GLOBAL LEADERSHIP

IN COMPUTER AND INFORMATION SYSTEMS SECURITY (INFOSEC)

A Dissertation

Presented to the

Faculty of the

School of Business Administration

Kennedy-Western University

In Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy in Management Information Systems

by

Donald Joseph Gray Chiarella

Hanover, Maryland

Abstract of Dissertation

GLOBAL LEADERSHIP IN COMPUTER AND INFORMATION SYSTEMS SECURITY (INFOSEC)

by

Donald Joseph Gray Chiarella

Kennedy-Western University

THE PROBLEM

We work on computer systems every day in corporate America trusting in our national leaders, local party politicians, military and government agencies, and innovative companies to both guide and protect citizens from computer failures and hacker attacks on our national networks and computers. In deed, we are among the most technologically developed countries in the world (UK, France, Canada, Germany, Japan, Australia) and this study will show we are more vulnerable to terrorist attacks on our computer and information networks. Today, we depend more on systems in command and control and

strategic communications and database systems. We have declassified government secrets in an effort to show good faith to underdeveloped and previously communist countries (USSR and Soviet Satellites) struggling with developing new competitive market-driven economies. We have strong export laws on some high technology products, but those remaining small rogue terrorist foreign states and remaining communist states have a strict doctrine against capitalism. Harvard Business School MBA program and other top graduate business schools specialize in high technology advanced management programs. A western education in government and technology management is prized by many eastern cultures. Foreign enrollees and donors at American University are 13% of the total student population. Does openness and academic freedom of our own democratic society put us in a computer security catch-22 as the number of computer network attacks rises every year with the number of computer science graduates? If so, how are we working to mitigate these risks at the national, state, and local levels of computer security as a component of good computer technology management? How do government and private companies currently work together to ensure top-notch computer information security? Finally, what can we do to improve confidence in computer information security and computer security laws in general in the face of burgeoning open global trade and e-commerce? This paper discusses these problems and proposes simple, realistic solutions and recommendations to the CIO based on the findings of the study.

METHOD

The review of literature in the computer security and information security areas provides excellent insights to where we stand as a nation of secure databases and networks today. Internet searches on various subjects and agency websites and private companies in the information security business provided a good picture of who the president depends on for decisions in addition to the US intelligence community. Interdisciplinary views of management information resources and the computer infrastructure yielded many recent specific US computer laws that have set policy and created new computer agencies. Comparing United States Computer Laws with British computer laws gives us a flavor for just how far we have come and have to go in controlling computer hacker attacks. The number and types of laws will be compared and contrasted. Then we will discuss agency roles in computer intelligence and counterintelligence against foreign countries. The common themes of United States Computer and Information Security Policy countermeasures will be described by various literature, organizations, and agency experiences in the past. A database of the congressionally established Software Engineering Institute CERT will be used to indicate potential concerns in the increases of

hacker attacks in computer networks since 1988. There will be differentiation of the most and least likely types of attacks based on CERT data and SANS institute data on network security best practices. A public advisory of data from the new FBI National Infrastructure Protection Center (NIPC) showed increases in INTERNET incidences of computer crime and hacker attacks on network resources in the United States. Several other data sources were found in the literature search that support the hypothesis that white collar computer crime on the INTERNET is increasing and must be strategically handled inside America's infrastructure today and tomorrow. One book discusses the increase in the number of computer laws both in America and the United Kingdom in the last 50 years. A George Washington University Cyber Policy Institute data report indicates that the number of foreign encryption products has increased during American export control of encryption products. Initially, measures of central tendency and statistics were to be analyzed using Minitab to prove the hypothesis that more incidences of computer crime were occurring in America. This method changed after the obvious conclusions of truth of the hypothesis became clear as evidenced by the increases in a) Presidential Public Press Releases with the words or terms "Computer Technology", b) reported incidences in network crime by the SEI and FBI, c) network crime reported by the Navy and Air Force CERT teams, d) the number of computer laws passed in the last quarter century by the United Kingdom and America. The obvious fact that computer crime is increasing was accepted without running

advanced statistical analysis and the study then focused on identifying best practices in cryptology and computer security in the government to minimize the risk these computer incidences are causing to organizations heavily invested in public and private computer networks.

FINDINGS

Alan Campen in Cyberwar 2.0, Signal Magazine, Proceedings Magazine and other military authors suggest that Information warfare is a reality to be dealt with judiciously under national security. The U.S. Navy leadership is using “network centric” to defeat enemy using information before an engagement starts using military intelligence from satellite and other sensors as input to command and control and then shooting weapons platforms. The NRO and CIA have used various satellite sensors such as CORONA since the early 1960’s. Today’s satellites have 1-2 meter imagery resolution capability through all weather and instant computer feedback to ground stations and a satellite terminal. Milburn, an Australian physicist and student of Richard Feynman, states we are generally headed for smaller and faster light based quantum chip computers in the future. Today, a host of private company “patriots” provide advice to the CIA, NRO, NSA, NSC and president on matters concerning US computer information security. One of these companies providing computer network security policy advice and operational training is

the SANS Institute. To fully understand the computer information security one must know thy enemy better than thyself. Kahn tells us about U.S. cryptology history in “The Codebreakers”. Several ex-Soviet authors tell us more about the state of the Soviet KGB and GRU intelligence agencies and the poor quality of technical computer and communications equipment in the former Soviet Union. The top 10 U.S. IT government contractor companies are also top weapons contractors by no accident. In times of war, the private economy usually gears up to provide industrial war machine capabilities. In the information age this means much better conversion of Information Technology as one component of national security intelligence rather than business intelligence. Microsoft, Oracle, Software AG, Dell, and other IT market-share leaders provide product support to government agencies requiring better information and computer security. Teamwork and strength of character means a lot in this business. A government agency or government contractor must also stay abreast of new standards changes at the NIST Computer Security lab in Gaithersburg, Maryland. The standards can help tell the manager what current laws are already implemented by government agencies and what laws may be obsolete. NIST standards for the computer network environment security are discussed. A beta product that does not receive certification will not be used on secret projects according to the “Orange Book Series” classified processing standards at the National Computer Security Center at Fort Meade, Maryland. Only people with the “need to know” may have access

to certain information, computer or otherwise. The role of cryptography is discussed in how it may help an agency improve privacy and security. State government has the additional burden of state laws and regulations on computer security. This study will show how an analysis of the probable recent computer network attacks by hackers on national networks can be used to thwart attacks here in Maryland and improve the state of security on our computer information systems. There will also be discussion of the scalability problems faced by small local agencies and larger data processing agencies when ensuring computer security. Networks, operating systems, and databases all have different types of computer security hardware and software that we explore and use on daily basis. Software networks of today are capable of encrypting our every message without our intervention or permission as agents of government organizations. James Martin provided an excellent “Onionskin” layered model for all computer security which will also be discussed for application by security managers and consultants (Martin, 1982). This paper will then provide workable strategic solutions such as reform in computer security education under a new university discipline, a new role under the CIO and CEO, encryption techniques and algorithms to be applied, and a framework for better computer security by the government and non-government computer executive alike. It’s significant that William Jefferson Clinton appointed 21 technology experts to consult current president George W. Bush and vice president Richard Cheney on the last day of his administration.

Mr. Clinton was kindly turning the reigns of the most powerful technological society over to the new administration. The data on press releases technology subjects showed that Mr. Clinton learned over his tenure that technology drives the new information age economy and employs people in all sectors of society. This paper shows that the United States takes the global lead in Information Security (INFOSEC) component of INTERNET technology including satellite intelligence, network centric theatre-wide battlefield strategies, biometrics, network administration, applications development, encryption methods, and NIST Standards. And yet the comparison of Foreign Computer Laws with United States Laws suggests other countries (democracies) may be learning and developing their own capabilities in INFOSEC. In fact, foreign encryption algorithms grew in number when United States restricted access to our more secret algorithms. Foreign countries have become much less dependent on the United States as sole producer of encryption products, which is good for global prosperity. The data in this report shows the United States currently leads other countries in INFOSEC and will continue to do so into the 21 century. Some data is presented that indicates how the United States households have increased purchasing of INTERNET and stand alone computers and cellular telephones in the last decade. This is evidence of our economical dependence on computer technology and the high level of market saturation of the information age in our society. The data looks at age, education level, region of the country, and racial composition of computer new

household users. We have a resilient armed services and congress who help to ensure security of national INFOSEC resources and government secrets. America leads because it has legislated innovation since the birth of our nation and because our free democracy allows engineers, managers, and programmers the freedoms they can not find elsewhere in the world. America is the hope and shining star of the sometimes clandestine INFOSEC global community. We lead in INFOSEC and Intelligence products using the constitution and free enterprise system given to us by our forefathers. We lead in high technology because we always take pride in being the largest, most generous technology factory in the world since 225 years ago (1776 signing of Declaration of Independence). Our forefathers would be amazed at how leaders of today use the lessons of their struggles in the Revolutionary War and innovative new technological ideas of the information age to protect global freedom. The data shows we must keep a vigil on computer criminals and computer terrorists to maintain U.S. dominance in the technological 21 st century on the other side of the bridge.

