Medicine and Surgery (2002, January 23). *Information Assurance: Information Systems Security policy manual*. Retrieved September 7, 2003 from https://imcenter.med.navy.mil/035department/security_policy.htm

New twist in virus attacks expected Friday (2003, August 22). Retrieved April 5, 2004 from <http://www.nbc4.com>

Nichols, A. (2002). *A perspective on threats in the risk analysis process*. SANS Institute. Retrieved January 11, 2004 from <http://www.sans.org>

Nicolett, M. (2003, March 25). *Managing IT security risk in a dangerous world*. Retrieved January 11, 2004 from <http://www.gartner.com>

Nicolett, M. (2003, November 20). *Predicts 2004: security and privacy*. Retrieved January 11, 2004 from <http://www.gartner.com>

Nicolett, M. (2003, September 3). *Vulnerability management defined*. Retrieved January 11, 2004 from <http://www.gartner.com>

Nicolett, M. and Colville, R. (2003, March 18). *Robust patch management requires specific capabilities*. Retrieved January 11, 2004 from <http://www.gartner.com>

Noakes-Fry, K. and Diamond, T. (2003, February 24). *RiskWatch risk analysis software*. Retrieved January 11, 2004 from <http://www.gartner.com>

Oribello, A. (2004, April). Protecting turnkey systems. *Computer Security Alert*, 3.

Page, P. (2003, May 24). *Security auditing: a continuous process*. SANS Institute. Retrieved January 11, 2004 from <http://www.sans.org>

Port knocking (2004). Retrieved April 5, 2004 from <http://www.prtnocking.org/>

Primary Response 1.0 FAQ. Sana Security. Retrieved March 1, 2004 from <http://www.sanasecurity.com>

Protecting against "zero day" attacks (2004, March 24). Retrieved April 5, 2004 from <http://enterprisesecurity.symantec.com>

Richardson, R. (2004, April). Fixing the cost of fixes. *Computer Security Alert*, 1-2.

Roberts, P. (2003, November 17). *CERT warns about new Microsoft vulnerability*. Retrieved April 5, 2004 from <http://enterprisesecurity.symantec.com>

Ross, R. and Swanson, M. (2003, June). *Guide for the security certification and accreditation of federal information systems*. Gaithersburg, Maryland: National Institute of Standards and Technology.

Schwartz, M. (2004). *Making products talk vulnerabilities*. Retrieved February 26, 2004 from <http://www.avdl.org>

Shipley, G. (2003, January 23). Secure to the core. *Network Computing*, p. 34-43.

Stytz, M. (2004, March/April). Hacking for understanding. *IEEE Security and Privacy*, 2, 2, 8.

Sullivan, B. (2004). *Could your computer be a criminal?* Retrieved April 5, 2004 from <http://msnbc.msn.com/id/3078454>

Swanson, M. et al (2003, July). *Security metrics guide for information technology systems*. Gaithersburg, Maryland: National Institute of Standards and Technology.

Tittel, E. (2003, July 16). *Security audit action list for CIOs*. Retrieved April 5, 2004 from <http://techrepublic.com.com/5102-6296-5054775.html>

Trope, R. (2004, March/April). A warranty of cyberworthiness. *IEEE Security and Privacy*, 2, 2, 73-76.

U.S. Government attack and vulnerability services. Retrieved April 5, 2004 from http://icat.nist.gov/vt_portal.cfm

United States General Accounting Office (2003, June). *FDIC information security: progress made but existing weaknesses place data at risk*. GAO-03-630. Retrieved March 31, 2004 from <http://www.gao.gov/new.items/d03630.pdf>

Visintine, V. (2003, August 8). *An introduction to information risk assessment*. SANS Institute. Retrieved January 11, 2004 from <http://www.sans.org>

Vulnerability scanning requirements for GISRA under OMB M-02-09 (2002, October). SANS Institute Report 02-103.

Wai, C. T. (2002). *Conducting a penetration test on an organization*. SANS Institute. Retrieved January 11, 2004 from <http://www.sans.org>

Wayner, P. (2004, March/April). The power of candy-coated bits. *IEEE Security and Privacy*, 2, 2, 69-72.

Wheatman, V. et al (2003, May 30). *Hype cycle for information security, 2003*. Retrieved January 11, 2004 from <http://www.gartner.com>

Windows-based ATMs not safe from Net worms (2003, December 9). Retrieved April 5, 2004 from <http://www.telecomasia.net>

Witty, R. et al (2001, June 8). *The price of information security*. Retrieved January 11, 2004 from <http://www.gartner.com>

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A. SAMPLE HTML RESEARCH QUESTIONNAIRE

Naval Medicine Online	
Information Assurance Management Survey	
As Navy Medicine IT leaders dealing with dynamic and complex environments, I am respectfully requesting your assistance in completing my thesis research at Naval Postgraduate School. The most recent trends in Information Assurance have illustrated the worsening of vulnerabilities and exploits. This trend is easily identified in historical CERT summary reports. My thesis topic focuses on identifying more manageable methods to conduct vulnerability scans and patch management tasks. This study is resultant of my past experiences with our seemingly ceaseless efforts to keep NMIMC's systems scanned and patched by utilizing manual methods. As part of my research, I am posting this four-section Information Assurance Management Survey totaling 30 questions that should take approximately 10-15 minutes to complete. As noted on the survey form, your input will remain completely anonymous for obvious reasons. Your assistance in completing this survey no later than April 30, 2004 would be greatly appreciated. Your input will make a difference. A single use survey key has been provided to you to ensure each command responds only once. This survey instrument has been validated by a number of professors within the Center for Information Systems Security Studies and Research (CISR) at NPS and tested among local professionals managing the NPS networks. The final review was performed by Dr. Dorothy Denning, a well respected information security expert. I thank you in advance for your consideration and participation in this study. If you are interested in obtaining a copy of the results, please send an e-mail request to (spreinke@nps.navy.mil) at your earliest convenience. Very Respectfully, LTJg Steven Reinkemeyer	

* Answer Required.
Section I - Demographics
Please choose one response per question.
1. What is your title? *
☐ CIO ☐ ISSM ☐ ISSO ☐ Other
2. How many years of IT experience do you have? *
☐ 0-1 ☐ 2-3 ☐ 4-5 ☐ 6-7 ☐ 8+
3. Where is your geographic location? *
☐ INCONUS ☐ OUTCONUS
4. How many personnel are employed within your organization? *
☐ < 200 ☐ 201 - 1000 ☐ > 1000

Section II

Please choose one response for each question.

5. Are all of your organization's applications certified and accredited under a full Authority to Operate (ATO)? *

- ☐ Yes
- ☐ No
- ☐ Planned
- ☐ Don't Know

6. Are all of your organization's servers certified and accredited under a full Authority to Operate (ATO)? *

- ☐ Yes
- ☐ No
- ☐ Planned
- ☐ Don't Know

7. Is your organization's network certified and accredited under a full Authority to Operate (ATO)? *

- ☐ Yes
- ☐ No
- ☐ Planned
- ☐ Don't Know

8. Does your organization have a written vulnerability assessment policy (e.g., maximum amount of time between assessments)? *

- ☐ Yes
- ☐ No
- ☐ Planned
- ☐ Don't Know

9. Does your organization have a written patch management policy (e.g., patch prioritization based on risk or threat)? *

- ☐ Yes
- ☐ No
- ☐ Planned
- ☐ Don't Know

10. Does your organization perform <u>automated</u> vulnerability assessments? *
☐ Yes ☐ No ☐ Planned ☐ Don't Know
11. Does your organization use <u>automated</u> patch management tools? *
☐ Yes ☐ No ☐ Planned ☐ Don't Know
12. Does your organization perform manual vulnerability assessments? *
☐ Yes ☐ No ☐ Planned ☐ Don't Know
13. Does your organization apply patches manually? *
☐ Yes ☐ No ☐ Planned ☐ Don't Know
14. Does your organization use stand-alone systems to test patches before applying them to affected systems? *
☐ Yes ☐ No ☐ Planned ☐ Don't Know

Section III

The response options for questions 15-24 are approximations. Please choose one response per question.

15. How many known system compromises (e.g., unauthorized system events or data theft) including e-mail and Web-based deliveries of malware have occurred within your organization in the past year?

**** If you select 0, skip to question 23.**

- ☐ 0
- ☐ 1-4
- ☐ 5-9
- ☐ 10 +

16. How many of those compromises were considered as serious (e.g., great effort to restore, many systems affected, or higher authority intervention)?

- ☐ 0
- ☐ 1-4
- ☐ 5-9
- ☐ 10 +

17. How many of the compromises may have been prevented if the available patches had been installed?

- ☐ 0
- ☐ 1-4
- ☐ 5-9
- ☐ 10 +

18. How many known system compromises (e.g., unauthorized system events or data theft) were from e-mail delivered malware (e.g., worms, viruses, Trojans, etc.) in the past year?

**** If you select 0, skip to question 21.**

- ☐ 0
- ☐ 1-4
- ☐ 5-9
- ☐ 10 +

19. How many of the e-mail delivered compromises were considered as serious (e.g., great effort to restore, many systems affected, or higher authority intervention)?
☐ 0 ☐ 1-4 ☐ 5-9 ☐ 10 +
20. How many of the e-mail delivered compromises may have been prevented if anti-virus signatures had been up to date?
☐ 0 ☐ 1-4 ☐ 5-9 ☐ 10 +
21. How many known system compromises (e.g., unauthorized system events or data theft) were <u>from Web-based malware</u> (e.g., worms, viruses, Trojans, etc.) in the past year?
☐ 0 ☐ 1-4 ☐ 5-9 ☐ 10 +
22. What is the <u>average</u> number of hours spent per month to decontaminate or remediate <u>EACH</u> system compromise within your organization?
☐ 0 ☐ 1-4 ☐ 5-9 ☐ 10 +

23. What is the average number of hours spent per month to keep EACH system patched and configured to meet new security threats?

- ☐ 0
- ☐ 1-4
- ☐ 5-9
- ☐ 10 +

24. How many system administrators does your organization employ to perform patch management/system configuration tasks that are incorporated with their other responsibilities? *

- ☐ 0
- ☐ 1-4
- ☐ 5-9
- ☐ 10 +

Section IV

Questions 25-30 have a variety of responses. Please read carefully and choose one response per question.

25. How many system administrators does your organization employ to perform patch management/system configuration tasks on your network as their primary duty? *

- ☐ 0
- ☐ 1
- ☐ 2
- ☐ 3+

26. How many months pass between each systems vulnerability/penetration test? *

- ☐ 1-3
- ☐ 4-6
- ☐ 7-9
- ☐ 10-12 +

27. Approximately how many servers reside on your network? *
☐ 0-50 ☐ 51-100 ☐ 101-150 ☐ > 150
28. Do you believe you have sufficient resources to keep each system patched and configured to meet new security threats? *
☐ Yes ☐ No ☐ Planned ☐ Don't Know
29. What is your greatest concern with using automated vulnerability/patch management tools? *
☐ Effectiveness ☐ Reliability ☐ Compatibility ☐ Other
30. What type of assistance from the DoD would most greatly assist you in your IA efforts? *
☐ Training ☐ Funding ☐ Tools ☐ Services
* Answer Required.

Submit Survey

APPENDIX B. SURVEY PRE-TEST QUESTIONNAIRES

Information Assurance Management Survey

This research is being conducted at the Naval Postgraduate School in partial fulfillment of the requirements for a Masters of Science degree in Information Systems Technology.