TABLE OF CONTENTS

CHAPTER

Acknowledgements

The people around us make us better. I've been blessed to have wonderful people around me all my life. Any work that takes time is using your most valuable resource. My family has been understanding about my zeal to complete this project. My co-workers have watched me bury my head in the computer screen for hours at a time. My parents, Don and Greta, brother Tony, and my wife, Mimi have been supportive of my academic projects all through my life. I would like to thank the following people who helped me understand computer security and information systems security over the years from inside the federal government: Colonel Charles Bruce Morris (US Army Retired), Mr. Jerome Nelson (Navy Civil Service), Commander Alan F. Stonebraker (USNR Retired), and Ms. Margaret Truntich (GSA Civil Service). All of these people had the patience to answer my questions about good computer security practices during source code implementation and policy projects on their staffs. Thanks to the directors at University of Maryland University College, Dr. Nick Duchon and Dr. Sam Bhaskar for the teaching assignments and time to complete the requirements for this Ph.D. My current boss, director Manu Shah and supervisory friend Bob Cunningham have been great friends and colleagues in safety engineering and have been very supportive whenever I had academic needs and questions related to computer sciences and the business processes we manage at

State Highway Administration to make a difference in the world.

Dr. Carol Rollins was very positive about my entrance into the Kennedy Western University Ph.D. program and never gave up on me, even after I tried once and was distracted from the program by real world activities in 1998. She helped nurture me towards the academic goals I have always aspired since age 8. Then, while living in Topeka before moving to Maryland, I said I was going to the University of Kansas to become a Jayhawk. I'd like to thank those at Kennedy Western who wrote the online software as it has been very easy and convenient to use through INTERNET and is the way of the future.

I would also like to thank my close friend John Paul Pellechia, my college roommate at University of Maryland, who went on to graduate studies at Penn State and later worked at the Defense Intelligence Agency and always gave me more courage to see things through. He has been more than a great friend when I needed one most. I'd like to thank my current best friend Maryland State Trooper Guy Ramsey who is a champion for goodness in life and always gives me hope for mankind with his great attitude, kind words, and winning ways. I'd also like to thank those officers and fellow cadets in Air Force Academy squadron 18 in the class of 1978 and the staff of the Air Force Academy who showed us how to "push the envelope". "78 is Great!!".

My father provided a lot of inspiration for this project and degree when he told

me about his classified work with the Air Force and Navy after president Clinton declassified information on military projects that were once top secret. My father always has good advise and has kept watch over me since college. My mother and wife have put up with my moods and intensity on computer related projects. Mom always said I was the best in mathematics. I'm also a blessed and richer man for having had such good children as Donald, Mia, David, and Michaela. They have instinctively helped me be a better father. At my NSA interview I scored in the 90th percent on the Psychology Tests, yet I was not selected by the agency even though I had held secret clearances on many software projects before that in private industry and had 18 years federal service and I had taught NSA workers college courses through University of Maryland and Anne Arundel Community College. I'm sure the person(s) making the hiring decision had their reasons. It's like we learned in sports, take the bumps and bruises and losses with the victories and always keep the faith.

Finally, my pastors, United Methodist Chaplain Kristi Pappas, Steve Austin, Presbyterian Chaplain Greg Tyree, and friends at the Fort Meade Historic Chapel Protestant congregation have always been supportive despite my poor attendance at times. God gives us all many friends and gifts that we steward for the goodness of mankind while we are alive. Thank God for giving me insights required to complete this project and thank everyone who has helped me over the years.

Since most of the research on this project was done in my spare time, any errors in this dissertation are mine alone and not attributed to any others involved in interviews or interpretation of reference readings or website query results. Great thanks to all who helped me understand the dissertation process and subject matter.

Cordially Signed,

Donald JG Chiarella, Ph.D. Candidate

Kennedy Western University

LIST OF FIGURES

Figure

LIST OF WEB SITES

Website Sponsor Name **URL Address**

1. Federal of American Scientists…….www.fas.org
2. Software Engineering Institute CERT at Carnegie-Mellon University……www.sei.cmu.edu
3. National Security Agency (NSA) National Computer Security Center ……..……..www.nsa.gov
4. National Institute of Standards and Technology (NIST) Computer Security Laboratory……..……..www.nist.gov
5. General Service Administration (GSA) IT Policy……..www.gsa.gov
6. SANS Institute……..……..www.sans.org
7. Department of Energy CIAC……..……..www.ciac.gov
8. Central Intelligence Agency (CIA)……www.cia.gov
9. Library of Congress……..……..thomas.loc.gov
10. United States Senate……..www.senate.gov
11. White House……..……www.whitehouse.gov
12. McAfee Inc……..……..www.mcafee.com
13. Software Technology Conference (STC – Hill AFB Utah)……..…….www.stc.org
14. US Navy……...www.navy.mil
15. US Army…….www.army.mil

16. US Air Force……..www.airforce.mil
17. US Marines Corps……www.marines.mil
18. National Aeronautics and Space Administration……....www.nasa.gov
19. Federal Communications Commission (FCC)……www.fcc.gov
20. Government Accounting Office (GAO)……..……www.gao.gov
21. Office of Budget and Management (OMB)……..….www.omb.gov
22. George Washington University (National Law Center) ……..……www.gwu.edu
23. GW University Cyber Policy Institute……..... www.cpi.seas.gwu.edu
24. American University (Law School)…….www.american.edu
25. University of Maryland at Baltimore (Law)…….www.umd.edu
26. National Defense University (NDU)…….www.ndu.edu
27. Naval Postgraduate School (CISR)……..www.cisr.nps.navy.mil
28. Villanova Law School (US Code Online)……...www.villanova.edu
29. University of Edinburgh…..……..……..www.edinburgh.edu
30. St Andrews University……..……..…….www.standrews.edu
31. Harvard University JFK School Government……..….www.harvard.edu
32. Washington Post……...…..…www.washingtonpost.com
33. Wall Street Journal……..…www.wsj.com

34. New York Times……www.nytimes.com

35. Armed Forces Electronic Communications Association (AFCEA).. ……..www.afcea.org

36. Association of Computing Machinery (ACM)……..www.acm.org

37. Institute of Electronics and Electrical Engineers (IEEE)……. ……www.ieee.org

38. Rutgers Technology Law School……www.rutgers.edu

39. Concord Online Law School……..…….www.concord.edu

40. US Air Force Academy……..…….www.usafa.edu

41. US Naval Academy……..www.usna.edu

42. US Military Academy……..……www.usma.edu

43. Johns Hopkins University (JHU) Applied Physics Laboratory ……..……..www.jhu.edu/apl

44. Capitol College……www.capitol.edu

45. University of Maryland Baltimore County……...www.umbc.edu

46. University of Maryland University College……..…www.umuc.edu

47. University of Baltimore Law School……www.ubalt.edu

48. US Navy Civilian Human Resources……..…www.donhr.navy.mil

49. Federal Bureau of Investigation (FBI)……..www.fbi.gov

50. Maryland State Government……..…….www.mec.md.state.us

51. Computer Sciences Corporation……..……...www.csc.com

52. Lockheed-Martin Corporation……..……..www.lockheed.com

53. Bell Atlantic Network Integration……..www.bani.com

54. Orkand Corporation……..….www.orkand.com

55. Telos Systems Engineering……...……..www.telos.com

56. Mnemonic Systems…….……www.mnemonic.com

57. Richard S. Carsons and Associates……www.rscarsons.com

58. Pentagon……..….www.defenselink.gov

59. Defense Information Systems Agency (DISA)……..www.disa.gov

60. Defense Intelligence Agency (DIA)……..……...www.dia.gov

61. Government Executive Magazine……...www.govexec.com

62. IEEE Cipher Newsletter……

……..www.itd.nrl.navy.mil/ITD/5540/ieee/cipher/cipher-archive.html

63. Department of Justice……...www.cybercrime.gov

LIST OF APPENDICES

Appendix Name

Global Leadership in Computer and Information Security

Chapter 1

Statement of the Problem

Leadership in Computer and Information Security in the 21st century is crucial to National Security, economic fitness, and global trade markets of America. There is so much technology used today, that computer security has become a business that quite often makes the daily news headlines. Hollywood made a movie called "War Games" that highlighted the teenager hacker problem in government systems. The movie "Independence Day" showed a way to destroy alien invaders using a computer virus to disrupt their systems command and control. The novelist Buchannan wrote a fiction book called "Virus" that talked about Iranian terrorism hacking and destruction of our space anti-ballistic missile defense network in the year 2010 by unleashing a computer virus. Novelist Tom Clancy wrote a book called "Net Force" to describe government (FBI) enforcement of "Net Laws" in the year 2010 against computer crackers. This study quantifies the real national computer security crisis and then describes some solutions and recommended operational programs to keep organizational computer security policies sound and fit. The paper is divided into 5 parts or chapters and each part plays an integral role in defining aspects of the problem and solutions of global