**** Your answers will remain anonymous.**

Please choose one response in each category

Job Title ☒ CIO ☐ ISSM ☐ ISSO ☐ Other

Years of Experience ☒ 0-1 ☐ 2-3 ☐ 4-5 ☐ 6-7 ☐ 8+

Geographic Location ☒ INCONUS ☐ OUTCONUS

Organization Size ☒ < 200 personnel ☐ 201 - 1000 personnel ☐ > 1000 personnel

1	Are all of your organization's <u>applications</u> certified and accredited under a full Authority to Operate (ATO)?	☒ Yes	☐ No	☐ Planned	☐ Don't Know
2	Are all of your organization's <u>servers</u> certified and accredited under a full Authority to Operate (ATO)?	☒ Yes	☐ No	☐ Planned	☐ Don't Know
3	Is your organization's <u>network</u> certified and accredited under a full Authority to Operate (ATO)?	☒ Yes	☐ No	☐ Planned	☐ Don't Know
4	Does your organization have a written vulnerability assessment policy (e.g., maximum amount of time between assessments)?	☒ Yes	☐ No	☐ Planned	☐ Don't Know
5	Does your organization have a written patch management policy (e.g., prioritization based on risk or threat)?	☒ Yes	☐ No	☐ Planned	☐ Don't Know
6	Does your organization perform <u>automated</u> vulnerability assessments?	☒ Yes	☐ No	☐ Planned	☐ Don't Know
7	Does your organization use <u>automated</u> patch management tools?	☒ Yes	☐ No	☐ Planned	☐ Don't Know
8	Does your organization perform manual vulnerability assessments?	☒ Yes	☐ No	☐ Planned	☐ Don't Know
9	Does your organization apply patches manually?	☒ Yes	☒ No	☐ Planned	☐ Don't Know
10	Does your organization use stand-alone systems to test patches before applying them to affected systems?	☒ Yes	☐ No	☐ Planned	☐ Don't Know

The response options for questions 11- 19 are approximations.

11	How many known system compromises (e.g., unauthorized system events or data theft) have occurred within your organization in the past year? <i>If you select 0, skip to question 18.</i>	0	1-4	5-9	☒ 10 +
12	How many of those compromises were considered as serious (e.g., great effort to restore, many systems affected, or higher authority intervention)?	☒ 0	1-4	5-9	10 +



each system

13	How many of the compromises may have been prevented if the available patches had been installed?	0	1-4	5-9	10 +
14	How many known system compromises (i.e., unauthorized system events or data theft) were from email delivered malware (e.g., worms, viruses, Trojans, etc.) in the past year? <i>If you select 0, skip to question 17.</i>	0	1-4	5-9	10 +
15	How many of the email delivered compromises were considered as serious (e.g., great effort to restore, many systems affected, or higher authority intervention)?	0	1-4	5-9	10 +
16	How many of the email delivered compromises may have been prevented if anti-virus signatures had been up to date?	0	1-4	5-9	10 +
17	What is the <u>average</u> number of hours spent per month to decontaminate or remediate each system compromise within your organization?	0	1-4	5-9	10 +
18	What is the <u>average</u> number of hours spent per month to keep each system patched and configured to meet new security threats?	0	1-4	5-9	10 +
19	How many system administrators does your organization employ to perform patch management/system configuration tasks that are incorporated with their other responsibilities?	0	1-4	5-9	10 +

The remaining questions have a variety of responses. Please read carefully.

20	How many system administrators does your organization employ to perform patch management/system configuration tasks on your network(s) as their <u>primary</u> duty?	0	1	2	3 +
21	How many months pass between each systems' vulnerability/penetration test?	1-3	4-6	7-9	10-12 +
22	Approximately how many servers reside on your network?	0-50	51-100	101-150	> 150
23	Do you believe you have sufficient resources to keep each system patched and configured to meet new security threats?	Yes	No	Planned	N/A
24	What is your greatest concern with using automated vulnerability/patch management tools?	Effective-ness	Reliability	Compati-bility	None
25	What type of assistance from the DoD would most greatly assist you in your IA efforts?	Training	Funding	Tools	Services

Information Assurance Management Survey

This research is being conducted at the Naval Postgraduate School in partial fulfillment of the requirements for a Masters of Science degree in Information Systems Technology.

**** Your answers will remain anonymous.**

Please choose one response in each category

Job Title	CIO	XISSM	ISSO	Other
------------------	-----	-------	------	-------

Years of Experience	0-1	2-3	4-5	X6-7	8+
----------------------------	-----	-----	-----	------	----

Geographic Location	XINCONUS	OUTCONUS
----------------------------	----------	----------

Organization Size	< 200 personnel	201 - 1000 personnel	X> 1000 personnel
--------------------------	-----------------	----------------------	-------------------

1	Are all of your organization's <u>applications</u> certified and accredited under a full Authority to Operate (ATO)?	Yes	No	XPlanned	Don't Know
2	Are all of your organization's <u>servers</u> certified and accredited under a full Authority to Operate (ATO)?	Yes	No	XPlanned	Don't Know
3	Is your organization's <u>network</u> certified and accredited under a full Authority to Operate (ATO)?	Yes	No	XPlanned	Don't Know
4	Does your organization have a written vulnerability assessment policy (e.g., maximum amount of time between assessments)?	XYes	No	Planned	Don't Know
5	Does your organization have a written patch management policy (e.g., prioritization based on risk or threat)?	XYes	No	Planned	Don't Know
6	Does your organization perform <u>automated</u> vulnerability assessments?	XYes	No	Planned	Don't Know
7	Does your organization use <u>automated</u> patch management tools?	xYes	No	Planned	Don't Know
8	Does your organization perform manual vulnerability assessments?	xYes	No	Planned	Don't Know
9	Does your organization apply patches manually?	xYes	No	Planned	Don't Know
10	Does your organization use stand-alone systems to test patches before applying them to affected systems?	xYes	No	Planned	Don't Know

The response options for questions 11- 19 are approximations.

11	How many known system compromises (e.g., unauthorized system events or data theft) have occurred within your organization in the past year? <i>If you select 0, skip to question 18.</i>	x0	1-4	5-9	10 +
12	How many of those compromises were considered as serious (e.g., great effort to restore, many systems affected, or higher authority intervention)?	x0	1-4	5-9	10 +

13	How many of the compromises may have been prevented if the available patches had been installed?	0	1-4	5-9	x10 +
14	How many known system compromises (i.e., unauthorized system events or data theft) were from email delivered malware (e.g., worms, viruses, Trojans, etc.) in the past year? <i>If you select 0, skip to question 17.</i>	0	1-4	5-9	x10 +
15	How many of the email delivered compromises were considered as serious (e.g., great effort to restore, many systems affected, or higher authority intervention)?	x0	1-4	5-9	10 +
16	How many of the email delivered compromises may have been prevented if anti-virus signatures had been up to date?	0	x1-4	5-9	10 +
17	What is the <u>average</u> number of hours spent per month to decontaminate or remediate each system compromise within your organization?	0	1-4	5-9	x10 +
18	What is the <u>average</u> number of hours spent per month to keep each system patched and configured to meet new security threats?	0	1-4	5-9	x10 +
19	How many system administrators does your organization employ to perform patch management/system configuration tasks that are incorporated with their other responsibilities?	0	1-4	5-9	x10 +

The remaining questions have a variety of responses. Please read carefully.

20	How many system administrators does your organization employ to perform patch management/system configuration tasks on your network(s) as their <u>primary</u> duty?	0	1	x2	3 +
21	How many months pass between each systems' vulnerability/penetration test?	x1-3	4-6	7-9	10-12 +
22	Approximately how many servers reside on your network?	0-50	51-100	x101-150	> 150
23	Do you believe you have sufficient resources to keep each system patched and configured to meet new security threats?	Yes	xNo	Planned	N/A
24	What is your greatest concern with using automated vulnerability/patch management tools?	Effective-ness	xReliabil-ity	Compati-bility	None
25	What type of assistance from the DoD would most greatly assist you in your IA efforts?	Training	Funding	xTools	Services

APPENDIX C. ENTIRE POPULATION – RAW DATA SURVEY RESPONSE SPREADSHEET

1. What is your job title?	2. How many years of IT experience do you have?	3. Where is your geographic location?	4. How many personnel are employed within your organization?	5. Are all of your organization's applications certified and accredited under a full Authority to Operate (ATO)?
Other	8+	INCONUS	< 200	No
CIO	8+	INCONUS	201 - 1000	No
CIO	2-3	INCONUS	< 200	Yes
CIO	8+	INCONUS	201 - 1000	Planned
ISSM	8+	INCONUS	< 200	Planned
CIO	6-7	INCONUS	201 - 1000	Planned
CIO	8+	INCONUS	201 - 1000	Yes
CIO	8+	INCONUS	< 200	No
CIO	4-5	OUTCONUS	< 200	Don't Know
ISSM	8+	INCONUS	201 - 1000	Don't Know
CIO	2-3	INCONUS	201 - 1000	No
CIO	8+	INCONUS	< 200	No
CIO	8+	OUTCONUS	201 - 1000	Yes
CIO	8+	INCONUS	< 200	Yes
CIO	8+	INCONUS	201 - 1000	Planned
CIO	2-3	INCONUS	201 - 1000	Yes
CIO	8+	INCONUS	201 - 1000	Don't Know
CIO	4-5	OUTCONUS	201 - 1000	No
CIO	4-5	INCONUS	< 200	Don't Know
CIO	8+	INCONUS	201 - 1000	No
ISSM	8+	INCONUS	201 - 1000	Yes
CIO	8+	INCONUS	201 - 1000	Planned
CIO	8+	INCONUS	> 1000	Planned
CIO	8+	INCONUS	> 1000	Planned
CIO	8+	INCONUS	> 1000	No
CIO	8+	INCONUS	201 - 1000	No
CIO	8+	OUTCONUS	201 - 1000	Planned
CIO	6-7	INCONUS	201 - 1000	No
CIO	4-5	INCONUS	> 1000	No
CIO	8+	INCONUS	< 200	Planned
CIO	8+	OUTCONUS	< 200	No

6. Are all of your organization's servers certified and accredited under a full Authority to Operate (ATO)?	7. Is your organization's network certified and accredited under a full Authority to Operate (ATO)?	8. Does your organization have a written vulnerability assessment policy (e.g., maximum amount of time between assessments)?	9. Does your organization have a written patch management policy (e.g., patch prioritization based on risk or threat)?
No	No	No	No
Yes	Yes	Yes	Yes
Yes	Yes	Planned	Yes
Planned	Planned	Planned	No
Planned	Planned	Yes	Yes
Yes	Planned	Planned	Yes
Yes	Yes	No	No
No	No	Yes	Yes
No	Don't Know	Yes	No
Don't Know	Don't Know	Don't Know	Yes
No	No	No	Yes
Yes	Yes	Yes	Planned
Yes	Yes	Planned	No
Yes	Yes	Yes	Yes
Yes	Yes	Planned	Yes
Yes	Planned	No	No
Don't Know	Don't Know	Don't Know	No
No	No	Yes	No
Don't Know	Don't Know	Don't Know	Don't Know
No	No	No	No
Yes	Yes	Yes	Yes
Planned	Planned	Yes	Yes
Planned	Planned	No	Yes
Planned	Planned	Yes	No
No	Planned	No	No
No	No	No	No
No	No	Planned	Yes
Yes	No	No	No
No	No	Yes	No
Planned	Planned	Planned	Yes
Planned	Planned	Planned	Planned