leadership in computer security. The computer and "Information Age" did not just start yesterday, but the solutions and recommendations to improve Computer and Information Security have been with us for some time as the computer industry has matured. As computers proliferate in every market (and INTERNET), we will see more occupational evolution in the computer industry in the computer security officer position. Once computer security was a delegated task to ensure systems data is backed up and recoverable from disaster; now the security officer plays a much more active role in assessing internal vulnerabilities and monitoring potential threats to networks and personal computer workstations. These threats come from malicious and non-malicious sources outside our computerized communications network systems. The loss of a computer network can mean millions in lost revenue to a company and pure panic on the part of the end user community. This lost cost of operation is a formula that can be used by the computer security officer to report data loss value to superiors to impress the importance of having good computer security practices in place. The idea is that data is a valuable resource to the organization and any corruption or loss of data from any means, is unacceptable as businesses can not run on zero data. The formal definition of "security" in the Encylcopedia of Cryptology is "protection against any form of unwelcome intrusion" [Newton, 1997]. Unwelcome intrusion incidences are more prevalent in the year 2001 than they were 10 or even 5

years ago because more people are networked through INTERNET than ever before and as the number of valid visitors to a server go up, so do the number of hacker attempts according to the FBI. How does one decide who is friend and foe? How does the organization cope with the influx of potential threats when president Clinton mandated INTERNET wiring of all U.S. schools and educational assets to bridge the "Digital Divide" between social classes in America. Foreign hacker threats to the U.S. national infrastructure are sure to take advantage of the mask provided by the increased network traffic in America. In military agencies of the federal government, the "Information War" has replaced the Cold-War and the FBI is mobilized to fight white collar crime and foreign counterintelligence on the computer cyberspace battlefield. This paper shows data that proves there are more incidences in computer security and will show how the layman and professional can protect his computer assets from devastation with better understanding and countermeasures. Some of the recommended solutions are simple, others require basic to advanced understanding of computers, programming, and communications electronics. On the whole, if the national computer security policy is to be successful, the computer savvy society must help the unsophisticated computer newcomers with practicing computer security in their daily routines. By reading this study, you will ensure that you understand some of the basic principles and reasons behind national Computer and Information Security

efforts and the countermeasures one can use in a networked computer environment.

Importance of the Study

The importance of leadership in national computer security has been recognized since world war II when computers helped research the first atomic bomb and decrypt German and Japanese diplomatic messages. In Vietnam, the U.S. used computers extensively for military intelligence analysis from bases in Hawaii [McChristian,1974]. Intelligence is always required to be sure of our friends and foes intentions in national politics. It is this role which computers play an increasingly important governmental role by crunching large amounts of data into intelligence information. Two historic incidences show the international importance of military intelligence. First, no-one predicted attacks like the one on the U.S.S. Liberty unarmed Intelligence ship by Israel in 1968 during the 7 day war that killed 34 U.S. sailors [Ennes, 1979]. The more famous intelligence debacle occurred at Pearl Harbor when a Japanese coded diplomatic message about the attack that was late in arriving in Washington and the US declared war on Japan. Japan was dishonored by the fact that they had started an undeclared war due to the mistake. It was the greatest one sided victory at sea in the 20th century due to poor United States intelligence and failure of human operators and

technology to detect the attack earlier [Kahn, 1968]. As the U.S. has used technology more wisely as a primary defensive weapon espoused by the Cold War nuclear détente, the world has made presumptions about America's intents regarding technology, in general. For instance, Communist party Chairman Mao Tse_Tung stated "The atom bomb is a paper tiger which the U.S. reactionaries use to scare people. It looks terrible, but in fact it isn't. " in 1946 after the atomic bombs were dropped on Hiroshima and Nagasaki. President Truman made the decision to end the 5 year war and save 1 million American soldiers during a probable bloody invasion of Japan estimated by his military intelligence [Meisner, 1996]. Chairman Mao indicated his lack of understanding of the new role technology played in the American mindset to ensure freedom against global tyranny. Mao basically stated that more people are the power, not the technology. Mao had a country of 2 billion in population; the most of any nation with no advanced technology. The United States on the other hand had a modest 200 million people and used technology to even the odds in a growing sophisticated world. Indeed, Truman created the NSA for the sole purpose of improving our national intelligence capabilities after world war II and NSA exists today in the largest intelligence community in the world [Kahn, 1968]. The U.S. has opened communications and trade with China for the first time in 25 years since president Nixon recognized during the Vietnam War that China backed North Vietnam interests.

We are now normalizing trade relations with China. The new post cold war world has provided prosperous times for the U.S. economy and more global peace, however many nations like China, Iran, Egypt, Balkans, and even Russia pose continuing threats our national Information Infrastructure by the mere existence of new nuclear arsenals of their own [Clawson, Bittman, Meisner, Suvorov]. This is important in our discussion because computer technology is the underlying technology that helps the U.S. maintain nuclear defense superiority as described on the website of the Federation of American Scientists. Through technology transfer from the military world, businesses can apply computers to most tasks effectively. The computer drives the data and intelligence of most businesses in terms of performance in the marketplace. In fact, the technology transfer process is so efficient that the president and congress regulates computer exports to foreign countries. A study at George Washington University Cyber Policy Institute has shown that during the regulation of computer encryption software and hardware exports from America, foreign countries have developed their own computer encryption software. The regulation may have had the reverse affect of improving foreign countries ability to develop their own computer encryption software, especially in Great Britain (Figure 14). The FBI has been tasked to assist with national computer security in recent years as computer technology usage has grown in free democratic societies and cultures [FBI Laboratory Annual Report

1999] and more threats to national infrastructure have been identified through data collected on hacker attacks. In 1984, Congress created the Software Engineering Institute at Carnegie-Mellon University and CERT to warn of malicious software. The data collected by the SEI CERT group supports the hypothesis that computer crime is increasing with computer usage (Figure 4). Recently, after the Year 2000 celebrations, "denial of service" attacks crippled several corporate networks for several days causing loss of business revenues. This type of attack is one that the FBI has coined a political event times attack. The origin of the network attacker was traced within in the United States with much difficulty. The algorithm tied up the communications lines by appearing to be many users logging on or "handshaking" at the same time, thus locking out valid network users ("denying service"). Information warfare of this sort is a reality of technology and the information age (Campen, 1998) and extends into e-commerce and business espionage. The U.S. must be forever vigilant against computer attacks on our national networks, supercomputers, military command and control systems, agency systems, and private corporate management systems. Few people fully understand the entire scope of this issue from politics to algorithms. The president has issued more computer system technology public press release statements than any other single issue according to his White House website (Figure 1). Some have been to create new computer security units and some have

been to explain that we are committed to improving computer literacy among our children. The stock markets have soared thanks to high technology stocks valuation in the great 1990's bull market. Federal IT executives and DOD systems contractors have a good understanding of the problem. Anyone who has experienced a loss of data on a computer hard drive by accidental means knows the value of a planned system backup. This study will look at the indicators of the increased magnification of the problem of national computer security including new computer laws and foreign computer laws. It will enhance the reader' s understanding of the need to ensure that the U.S. protect against those who would try to defeat the freedoms of democracy citizens have under the U.S. Constitution by subverting our primary computer and communications resources. Specific time-tested strategies and solutions are offered to improve corporate and personal computer network security and take a defensive stance during a troubling growth in computer crimes that the layman may not be familiar with [Martin, 1984]. Chapter 5 of this paper will give the reader a group of computer security activities that can be implemented in an organization by the professional computer security manager or by the novice end use. One does not have to write computer software to enforce good computer security practices. In fact, the reader will find that physical security of computer resources is the "outer" layer of an overall defense system of several combinations of techniques. Specific algorithms can be

written using RPC to undermine or “tunnel” under the network level protocols in the standard telecommunications protocol model [Bloomer, 1998]. The importance of following a prescribed successful methodology to ensure computer and information security can not be overstated. The SANS institute prescribes certain network administration best practices for it’s governmental customers and students. A good incidence recovery strategy could save your computer system operational data assets from being totally lost and result in corporate bankruptcy.

Purpose of the Study

This study examines the extent of increase in computer crimes and security incidences reported to national sources of the United States government to prove the case for more enhanced national and private network infrastructure protection. The results will show how the United States leads the world in computer security laws and computer sciences education and assumes a most responsible position as a result of our national technical prowess. This leadership is related to the hard work of thousands of well-trained scientists and managers who have an understanding of the severity of the current deluge in computer viruses, hacker attacks, and possible foreign penetration attacks into our computer systems. The attacks will come when we are least expecting them according to the SANS institute. The data will prove the trends

that mandate more scrutiny by all IT managers and workers to ensure increased computer security in the future. To say the U.S. has a computer security crisis is an understatement once you understand the U.S. computer security policy and standards history through the literature, the current computer crime data trends, and how much some nations would like to control and/or destroy our computer infrastructure. The study will also enlighten both the reader and the researcher to the renewed requirements for excellence in computer security management planning and IRM acquisition in the government and private sector partnership agreements.