10. Does your organization perform automated vulnerability assessments?	11. Does your organization use automated patch management tools?	12. Does your organization perform manual vulnerability assessments?	13. Does your organization apply patches manually?	14. Does your organization use stand-alone systems to test patches before applying them to affected systems?
No	No	No	Yes	No
Yes	Yes	Yes	Yes	Yes
No	Yes	Yes	Yes	Don't Know
Planned	Yes	Yes	Yes	No
Yes	Yes	Yes	No	No
Yes	Yes	Yes	Yes	No
No	No	Yes	No	No
Yes	Yes	Yes	Yes	Yes
Yes	Yes	Yes	No	No
Yes	Yes	Don't Know	Yes	Don't Know
Yes	No	Yes	Yes	No
Yes	Yes	Yes	Yes	Yes
No	Yes	No	Yes	No
Yes	Yes	Yes	Yes	Yes
Yes	Yes	Yes	Yes	Yes
No	Yes	No	No	No
Yes	Yes	No	No	No
Yes	Yes	Yes	Yes	No
Don't Know	Don't Know	Don't Know	Don't Know	Don't Know
No	No	Yes	Yes	No
No	Yes	No	Yes	No
Yes	Yes	Yes	Yes	Yes
No	Yes	No	No	No
Yes	Yes	No	No	Yes
Yes	Yes	Yes	Yes	Planned
No	Yes	No	No	No
No	Yes	Yes	Yes	No
Yes	Yes	No	Yes	No
Yes	Yes	Yes	Yes	Yes
No	Planned	No	Yes	No
Yes	Yes	Yes	Yes	No

15. How many known system compromises (e.g., unauthorized system events or data theft) including e-mail and Web-based deliveries of malware have occurred within your organization in the past year? ** If you select 0, skip to question 23.	16. How many of those compromises were considered as serious (e.g., great effort to restore, many systems affected, or higher authority intervention)?	17. How many of the compromises may have been prevented if the available patches had been installed?	18. How many known system compromises (e.g., unauthorized system events or data theft) were from e-mail delivered malware (e.g., worms, viruses, Trojans, etc.) in the past year? ** If you select 0, skip to question 21.
1-4	1-4	1-4	0
0			
0			
0			
1-4	0	0	0
10 +	0	1-4	10 +
0	0	0	1-4
1-4	0	1-4	0
0			
0	0	0	0
1-4	0	0	1-4
0			
5-9	1-4	1-4	1-4
0			
0			
1-4	0	1-4	1-4
1-4	1-4	0	1-4
1-4	0	0	1-4
0			
5-9	0	0	5-9
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0			
1-4	1-4	1-4	1-4
0	0	0	
1-4	0	0	1-4
1-4	0	0	1-4
0	0	0	0
1-4	0	1-4	1-4

19. How many of the e-mail delivered compromises were considered as serious (e.g., great effort to restore, many systems affected, or higher authority intervention)?	20. How many of the e-mail delivered compromises may have been prevented if anti-virus signatures had been up to date?	21. How many known system compromises (e.g., unauthorized system events or data theft) were from Web-based malware (e.g., worms, viruses, Trojans, etc.) in the past year?	22. What is the average number of hours spent per month to decontaminate or remediate EACH system compromise within your organization?
		0	10 +
0	0	0	1-4
1-4	1-4	0	1-4
0	0	0	1-4
		0	0
0	0	0	1-4
0	1-4	0	0
1-4	1-4	1-4	1-4
0	1-4	0	1-4
1-4	0	1-4	1-4
0	0	0	0
0	0	0	1-4
0	0	0	0
0	0	0	0
		0	0
0	0	0	0
1-4	0	0	10 +
0	0	1-4	1-4
1-4	0	0	1-4
		0	1-4
0	1-4	0	0

23. What is the average number of hours spent per month to keep EACH system patched and configured to meet new security threats?	24. How many system administrators does your organization employ to perform patch management/system configuration tasks that are incorporated with their other responsibilities?	25. How many system administrators does your organization employ to perform patch management/system configuration tasks on your network as their primary duty?	26. How many months pass between each systems vulnerability/penetration test?
1-4	1-4	0	10-12 +
10 +	1-4	0	1-3
1-4	1-4	1	1-3
10 +	1-4	1	10-12 +
10 +	1-4	1	1-3
10 +	1-4	1	1-3
1-4	1-4	1	1-3
0	1-4	0	10-12 +
10 +	1-4	1	10-12 +
1-4	1-4	1	1-3
10 +	1-4	1	1-3
10 +	1-4	0	10-12 +
10 +	1-4	1	7-9
1-4	1-4	2	4-6
1-4	1-4	0	1-3
10 +	0	0	10-12 +
1-4	1-4	1	10-12 +
10 +	1-4	1	1-3
1-4	0	0	1-3
0	1-4	0	10-12 +
10 +	5-9	3+	1-3
1-4	1-4	1	1-3
1-4	1-4	1	7-9
10 +	5-9	3+	1-3
10 +	1-4	3+	4-6
10 +	1-4	0	10-12 +
1-4	1-4	0	10-12 +
10 +	1-4	1	4-6
10 +	1-4	2	4-6
10 +	1-4	1	1-3
10 +	1-4	0	10-12 +

27. Approximately how many servers reside on your network?	28. Do you believe you have sufficient resources to keep each system patched and configured to meet new security threats?	29. What is your greatest concern with using automated vulnerability/patch management tools?	30. What type of assistance from the DoD would most greatly assist you in your IA efforts?
0-50	No	Other	Funding
0-50	No	Reliability	Tools
0-50	No	Compatibility	Funding
0-50	No	Reliability	Funding
0-50	Yes	Reliability	Training
0-50	Yes	Reliability	Funding
0-50	Yes	Reliability	Training
0-50	Yes	Other	Funding
0-50	No	Effectiveness	Services
0-50	Yes	Effectiveness	Training
51-100	No	Reliability	Funding
0-50	No	Effectiveness	Training
0-50	No	Reliability	Tools
0-50	Yes	Effectiveness	Tools
0-50	Yes	Compatibility	Funding
0-50	No	Reliability	Funding
0-50	Yes	Effectiveness	Training
0-50	Yes	Reliability	Tools
0-50	Don't Know	Other	Training
0-50	No	Effectiveness	Tools
101-150	Yes	Effectiveness	Training
0-50	Yes	Reliability	Funding
51-100	Yes	Effectiveness	Tools
101-150	No	Reliability	Funding
0-50	No	Effectiveness	Funding
0-50	No	Reliability	Training
0-50	Yes	Effectiveness	Tools
0-50	Yes	Reliability	Tools
101-150	No	Other	Tools
0-50	No	Compatibility	Tools
0-50	Yes	Reliability	Tools

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX D. ENTIRE POPULATION – END ANCHORED DATA CODING SPREADSHEET FOR QUESTIONS 5 THROUGH 30

	#1	#2	#3	#4	#5	#6	#7	#8	#9	#10	#11	#12	#13	#14	#15	#16	#17	#18	#19	#20	#21	#22	#23	#24	#25	#26	#27	#28	#29	#30	
Svy1	Other	8+	INC<200	2	2	2	2	2	2	2	2	2	1	2	2	2	2	1			1	4	2	2	1	4	1	2	4	2	
Svy2	CIO	8+	INC201-	2	1	1	1	1	1	1	1	1	1	1	1	1	1						4	2	1	1	1	2	2	3	
Svy3	CIO	2-3	INC<200	1	1	1	1	3	1	2	1	1	1	4	1								2	2	2	1	1	2	3	2	
Svy4	CIO	8+	INC201-	3	3	3	3	3	2	3	1	1	1	2	1								4	2	2	4	1	2	2	2	
Svy5	ISSN	8+	INC<200	3	3	3	3	1	1	1	1	1	2	2	2	1	1	1	1	1	1	1	2	4	2	2	1	1	2	1	
Svy6	CIO	6-7	INC201-	3	1	3	3	3	1	1	1	1	1	2	4	1	2	4	2	2	2	1	2	4	2	2	1	1	2	2	
Svy7	CIO	8+	INC201-	1	1	1	2	2	1	2	2	1	2	2	1	1	1	2	1	1	1	1	2	2	2	2	1	1	2	1	
Svy8	CIO	8+	INC<200	2	2	2	2	1	1	1	1	1	1	1	2	1	2	1			1	1	1	1	2	1	4	1	4	2	
Svy9	CIO	4-5	OUT<200	4	2	4	4	1	2	1	1	1	2	2	1								4	2	2	4	1	2	1	4	
Svy11	ISSN	8+	INC201-	4	4	4	4	4	1	1	1	4	1	4	1	1	1	1	1	1	1	1	2	2	2	2	1	1	1	1	
Svy11	CIO	2-3	INC201-	2	2	2	2	2	1	1	2	1	1	2	2	2	1	1	2	1	2	1	1	4	2	2	1	2	2	2	
Svy12	CIO	8+	INC<200	2	1	1	1	1	3	1	1	1	1	1	1								4	2	1	4	1	2	1	1	
Svy13	CIO	8+	OUT201-	1	1	1	1	3	2	2	1	2	1	2	3	2	2	2	2	2	2	2	2	4	2	2	3	1	2	2	3
Svy14	CIO	8+	INC<200	1	1	1	1	1	1	1	1	1	1	1	1								2	2	3	2	1	1	1	3	
Svy15	CIO	8+	INC201-	3	1	1	1	3	1	1	1	1	1	1	1								2	2	1	1	1	1	3	2	
Svy16	CIO	2-3	INC201-	1	1	3	2	2	2	2	1	2	2	2	2	2	1	2	2	1	2	1	2	4	1	1	4	1	2	2	
Svy17	CIO	8+	INC201-	4	4	4	4	4	2	1	1	2	2	2	2	2	2	1	2	2	1	2	2	4	1	1	4	1	1	1	
Svy18	CIO	4-5	OUT201-	2	2	2	2	1	2	1	1	1	1	2	2	2	1	1	2	1	1	1	1	4	2	2	1	1	2	3	
Svy19	CIO	4-5	INC<200	4	4	4	4	4	4	4	4	4	4	4	1								2	1	1	1	1	4	4	1	
Svy20	CIO	8+	INC201-	2	2	2	2	2	2	2	2	1	1	2	3	1	1	3	1	1	1	1	2	1	2	1	4	1	2	1	3
Svy21	ISSN	8+	INC201-	1	1	1	1	1	1	2	1	2	1	2	1	2	1	1	1	1	1	1	1	4	3	4	1	3	1	1	1
Svy22	CIO	8+	INC201-	3	3	3	3	3	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	1	1	2	2	
Svy23	CIO	8+	INC>100	3	3	3	3	2	1	2	1	2	2	2	2	1	1	1				1	1	2	2	2	3	2	1	1	3
Svy24	CIO	8+	INC>100	3	3	3	3	1	2	1	1	2	2	1	1	1	1	1	1	1	1	1	1	4	3	4	1	3	2	2	2
Svy25	CIO	8+	INC>100	2	2	3	2	2	2	1	1	1	1	3	1								4	2	4	2	1	2	1	2	
Svy26	CIO	8+	INC201-	2	2	2	2	2	2	2	1	2	2	2	2	2	2	2	2	2	1	1	4	4	2	1	4	1	2	2	1
Svy27	CIO	8+	OUT201-	3	2	2	3	1	2	1	2	1	1	1	2	1	1						2	2	1	4	1	1	1	3	
Svy28	CIO	6-7	INC201-	2	1	2	2	2	2	1	1	2	1	2	2	2	1	1	2	1	1	2	2	4	2	2	2	1	2	3	
Svy29	CIO	4-5	INC>100	2	2	2	2	1	2	1	1	1	1	1	2	1	1	2	2	1	1	2	4	2	3	2	3	2	4	3	
Svy31	CIO	8+	INC<200	3	3	3	3	3	3	1	2	3	2	1	2	1	1	1	1		1	2	4	2	2	1	1	2	3	3	
Svy31	CIO	8+	OUT<200	2	3	3	3	3	3	3	1	1	1	2	2	2	1	2	2	1	2	1	1	4	2	1	4	1	1	2	3