Overview of the Study

The typical US computer sciences and management information systems graduate student is only taught the basics about computer security unless one has actually had tasks assigned that require advanced thinking about the topic. Most people do not assume to be attacked, but this is a primary assumption for a good computer security officer. In other words, a little paranoia is a good trait in a computer security officer. This person should be high enough on the organizational chart to report directly to the CIO, CFO, or CEO level.

The fact that foreign nations send so many people through American business and management university programs to obtain legal and high tech perspectives they

could not receive in a non-western culture is a testament to our global reach. Some of the best breakthroughs in United States technological innovations have been by scientists who have migrated here from other countries such as Andrew Carnegie, Albert Einstein and Werner Von Braun. Traditionally, cryptology and cryptanalysis has been the domain of mathematicians (AlanTuring) and authors (Edgar Alan Poe) who had an interest in secret writings [Kahn, 1968]. All government diplomats have a need for cryptology and enciphering codes as described by Kahn [Kahn, 1968], and Bauer [Bauer, 1997]. As modern information technology has matured, computer security has become more academically important such as the Mathematics 400 level course in Cryptology at the University of Maryland, College Park. The federal government has compiled a host of computer security related laws and standards which include various crypto algorithms. The NSA provides our best computer security program evaluation standpoint with a standing policy on classified systems access [Orange Book]. The president has recently changed the rule on declassification of government secrets and reduced the time frames on classified information from 25 years to 10 years [Federation of American Scientists, 2000]. This hurt rather than helped the U.S. disguise computer technology secrets. Additionally, fewer congress elected officials had military experience in 1999 than in 1993 (Figure 2) due to a natural decline in WWII veterans. This is a troubling statistic that means our top decision-makers in the future may not

have any working level understanding of technology or how it is used for political advantage. Yet, they will most certainly be well versed in using positive information and negative dis-information to gain elective office. The U.S. as a nation can not afford to assume it will be treated fairly by the entire world given the terrorist attacks on government building in Oklahoma City, NY World Trade Center, and Pan Am Flight 103 over Lockerbie, Scotland. In this area, this paper explains why the U.S. must always remain on guard against infrastructure systems attacks which will be much more silent in nature than actual explosives, but just as deadly. Surely, most Americans are aware that computer technology has had widely reported incidences and that the general public never knows all the actual threats to national security. It is not good security practice to publish too much about security in the public forum. The word is not “prudent”. There are some 230 nations and we can not rationally hope to be allied with them all. This study assumes that the United States has many global economic trade interests and computer security is both a national security and economic issue. This study will use facts, data, and summary data to describe the current computer security crisis in America. An assessment of how one can proactively manage and reduce the crisis according to experts in computer and communications security will also be described [Martin, 1984; Pfleeger, 1989; SANS Institute, 2000].

Problem Details

The problem of funding more resources to government and corporate computer security in our national infrastructure is best approached from a rational statistical method to prove the problem has increased in recent years as Internet and other computer and communications technologies expand throughout the world. Yet governments and corporations are asked to do more with less resources. It follows that once one can show that the computer security problem is skyrocketing, that one can obtain funding in Washington to help prevent the computer crimes and malicious behavior of certain people intent on developing worms, viruses, Trojan horses, logic bombs, against government agency networks (Morris vs. NSA). Even though Washington has been very active in creating new computer laws in recent years by the increased number of computer security laws, congress must do even more as the U.S. experiences more malicious computer network activity and the number of intellectual property copyright violations has skyrocketed (Napster hearings). Aggrandizing computer criminals such as Mitnik in Congressional hearings may create heroes for young computer users instead of training them in ethics. Current graduate computer sciences departments are teaching enough about the mathematics of systems sciences. What they must also teach are the accompanying “computer ethics” and

behaviors that are required and expected of adult professional computer staff members. This was seen in the recent "Love Bug" virus student who demanded attention in a Phillipines computer course and was even identified by an instructor as having "criminal behavior" and intents [Time Magazine, May 2000]. This is a sadly recurring theme in computer security over the past few decades. Unfortunately, the technology is not as weak as the human ethical instincts of the computer criminal. One solution is to improve ethics education in undergraduate programs and on the job with written contracts of ethics in computer activities as recommended by the Association for Computing Machinery (ACM). Can an increasingly large contingent of security people avert a future communications network crippling crisis in 2020 when computers will write their own software? Furthermore, the larger question this paper addresses is what management resources can a young manager look to in order to fully understand government national computer security and best practices in both policy and operations level organizations?

Rationale of the Study / Developing an Hypothesis

The hypothesis of this study is that America has become so dependant on electronic systems and computers that often times America seems to underestimate the motives of foreign nationals and internal threats who would like to destroy the U.S.

communications infrastructure. The fact that there are more penetration attempts to systems as recorded by the SEI and FBI is an indication that America needs to improve laws to make American computing safer as well as developing new encryption algorithms to replace the old. Where is America going in the future development of both embedded and stand alone computer systems? There are futurists like Alvin Toffler and John Naisbitt who tell us (and congress) where society trends may be going. Gordon Moore's law (Intel Corp) says computer chip technology evolves to faster speeds and smaller designs every 18 months. But how long can systems get smaller and faster? Will they be more secure? There are physicists who say a limit will be reached based on quantum physics and Richard Feynman's photon light molecular processor [Milburn, 1998]. According to Gerald Milburn, a photon of light is the smallest molecular particle that a bit of data, either 1 or 0, can be represented in quantum physics and eventually computer chip firmware. In addition to speed and size reductions, light based computing is more secure. Fiber optics communications wires are very highly secure and can detect an intruder on the wire easier than copper wire. Milburn expects similar secured light characteristics to improve these systems as internal breadboards and buses convert to light signal carrier. Developing more advanced cryptographic algorithms also helps determine how much more secure American software systems will be in the future. This is the invisible war against

computer viruses (worms and replicating malicious software) that can spread through email and disable large networks in a matter of hours.

The secondary hypothesis will be that given the U.S. is experiencing more computer attacks on resources, one needs a set of managerial and technical solutions that will help combat computer security frauds in the future given that there is a crisis. These solutions include the security "layering" concepts as explained by James Martin and extending this concept to include several new layers of computer security. An annual risk assessment and risk mitigation report to management done by a computer security trained staff member is another tool to improve computer security based on observation of the environmental elements and identification of potential threats. Every known virus has antidotes programmed into good computer security virus detection software that correct software and eradicate any signs of computer bacteria on hard disks. Network security, often called "Information Security" is also needed to contain the spread of computer worms that replicate in an operating system. The SANS institute has a plethora of countermeasures in this arena. What new tools can the new computer security manager use to incorporate good practices into his daily regiment? Automating the virus cleaning procedures into boot up procedures is another protection we have from viruses.

Scope of the Study

Despite a clear hypothesis that can be drawn from the study, limitations to the study exist. The data is limited by the political goal of alerting the public to the need for more computer security and development of new computer security hardware, software, procedures, and education and training. Many a savvy politician and researcher can make statistics tell whatever "truth" he or she wishes given enough time to find the right data or study. Data used in this study is from reputable sources and will change over the next few years. A post study analyzing how the numerical changes actually compare to the predicted changes and interpolations of data lines would be wise at a later date to verify the statistical confidence level of the predicted numbers of hacker attacks and hotline calls to the Software Engineering Institute (SEI). Most of the solutions are a matter of perspective of what has worked well over a career of 25 years and what is practical and inexpensive to implement in any computer network systems environment as good practices learned from federal agencies, academic, and private industry guidelines. This study will discuss the importance of management funding from Congress for all computer technologies. The NIST Computer Security Lab produces publications that discuss computer security management practices can sometimes be confusing to follow. Computer security resources are integrated into the

whole federal computer technology budget which will be discussed in charts. We must develop better government contracting methods to ensure the best systems at the best value to taxpayers. This study will also cover indicators from White House press releases for the year 2000 that show a higher level of commitment and concern for national computer security management improvements. Seven years of press releases are available online at the White House website which can be analyzed. One would hypothesize that more resources are being channeled towards the engineering and computing sciences in recent years by both government and specialized corporations. This is amazing as government contractors do not always make profits on government contracts that are commensurate with civilian commercial contracts according to Government Executive Magazine. Only for the most "patriotic" reasons would computer companies invest more in government than commercial businesses. However, the government's computer requirements are much more unique and companies can not always transfer technology from military systems. On the other hand, the Escrow Encryption Standards are an example of a computer security algorithm that originated in the private sector and was adopted by the federal government for use in all business lines of the government. Thus, the US government of today is a large corporation (ranked in top 5 in the world) demanding application of more cost-effective decision sciences applied to help reduce waste in business line

areas including computer systems. This paper also looks at the need to prevent other nation-corporations from owning stock majorities in the national computer and telecommunications industry. Germany and Italy are heavily invested in US computer assets according to Government Executive. History suggests that America can not trust either of these countries as demonstrated in World War I and II. The US Congress regularly convenes on these types of international regulatory issues.