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX E. ALL RESPONSE STATISTICS SPREADSHEET FOR QUESTIONS 5 THROUGH 30

Q # 5		Q # 6		Q # 7	
Mean	2.37931	Mean	2.066667	Mean	2.333333
Standard Error	0.181766	Standard Error	0.185282	Standard Error	0.187747
Median	2	Median	2	Median	2
Mode	2	Mode	1	Mode	3
Standard Devia	0.97884	Standard Devia	1.014833	Standard Devia	1.028334
Sample Variance	0.958128	Sample Variance	1.029885	Sample Variance	1.057471
Kurtosis	-0.8984	Kurtosis	-0.87913	Kurtosis	-1.12871
Skewness	0.118182	Skewness	0.49552	Skewness	0.075501
Range	3	Range	3	Range	3
Minimum	1	Minimum	1	Minimum	1
Maximum	4	Maximum	4	Maximum	4
Sum	69	Sum	62	Sum	70
Count	29	Count	30	Count	30
Confidence Level	0.372331	Confidence Level	0.378945	Confidence Level	0.383987

Q # 8		Q # 9		Q # 10	
Mean	2.333333	Mean	1.62069	Mean	1.5
Standard Error	0.187747	Standard Error	0.135132	Standard Error	0.133477
Median	2	Median	2	Median	1
Mode	3	Mode	1	Mode	1
Standard Devia	1.028334	Standard Devia	0.727706	Standard Devia	0.731083
Sample Variance	1.057471	Sample Variance	0.529557	Sample Variance	0.534483
Kurtosis	-1.12871	Kurtosis	2.649576	Kurtosis	3.474654
Skewness	0.075501	Skewness	1.339382	Skewness	1.701912
Range	3	Range	3	Range	3
Minimum	1	Minimum	1	Minimum	1
Maximum	4	Maximum	4	Maximum	4
Sum	70	Sum	47	Sum	45
Count	30	Count	29	Count	30
Confidence Level	0.383987	Confidence Level	0.276805	Confidence Level	0.272991

Q # 11		Q # 12		Q # 13	
Mean	1.266667	Mean	1.5	Mean	1.366667
Standard Error	0.126249	Standard Error	0.149712	Standard Error	0.122083
Median	1	Median	1	Median	1
Mode	1	Mode	1	Mode	1
Standard Devia	0.691492	Standard Devia	0.820008	Standard Devia	0.668675
Sample Variance	0.478161	Sample Variance	0.672414	Sample Variance	0.447126
Kurtosis	8.877688	Kurtosis	4.156476	Kurtosis	7.219289
Skewness	2.942952	Skewness	2.010164	Skewness	2.37972
Range	3	Range	3	Range	3
Minimum	1	Minimum	1	Minimum	1
Maximum	4	Maximum	4	Maximum	4
Sum	38	Sum	45	Sum	41
Count	30	Count	30	Count	30
Confidence Level	0.258207	Confidence Level	0.306196	Confidence Level	0.249688

Q # 14		Q # 15		Q # 16	
Mean	1.966667	Mean	1.566667	Mean	1.142857
Standard Error	0.155241	Standard Error	0.141286	Standard Error	0.078246
Median	2	Median	1	Median	1
Mode	2	Mode	1	Mode	1
Standard Deviation	0.850287	Standard Deviation	0.773854	Standard Deviation	0.358569
Sample Variance	0.722989	Sample Variance	0.598851	Sample Variance	0.128571
Kurtosis	1.483672	Kurtosis	2.057227	Kurtosis	3.138402
Skewness	1.14776	Skewness	1.436444	Skewness	2.201737
Range	3	Range	3	Range	1
Minimum	1	Minimum	1	Minimum	1
Maximum	4	Maximum	4	Maximum	2
Sum	59	Sum	47	Sum	24
Count	30	Count	30	Count	21
Confidence Level	0.317503	Confidence Level	0.288962	Confidence Level	0.163218

Q # 17		Q # 18		Q # 19	
Mean	1.285714	Mean	1.75	Mean	1.294118
Standard Error	0.101015	Standard Error	0.175844	Standard Error	0.113911
Median	1	Median	2	Median	1
Mode	1	Mode	2	Mode	1
Standard Deviation	0.46291	Standard Deviation	0.786398	Standard Deviation	0.469668
Sample Variance	0.214286	Sample Variance	0.618421	Sample Variance	0.220588
Kurtosis	-1.06433	Kurtosis	2.248449	Kurtosis	-1.16571
Skewness	1.023275	Skewness	1.21751	Skewness	0.993609
Range	1	Range	3	Range	1
Minimum	1	Minimum	1	Minimum	1
Maximum	2	Maximum	4	Maximum	2
Sum	27	Sum	35	Sum	22
Count	21	Count	20	Count	17
Confidence Level	0.210714	Confidence Level	0.368045	Confidence Level	0.241481

Q # 20		Q # 21		Q # 22	
Mean	1.294118	Mean	1.15	Mean	1.7
Standard Error	0.113911	Standard Error	0.081918	Standard Error	0.163836
Median	1	Median	1	Median	2
Mode	1	Mode	1	Mode	2
Standard Deviation	0.469668	Standard Deviation	0.366348	Standard Deviation	0.732695
Sample Variance	0.220588	Sample Variance	0.134211	Sample Variance	0.536842
Kurtosis	-1.16571	Kurtosis	2.775855	Kurtosis	3.979013
Skewness	0.993609	Skewness	2.12306	Skewness	1.445108
Range	1	Range	1	Range	3
Minimum	1	Minimum	1	Minimum	1
Maximum	2	Maximum	2	Maximum	4
Sum	22	Sum	23	Sum	34
Count	17	Count	20	Count	20
Confidence Level	0.241481	Confidence Level	0.171456	Confidence Level	0.342912

Q # 23		Q # 24		Q # 25	
Mean	3.133333	Mean	2	Mean	1.933333
Standard Error	0.201907	Standard Error	0.067806	Standard Error	0.165629
Median	4	Median	2	Median	2
Mode	4	Mode	2	Mode	2
Standard Deviation	1.105888	Standard Deviation	0.371391	Standard Deviation	0.907187
Sample Variance	1.222989	Sample Variance	0.137931	Sample Variance	0.822989
Kurtosis	-1.40655	Kurtosis	5.581349	Kurtosis	0.727628
Skewness	-0.60801	Skewness	0	Skewness	1.028411
Range	3	Range	2	Range	3
Minimum	1	Minimum	1	Minimum	1
Maximum	4	Maximum	3	Maximum	4
Sum	94	Sum	60	Sum	58
Count	30	Count	30	Count	30
Confidence Level	0.412946	Confidence Level	0.13868	Confidence Level	0.338749

Q # 26		Q # 27		Q # 28	
Mean	2.266667	Mean	1.266667	Mean	1.566667
Standard Error	0.248829	Standard Error	0.11679	Standard Error	0.123952
Median	2	Median	1	Median	1.5
Mode	1	Mode	1	Mode	1
Standard Deviation	1.362891	Standard Deviation	0.639684	Standard Deviation	0.678911
Sample Variance	1.857471	Sample Variance	0.409195	Sample Variance	0.46092
Kurtosis	-1.77704	Kurtosis	3.701688	Kurtosis	4.070435
Skewness	0.355192	Skewness	2.249556	Skewness	1.513353
Range	3	Range	2	Range	3
Minimum	1	Minimum	1	Minimum	1
Maximum	4	Maximum	3	Maximum	4
Sum	68	Sum	38	Sum	47
Count	30	Count	30	Count	30
Confidence Level	0.508912	Confidence Level	0.238862	Confidence Level	0.25351

Q # 29		Q # 30	
Mean	1.966667	Mean	2.166667
Standard Error	0.169403	Standard Error	0.159621
Median	2	Median	2
Mode	2	Mode	3
Standard Deviation	0.927857	Standard Deviation	0.874281
Sample Variance	0.86092	Sample Variance	0.764368
Kurtosis	0.293101	Kurtosis	-1.05533
Skewness	0.901792	Skewness	-0.01229
Range	3	Range	3
Minimum	1	Minimum	1
Maximum	4	Maximum	4
Sum	59	Sum	65
Count	30	Count	30
Confidence Level	0.346468	Confidence Level	0.326462

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX F. LESSONS LEARNED DURING RESEARCH

Three humbling lessons were learned during the development and analysis of this research project. The first was the incorrect assumption on my part that the survey participants would be more eager to participate since the research was targeted to justify additional resources to facilitate their shortages in information assurance tools, training, funding, etc. The second was the assumption that MS Word could maintain very large files. Lastly, the belief that the electric company would have an uninterrupted power supply during data compilation was an inaccurate assumption.

Surveys in general are not something that people do to pass the time of day. I found myself doing quite a large number of follow up call and emails to encourage participation to an acceptable survey sample size. Since the database was anonymously populated, each solicited participant had to be contacted since there was no way to determine who had submitted a survey response. Anyone attempting to call around the globe should seriously consider purchasing prepaid phone cards or invest in a broadband phone to offset phone usage fees.

Always ensure you know the processing limitation of your software applications. Some applications are not forgiving of those that have not determined this in advance. If you intend to utilize the NPS thesis template, know that graphics and multiple pages of text add to the total file size rather quickly. Documents drafted in MS Word 2002 and MS Word XP docs can be created successfully up to 17 MB in file size. However, minor problems begin at around 13 MB if you start moving anchors, copying & pasting, TOC, indexing, etc. This issue can induce much aggravation and it is much more convenient to configure the maximum file size on Word documents to 12 MB.

When compiling large amounts of information, be sure that your computer automatically saves your information at a minimum of every five minutes. Power outages can occur in Marina, California on sunny days in the same way they occur during severe thunder storm days in the Midwest. Interruptions in electrical power can promote unnecessary increases in the blood pressure and heart rate when your document has not been saved recently...regardless of operating system.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, Virginia
2. Dudley Knox Library
Naval Postgraduate School
Monterey, California
3. Scott Coté
Department of Information Sciences, Code CS
Naval Postgraduate School
Monterey, California
4. Dan C. Boger
Department of Information Sciences, Code IS
Naval Postgraduate School
Monterey, California
5. Captain Sidney D. Rodgers, MSC, USN
Naval Medical Information Management Center
Bethesda, Maryland
6. Captain Richard C. Foster, MSC, USN
Naval Medical Information Management Center
Bethesda, Maryland
7. Captain L. J. Walters, MSC, USN, FACHE
Naval Healthcare Support Office, Naval Air Station
Jacksonville, Florida
8. Captain Nicolas Yamodis, MC, USN
Task Force Web, Commander, Atlantic Fleet
Norfolk, Virginia
9. Commander Wyatt Smith, MC, USN
Naval Medical Information Management Center
Bethesda, Maryland
10. Commander Laura S. Tillery, MSC, USN
Office of the Assistant Secretary of Defense (Health Affairs) and the TRICARE
Management Activity
Falls Church, Virginia