Definition of Terms in Chapter 1

The terms used in this study are outlined in the glossary and definitions section, but several main definitions are described here for use during the development of the primary hypothesis that "computer laws and incidences in the United States are increasing over the past few years" and secondary hypothesis the "there are definite managerial and technical programmatic actions that help prevent (counteract) computer security breeches". Please refer to the glossary for the proper decoded acronym as well as definition of an unfamiliar term. It is common in government writings to go overboard on acronyms, but that is a fact of life in any academic discipline where one may wish to memorize many different names in our small jargon code-words. Hopefully, the glossary is as well developed and will help understand the terms in this study. It should be noted that these terms have been collecting in the researcher's and

industry's vocabulary over the past 25 years and that certain terms have evolved such as "netizen", which today indicates citizen rights on Internet. Other terms have been around many centuries such as "crypto-code" which was used by early Eqyptians in the form of hyroglyphics. Although root word histories are not given, the reader should understand that this dichotomy exists.

Primary Terms for major topics used in this chapter include:

1. "Intelligence" – gathering of data pertaining to learning about an enemy or foe.
2. IRM – Information Resources Management meaning to acquire and manage information resources which include people, computers, data, procedures, files, and processes.
3. NIST – National Institutes of Science and Technology who published federal standards in technology including computer security from the Computer Security Laboratory.
4. "Risk Mitigation" – to solve certain high risk management problems with countermeasures that reduce risk at least cost to the agency.
5. FBI – Federal Bureau of Investigation or Fidelity, Bravery, and Integrity from inside the agency.
6. ACM – Association of Computing Machinery in New York.

7. NSA – National Security Agency at Ft. Meade, Maryland.
8. CSPAN – Cable TV network.
9. "Netizen" – A person who uses INTERNET and is a citizen of the United States of America with certain rights under the US Constitution.
10. "Crypto-code" – the codes used to make a message unreadable to human eye on initial view (without further analysis).
11. "Countermeasures" – an action that is intended to fight computer security attacks and incidences in our society and computer networks.
12. "Intruder" – an unauthorized person in a government or private computer network or operating system. Related to "intruder detection" software in computer networks.
13. "Statistically confident" – a measure of the 95%, 99% rankings or above probability of being a significant statistic using confidence intervals on a normal distribution.
14. "National infrastructure" – the United States computer network and computer database resources as developed since 1960's early DARPA INTERNET project.

15. DARPA – Defense Advanced Research Projects Agency.
16. “Computer ethics” – the application of rules of operation to the computer industry and computer programming practices.
17. ”Orange Book” - The NSA series from the National Computer Security Center on classified information treatment.
18. “Intelligence community” – The United States agencies involved with intelligence gathering and reporting to the CIA headquarters in Langley. Virginia.

Review of Related Literature

Chapter 2

Introduction

What defines good computer security and communications policies and practices in today's electronic world may be as varied as the number of companies who specialize in Information Technology. Certain texts in the literature focus on the problems and causes from a historical perspective [Kahn, Bauer, Nagle, Tannenbaum, Sapronov, Barrack] and others focus on the required laws and changes in future society to make effective "living" computer security policies that can be changed rapidly by new state and federal government laws [Bainbridge, Martin, SANS Institute, NSA "Orange Book" Series, NIST FIPS PUBS]. Even more texts describe the cold-war and post cold-war foreign national interests that are served by the infection and destruction of United States computer networks [Bittman, Clawson, McChristian, Suvorov]. Clearly, numbers suggest that the "Information Age" has given rise to many more computer security "incidences" from 1988 through 1999 as counted by the SEI at Carnegie Mellon University. There are authors who have discussed how computer security has become a race to encrypt emails, databases, websites and other electronic resources over time since World War II (Bauer, Campen, Newton) in what is called

"Information Warfare". This may be warranted concern. There are more organizations now than ever before to help deal with the increase in hacker attacks evidenced in the last twelve years. These organizations have websites designed to help with the identification and detection of white collar computer crime [FBI, SANS Institute, NSA, SEI CERT]. Government and private agency alike are stakeholders in the safeguarding of national computer networking resources. Practitioners would be wise to develop resources that help with managing the influx of computer security incidences predicted for the future. Harvey Deitel and Chris Date provide valuable insights into computer security best practices in Operating Systems and Database Management Systems in specialized chapters of their books. There are many things that the literature suggests Americans can do to protect computer resources [Bauer, Campen, Newton, Martin]. Finally, Paul Strassman, a past DOD computer head discusses shows us why typical executives usually have no clue as to why computer security is important to the overall health of the business.

Early Government Contracting

When America was in the making, congress created a committee with the sole purpose of acquiring military equipment for the Continental soldiers of General George Washington [Nagle, 1992]. America has used acquisition committees in congress as

the primary way we manage government business that is outsourced. This includes the way the government has grown to depend on computers that are embedded in weapons systems and on desktops. Every war America has participated in has required new and unique types of military equipment which today always includes computers and communications electronics. The government could not operate without the help of IT contractors who are responsible for electronic communications and communications security threat mitigation and evasion. Many of the companies who specialized in US equipment such as warbirds, bombers, missiles, helicopters, submarines, air craft carriers, and other combat systems, also have divisions to specialize in electronic data equipment which make them good candidates for government IT computer security contracts (Figure 10-13). Government contracts are the primary method that the US government receives most of it's deliverables**.** Indeed, the George Washington University National Law Center teaches government contracting in a very popular executive development program in Washington DC that has graduated congressional representatives among the hundreds of agency faithful. Professors emeritus Ralph Nash and John Cibinic run an admirable educational program for federal government contract managers and have created books that help with the many laws and regulations concerning government acquisition of computer equipment and software (Nash & Cibinic, 1993) that is used in computer security such

as the “clipper chip”. Many times acquisition of computer security resources requires in-depth knowledge by the contracting officer of “Fortezza”, “PKI” and “RSA” encryption methods for communications applications, “Trusted” database and operating system software, and “Tempested” hardware.

Recent Computer Security History

Computer security history studies lead the researcher to study the technology used to win World War I and World War II in the 20th century to find the first automated computer machinery used in deciphering enemy messages [Kahn, 1968]. The Colossus machine was used by the British to decode German intercepts. Germany was using the Enigma machine to encode it’s messages from the German high command. America effectively countered the Japanese codes with Navaho code talkers in the Pacific. Kahn discusses in great detail the means of deciphering various codes through all history. His book has often been called the “NSA Bible” and has been called required reading by NSA employees. It has a chapter on the history of NSA which was established in 1949 to have overall coordinated control of national efforts at intelligence. A personal informal survey of NSA students in undergraduate courses at Ft. Meade indicated that many junior staff have not heard of the Kahn book but are very familiar with SANS institute and other private solution sources. The technology for the

atom bomb was also partially derived by computers in World War II on the Manhattan Project. By 1949, the United States realized “intelligence” was the single most important asset that helped win World War II and future wars. Kahn describes the peacetime uses of cryptography to keep government secrets secured using computer like the Cray supercomputer. His work is recognized as the definitive work on secret writings. The role of the cryptanalysts can not be understated in determining the outcome of past wars including the Korean War, Vietnam, and Gulf War. Kahn gives the novice enough information to encrypt his own messages using ancient methods or more modern methods. He explains the nature of “The CodeBreaker” thinking about the many patterns a secret writing may take and his value to the Unites States security in the future.

Military Counterintelligence Use of Computers

Since World War II, US military intelligence use of computers and communications equipment has been significant for processing battlefront data. US Army General McChristian described how he used Automatic Data Processing (ADP) computers to process battlefield data during Vietnam in Hawaii from 1965-67 in his book [McChristian, 1974]. The idea was to recognize and counter general patterns in the offensive movements of the North Vietnamese Army to win specific battles and

protect our personnel resources.

The United Kingdom computer security group states that they have been using radio and communication technology in military intelligence since the end of World War I or 80 years. They recruit young computer security experts online through the world wide web. Today, US satellites take high altitude aerial photographs that are computer enhanced and monitored every day. Every president receives a daily CIA world report produced by electronic desktop publishers covering overnight world events according to a History Cable Channel special story. These same pictures are used to monitor recent NATO “police actions” in Africa and the Balkans to determine threats to our forces deployed over the world. The network of satellites delivering the pictures are subject to computer viruses and electronic attack by foreign “Information Warriors”. The challenge according to USMC General Gray is to “protect our own electronic resources while learning enemy activity”. The Air Force Computer Emergency Response Team (AFCERT) is organized to meet the threats to US Air Force computer and communications systems. The Army has intelligence groups at NSA along with other branches of the service to collect communications signal intelligence from foreign broadcasts. Intelligence is required for military decision making the same way it is required for business decision making under the guise of market research (and sometimes industrial espionage). This organizational function requires computer

technology. Two books discuss the computer cryptologic capabilities of the former Soviet Union from inside the former KGB and Soviet Army [Bittman, Suvorov]. During the cold war they had a distinct command structure for obtaining information on the US from any sources located here in the states. Many court cases such as the John Walker & son case proved the capabilities of Soviets to gain access to inside military information and technical design plans on US systems for a fee. The Soviets even tried to steal a copy of ADABAS for $50,000 in the early 1980's. ADABAS is an inverted-list database management system selected by the US Marines and FBI headquarters for large IBM mainframe data storage projects. This fact was used in the advertising of the ADABAS products by Software AG (of Germany) to United States military components. ADABAS has cryptographic algorithms for file protection, a unique computer security access system, and unique low level file access routines (RABNS – Relative ADABAS Block Numbers) that form the physical schema and are more complex than the typical three common types of databases taught in college courses such as hierarchical, network, and relational data models. It was also common knowledge that electronic radiation emanations from computers could be detected through a window at a DOD facility and TEMPEST machines countered this threat. Database files relating to troop mobility had to be encrypted by proprietary database algorithms before transmission on DOD phone lines or storage on magnetic

disks. The transmissions on commercial carrier grade lines could easily be passively wire tapped by any foreign countries without detection on older wiring technology. CDROM technology was tested by the Marines for its durability under extreme stress (heat, cold, pressure) and proved to be a good computer medium for transmitting and storing data for “Information Warriors”. An example of this was the Fight Smart Marine Corp CDROM containing training video clips and a speech by the commandant , General Kelly, in the late 1980’s. Today encrypted databases can be placed on numerous new types of electronic media that were not available 30 years ago, before the popularity of the microprocessors that power personal computers.

Soviet KGB and GRU Dis-Information

The stories of the Soviet KGB and GRU are told in two books recently acquired [Bittman, 1985; Suvorov, 1984]. The KGB is the counterpart of the FBI. The GRU is similar to the CIA in that it concerns itself with countries external to the Russia. The GRU runs spy networks through the embassies to foreign countries. Suvorov describes his life inside the GRU. Suvorov lives in Great Britain and his whereabouts are a secret. Although the cold war may be done, the book describes an agency that stops at nothing to obtain information and create dis-information about Russia. These books are significant to the researcher

because of the threat a former KGB officer as premier of Russia poses to the United States. Vladimir Putkin was once a KGB man and his knowledge of world events may only parallel that of ex-CIA Chief and ex-president Bush. To say one is more wise when one knows where his information is coming from is a godsend. George Washington was also well known for his leadership ability in military intelligence and as president.

The GRU was to prevent the external collapse of the Soviet Union and obviously did not fair well in 1989 with the collapse of the Berlin Wall. The United States had a mole in the top levels of the Soviet Union for many years who reported directly through the CIA to former presidents according to one “History Channel” show on “Master Spies”.

The GRU has all the same technology elements capabilities as the CIA. The Russians have military forces who are trained to performed electronic surveillance from ships, aircraft, and satellites. These elite are trained at Soviet military academies on covert and overt intelligence operations. The United States leads the Soviets in having a strong market economy under capitalism that also supports U.S. intelligence equipment supply efforts. It is due to this lack of strong supply chains and internal industrial information age economy that the Soviet intelligence system struggles behind the United States and Great Britain.

CIA's Perspective

The Director of the CIA, George J. Tenet gave a statement to the Senate Select Committee on Intelligence on & January 2001 and stated that "new communications technology that enables the efforts of terrorists and narcotraffickers as surely as it aides law enforcement and intelligence." [Tenet, 2001] Tenet further discussed terrorists intentions and that "Some groups are acquiring rudimentary cyberattack tools. Terrorist groups are actively searching the internet to acquire information and capabilities for chemical, biological, radiological, and even nuclear attacks. Many of the 29 officially designated terrorist organizations have an interest in unconventional weapons, and Usama bin Ladin in 1998 even declared their acquisition a "religious duty." The CIA official position is one of terrorist prevention through counterintelligence efforts that use computer and satellite technology also. Tenet further describes to the senate that the United States is very dependent on the dominance of information systems. Computers could give our adversaries great occasion to circumvent our conventional military powers. Attacks on our information infrastructure, military, and economic system can occur from anywhere in the world according to Mr. Tenet. This would be the opportunity for a terrorist hacker attack on our computer systems. Additionally, foreign countries may want to attack our space based assets to blind our global imaging capabilities and attack our space based military satellites. Since Mr. Tenet was recently reconfirmed as the Director of the CIA, it would

be assumed this thinking will be continued in our intelligence community for some time to come during the George W. Bush administration.

NRO Satellite Wars

For years the National Reconnaissance Office (NRO) grew from a small agency of spy planes into a large contingent of spy satellites. Documents on the George Washington University National Security Archive website show the memoranda that gave the Air Force the function in the 1950's using the U2 and SR71 spy planes to take pictures at high altitude over the Soviet Union. The Francis Gary Powers affair stained the secrecy of this program. This was replaced by the CIA CORONA satellite which could take pictures at a resolution of 9-25 meters in the early 1960's. Satellites had been used before that by the United States by none were effective nor successful. The Soviet Sputnik satellite put pressure on the United States to develop the CORONA program and our national space program. Many other successors to CORONA have given the United States 24 hour all weather imaging capability close to 2 meters resolution. The Air Force Special Projects Office ran the SAMOS program and became the NRO Program A. The Navy had the GRAB (Galactic Radiation and Background) satellite which was run by the Naval Research Lab until 1971 according to documents in the archive. The mission of the NRO became to coordinate the overhead intelligence operations of satellites as the photographic

capabilities and data transmission of the satellites turned into a real-time channel operating 24 hours a day over any continent of the world. Infra-red images were soon available to cut through cloudy weather. CIA intelligence from CORONA was used in the Bay of Pigs to determine missile counts by the Soviets in Cuba. Our intelligence capability today from space is more accurate today than ever before by military or commercial satellites. These satellites are some of the sensors used in the "network centric" warfare. Tanenbaum describes how satellites are "repeaters" in the sky who provide a channel to ground stations and convert the transmission signal to coaxial cable or fiber optics. More than nuclear détente, vigilance and the improvements in satellite technology has led the United States to peaceful times where no military actions around the world can go unnoticed without viewing from space. The fact that this information was available on INTERNET is quite disturbing to this researcher even though it has been declassified. Any information that could potentially help foreign powers should be kept under lock and key. The purposeful dis-information and propaganda information wars are part of the domain of some countries around the world.

Information Warfare

The Armed Forces Communications Electronics Association (AFCEA) is primarily concerned with waging information warfare. Al Campen describes the

computer warfare in “Cyberwar 2.0” published by AFCEA [Campen, 1999]. He also writes articles for the AFCEA periodical entitled “Signal Magazine” in which he has described the need for an “Information Corps” within some units of the military who specialize in computer information warfare. The number of systems that are controlled and commanded by computers in the US Department of Defense are so immense that it is impossible to calculate the total assets invested in computerized systems (embedded and stand alone systems). The execution of the “Gulf War” order of battle included deployment of intelligence gathering computers systems and command and control computer networks to the dusty Saudi Arabian environment. These systems were ”ruggedized” for use under any weather conditions by Army personnel. Future wars will never be the same. A cyber war may be the first war that is fought as opposing sides attempt to dominate cyberspace without firing any shots using ancient kinetic weapons. Campen explains how we have evolved to such as dependency on computers in our military and everyday office life that runs much of the government.

Network Centric Warfare

The US Navy and other military branches are implementing “Network Centric” warfare as the most recent change in military strategy in 200 years. [Cebrowski, Stein] The Pentagon has a group established to study “network centric” operations. Lockheed Martin

had a TV commercial that sums up the term as information superiority on the battlefield of tomorrow where we may not have to fight because the enemy knows we are so superior in information and coordination of air, ground, sea, and space based attacks. The defense firms in figures 9 and 10 and weapons systems (platforms) in figure 12 are integrated into the network centric warfare model. All of these systems have various levels of computer security built into them. Admiral Cebrowski does an excellent job paralleling the management information infrastructures of leading companies like Wal-Mart and the new model of the military. The network centric battlefield depends on a bottom up communication and command cycle that can destroy an enemy by 50% within the first few minutes of engagement. The network-centric model contain three components – sensors (humans with laptops, satellites, aircraft, electronic eyes in the sky), command and control (humans and computers), and shooters (weapons platforms). The speed of command is increased under the network centric model of warfare in a local region of the world. The three “grids” of network centric warfare operate in unison under the Navy view called “cooperative engagement capability” of humans, computers and systems. This is quite different from the single-moded electronic direction of individual platforms or groups of platforms in the past. Sensors detect and there is automated command and control to firing solutions on a large scale basis. The engagement under the network centric model is powerful and continuous and leaves little time for an enemy to respond in kind in

conventional terms. Stein states that this vision is a reality by 2010. Admiral Cebrowski states that it has already been used in the recent Taiwan Straits Crisis in 1995 by the Navy.

The dynamic sensors are one primary key to the network centric approach and provide a constant vigil on the enemy. Any threats are processed immediately and command and control begins to direct a response. Cebrowski indicated that in one month recently an Air Craft Carrier sent out more than 54,000 email messages in the Pacific. This shows the bottom up nature of the general networking abilities in the fleet and in our society. The admiral shows a true understanding of the management of change in our society and he even calls for more specialized training in computer technologies to keep up with the changing network technologies and information age skill-sets. This leads to the usage of computer networking and communications to the battlefield of the future. The C4I (command, control, communications, computers and intelligence) website at the Pentagon confirms the experimentation of new communications technologies applied to the battlefield. This all requires a significant amount of electronic deception from any potential enemy while on the battlefield and electronic encryption is a given fact of life on the ruggedized computers and sensors. The best way to stop losses in war is to have more information than your opponent and deny him the opportunity to use his information against you. Clearly, private defense companies and the U.S. military are utilizing components of network security, computer security, and operating systems securities such as passwords

and even biometrics to allow access to the hardware integrated into the network centric equipment (sensors, information, and weapons platforms). The human is still in the decision making loop and has override capabilities that are important in network centric warfare to avoid situations similar to the "USS Stark" and "USS Vincennes" incidences involving computer and human responses to threats.

NSA "Rainbow" Series

The "Orange Book" and other books in the "Rainbow" series from the National Computer Security Center at NSA, Ft. Meade, Maryland discusses the requirements for federal and military computer security on all projects. The documents are known as the "Rainbow Series" because each document has a different colored cover. This set of documents basically outlines the various levels of classified information under a "need to know" for managers and technology workers. One can also use the set of books to set up a secure computing facility in the military agencies and her "trusted" contractors. NSA and SANS Institute welcome opportunities to provide intruder vulnerabilities assessments to organizations. President Clinton has issued an executive order recently that affects all classified information and reduced the time from 25 to 10 years for declassification of information on government top secret systems. A full copy of this executive order is available on the Federation of American Scientists

website who work on many of the federal projects. In fact, vice presidential candidate senator Lieberman was previously the chairman of the committee on government secrets. We need prudence in the handling of government secrets relating to national security**.** We lose national security when we compromise any secrets to foreign interests.

International Computer Laws

For the purposes of this study on computer security, international computer security laws have been compared to US computer laws in the 20th century. Two groups of international countries discussed are the members of the World Trade Organization (WTO) and the G8 European Countries. The best text on computer laws from the US Library of Congress is by David Bainbridge and was used for a University of Maryland undergraduate course curriculum on Computer Security Laws [Chiarella, 1999]. David Bainbridge's "Introduction to Computer Law" discusses United Kingdom computer laws including the four subclasses of laws such as Intellectual Property, Trade Secrets, Privacy, and Computer Crime [Bainbridge, 1999]. The lists for comparison of United States laws and United Kingdom laws in computer security are included in this report. The basic difference between US and UK computer laws is minimal, except that UK has a few more laws on Intellectual Property and Trademarks

earlier than the United States had them. It must be said that the scope of the two nations computer resources differs greatly based on the commercial and military strengths differences of the two nations. The United States benefits from examination of British computer laws. The Intellectual Property laws cover copyrighted property on electronic media and transmissions and are designed to protect the original author of a new idea. As an example, email is considered official government records by law today as admissible evidence in court. Information in emails (politically sensitive or not) are therefore now covered by new changes in the definition of “official records”. When data contains information about any persons, the public data administrator is required to take action to ensure the electronic privacy of those persons similar to the Privacy Act of 1974 in America. The official position is to protect the privacy of all citizen records containing names, addresses, and other personal attributable information. The government, especially law enforcement and counterintelligence (FBI) has a law to allow the selected filtering of telecommunications packets (sniffing) to solve crime cases. The FBI “Carnivore” system will have this capability as built by contractors and citizen’s must rely on the integrity of FBI operations staff to keep private information undisclosed and meet both requirements of the Electronic Privacy Act and the FBI exemption for law enforcement. Trade secrets acts protect corporations from spying on each other in a competitive environment. Encryption algorithms in the United

States are covered by patent laws for the standard 17 years from date of issue of the patent. The cost for patenting algorithms is upward of $2000 after patent search and determination by the patent officer. When government computer systems are delivered, the unique compiled software system becomes the property of the government agency. Proprietary software routines remain the property of the private company with a license issued for usage by the agency, even when the contract delivers source code. Bainbridge covers the details of computer laws in the western world and modern society as good as any written in America. The book also offers a database of case studies in British computer law available at the University where Bainbridge teaches in the United Kingdom.

Telecommunications Law

Telecommunication laws are changing because the companies are globalizing to provide more effective “long haul” economies of scale using satellites and fiber optics communications media. International political boundaries are basically transgressed in connecting a person or computer from one end to the other of the international circuit call. Lawyer Walter Saporov’s book, Telecommunications and the Law, describes the effect of the Telecommunications Deregulation Act of 1984 which basically opened competition between companies. The Act divested “Ma Bell” (AT&T) into “Baby Bells”

providing local and long haul services [Saporov, 1988]. The Sherman Antitrust Act was cited as a reason to prevent AT&T from monopolizing the government carrier service. The government has it's own FTS 2000 contract with different carriers every ten years.

Since the 1934 Communications Act, AT&T was the sole provider to the government for telecommunications resources with the monumental task of wiring America coast-to-coast. After the deregulation in 1984, other smaller companies were allowed to enter the local and long haul carrier markets and help drive down consumer prices (in theory). Today, congress is holding hearings with the FBI delegating authorities and FCC concerning foreign majority ownership of telecommunications companies (CSPAN Cable TV). New companies have been started in the last five years (1995-2000) and been very successful in obtaining investors for new projects. Some of these companies are owned in whole or part by foreign companies and are bidding for contractual work with the US government. The question in today's world is "Should the United States telecommunications infra-structure be run by foreign owned companies who may have sovereign interests above US interests?".

Computer Security, Accuracy, and Privacy

There is no discussion of computers in the last part of the 20th century without at least some reference to Dr. James Martin who has written more than 30 books on the

topic after working at IBM for 19 years [Martin, 1984]. One of Dr. Martin's books discusses the optional solution for developing computer security management according to a layered approach based on an onion skin with successive deterrents to the would be computer criminal. He stated that physical security, procedural security, environmental security, communications security, operating system security, algorithm security, and password security comprise the onion "layers". In government systems there also exists the political security which include legal security. The best security is total physical security where absolute denial of access to computer hardware by the intruder prevents any mischief. The easiest security to "crack" is the password code security. Thus, applying a combination of the security techniques layers the defense against a potential intruder and makes the task of "cracking" so time consuming as to be useless to attempt. Given time any secured system can be "cracked". The idea is to place more obstacles in the criminal's path to penetration of the computer system than he can thwart**.** Given Martin's paradigm, one has the armor to setup defensible computer security risk management plans that are successful. The US Navy adopted some of James Martin's strategies at the Bethesda Naval Medical Data Services Center from 1978-1985 in the form of new computer security risk management forms and procedures. Today, the advent of INTERNET computing and macro viruses in open communication systems creates a whole new set of computer security risks that are

being mitigated in personal computers and server workstations.

Comprehensive Computer Security

Comprehensive computer security practices are required in the computer technical world. [Pfleeger, 1989] Pfleeger describes the various types of computer security in great detail for the computer scientist. This book was used at the University of Maryland Baltimore County campus in the 1990's for computer science students who would be placed in government and private agencies in Maryland. According to Pfleeger there are many facets of computer security. He breaks the topic into sub-categories of Basic Encryption, Secure Encryption Systems, Operating Systems Security, Personal Computer Security, Communications Security, Computer Systems Security, Network Security, Physical Security, Risk Analysis, Legal Issues, Ethical Issues. I particularly liked the way he described access control matrices and lists, trap doors, Trojan Horses, salami technique, program memory leaks, viruses, worms, greedy programs, and infinite loops. This is a well rounded, robust treatment of computer security. It is one of the best books for use in academic programs on Computer Security the researcher found. Pfleeger has previous works in Computer Architectures and IBM 16 bit assembler language that ensure he is a reliable technical guru at the detail level used in undergraduate program at University of Maryland

University College in 1986. One can appreciate texts which can cover as much material as Pfleeger. The text is now 11 years old and may require updating to cover some of the newer encryption algorithms like the Encryption Escrow Algorithm. He discusses RSA and DES algorithms. He does not cover the Skipjack and Clipper Chip algorithm. He describes various cases of computer crime and fraud so the student is certain what behavior is acceptable and what is not. The book describes ethics at the end which gives students a code of ethics to adhere to over their career. This is a most effective tool in curbing computer crimes and educating young scientists. The book only cites 3 computer related laws. This research has cited many more computer related laws that include various subjects related to computer sciences like IRM, Computer Acquisition, DOD Systems, and foreign computer laws because of interpreting computer security to include some aspects of military intelligence and national security. In 1989, the U.S. did not have as many computer related laws as we have today. One would hope to convey the same level of detail on technology management issues and computer sciences issues as Pfleeger did in any texts I would produce on the subject of computer security.

Encyclopedia of Cryptology

Becoming familiar with the terminology of cryptology was easier with this

resource [Newton, 1997]. The book is a must for readers new to the cryptology field. Algorithms, technical terms, and legal concepts are all explained with equal attention to detail. One can use the entire text for building a vocabulary in cryptology fast. It was acquired over the INTERNET and highly recommended to the reader requiring more definition of cryptology terms and phrases in detail with pictures. The mathematical equations used are explained, but may be difficult without prior college level calculus courses. This book is a desk reference for every computer systems manager that will help him with building his computer security knowledge and vocabulary. The book was acquired through Amazon online books which allows book reviews prior to buying. This was useful in filtering the books to be used in the research process. Previous comments on the books always help with stratifying the selection process. The book is full of vivid photographs and pictures relating to the history of cryptology.

Decrypted Secrets

F.L. Bauer's book entitled "Decrypted Secrets: Methods and Maxims of Cryptography" describes everything about cryptography from ancient Egyptian methods of political cryptography up through modern times cryptography [Bauer, 1997]. It has a mathematical flavor at points and explains how encrypted messages work from the very ancient to present day. Bauer focuses on the algorithms and machines rather than the

people. This is a significant work because it parallels the Kahn book “CodeBreakers” in terms of the descriptions of historical events in WWI and WWII that helped America and allies win the wars. There are numerous pictures of coding machines, coding disc, and even a Cray super-computer used in deciphering algorithms. Bauer would be a must read for the professional cryptographer. The book was found on Amazon.com which is amazing as some of the systems in the book were once classified as top secret. Hopefully our enemies will not use our own open democracy against us in future wars. There are still many current day secret that are only on a “need to know” basis all the way to the White House. Some of the methods that Bauer discusses include simple substitution, polygraphic substitution and coding, linear substitution, transposition, families of alphabets, keys, and open encryption key systems. In the section of cryptanalysis he discusses combinatorial complexity, patterns, probable words, and frequencies. The rest of the text discusses more advanced topics in cryptography. The Bauer text is a must read for the interested reader or the seasoned computer security veteran. After reading the book one clearly feels illuminated by the past secrets Bauer reveals in the chapters. It is like viewing a segment on the History Channel that contains “close to” secret information. The author states it eloquently when he paraphrases Otto Horak (1994) and says “Protection of sensitive information is a desire reaching back to the beginnings of human culture” in his description of cryptography.

Distributed Systems Concepts and Design

This is a college undergraduate text on distributed systems taught at University of Maryland University college and the chapter on computer security is one of the best available for object oriented modern computer client-server architectures and three tier architectures [Coulouris, 1994]. The Byzantine General algorithm and Kerberos algorithm for authentication are explained with network topology maps in the sections on computer security in distributed systems . The view of systems security as a part of the systems manager and developers responsibility is up to par with current United States academic classification of disciplines. In late 1987, American graduate school and undergraduate school computer sciences departments were reclassified and expanded to include information sciences. Computer security may well be another discipline added to the college educational divisions and selected schools. In 1999, the Coulouris text was criticized heavily by undergraduate students. They stated that the 1994 publishing date was not recent enough to be included in the academic program. The book was relative in their understanding of how distributed databases and networks work in the academic and corporate world. The other comment was that the text was written from a very British view of the world by the use of language. Indeed it was created at the Queen Mary College and explained some systems in use

in the United Kingdom as well as other United States Schools such as Harvard and MIT. There is one professor at MIT who has excellent online course resources in Computer Security as was found on the internet.

Power Programming with RPC

The value of this text is in it's description of how to write programs that tunnel under a networks data link level without needing a password to connect to a remote computer. This technique was demonstrated by students who wrote programs to do just this for credit in learning about distributed systems. The book teaches how to bind C programs with code at both ends of the computer connection. A great book to learn how communications protocols are programmed. It has many examples of how to bind a protocol in a communications program on two remote PCs. RPC stands for Remote Procedure Calls and the book outlines network communications via RPC versus local calls. This is an excellent book to learn useful networked applications programming techniques [Bloomer, 1998]. This book is currently used by the University of Maryland to teach "Distributed Systems" programming in RPC at the undergraduate level in conjunction with the Coulouris book.

Computer Networks

The importance of this text is that it teaches computer network protocols and the Open Systems Interconnection International Standards Organization model of telecommunications [Tanenbaum, 1984]. There are diagrams galore that explain wireless communications, satellite communications, microwave, cellular, radio frequency communication, the Aloha protocol used in the Hawaiian islands after WWII, frequency division and amplitude division multiplexing, Network Operating Systems router programs, and the OSI ISO 7 layer model. The 7 layer model is explained in detail and it has been an important discussion topic in every data communication course ever taught as it is recognized as the single model on which all proprietary and academic digital networks are based. Tannenbaum explains the activity at every level of the model from low level physical layer to the high level applications layer of the 7 layered protocol model. The model can then be used as a building block for other data communications issues such as “Programming in RPC” or actual usage of telecommunications utilities on microprocessors such as File Transfer Protocol (FTP) and basic X, Y, and Z modem protocols. Issues such as handshaking are discussed. Datagrams and packet switching are discussed in detail along with how the INTERNET works (which was used by DARPA at that time). This book is invaluable in explaining normal telecommunications operations which then lends itself to understanding how file

encryption works during transmission of data from computer to computer. This book has been a telecommunications course reference book in the American University graduate program for many years. The DES algorithm in figure 17 is taken from this text.

Operating Systems Security

Since the early IBM Series 360 mainframe computers, computer security has been a problem to be solved by the computer engineers. Harvey Deitel's textbook entitled "An Introduction to Operating Systems" used in George Washington University Computer Science courses covers operating systems such as UNIX, VAX, CP/M, MVS, VM, and ADA [Deitel, 1984]. UNIX, MVS, VAX, VM, and ADA are still extensively used in the mainframe computing world. UNIX was created as a communications oriented operating system and today many microcomputer server machines run forms of UNIX, POSIX, or LINUX operating systems. MVS and VM are used extensively by the Department of Defense for data processing. ADA is used for weapons systems as was hailed as the single DOD computing language in the late 80's in several Pentagon directives. At one time a computer analysts career was not complete until he had developed projects on every type of operating system. Today, many new comers to the field feel that microcomputer and microcomputer server experience and knowledge is enough. Deitel's book is important

because he describes the common computer security components relevant to all the operating systems he describes in his case studies section. He describes a good security program that accounts for all computer resources. His proximity to Washington DC gives him a good vantage point for the three U.S. governmental security requirements during the early 1980's which included: DOD Directive 5200.28 (on classified information), Computer Security Technology Reference Manual (US. Air Force), and The Privacy Act of 1974 which required all information on individuals to remain private on government computers. He splits computer security into external security, user interface security, internal security, operational security, and physical security to form his "Total Approach" to security. External security (and physical) are protections against disaster to the hardware and facility. He has an approach to security similar to James Martin. He describes system surveillance as necessary to protect the hardware assets through voiceprint and fingerprint systems allowing access to the computer. We call this Biometrics technology today where we have computerized the access process totally using the micro computer. Deitel further discusses threat monitoring where computer software surveillance programs search for threats internal to the system. When surveillance programs have greater authority than users this is coined "amplification". Password protect uses three aspects about a person to record his unique identifier. They are: a) something about the person, b) something possessed by the person, and c) something known by the person. Biometrics helps

identify something about a person's physical appearance such as finger prints, thermal images of the face and body, voice print, etc. An audit log is used to analyze who has accessed a computer and who has done certain commands in the computer system. For example, ADABAS DBMS under VM and MVS uses a command log and data protection log in mainframe computing to provide for tracing and auditing of all database commands issued by all end users. This help the security analyst trace exact operations down to the microsecond. Access controls help classify the powers the end users are allowed to have while in the system. ADABAS uses an access control list which has a matrix of the authority granted to the end users and a file protection status for each file. Both of these numeric values are compared to each other when a user requests information from the file. If the user has a higher numeric value than is listed on the file for read access, then he gets to execute programs that can read the data. If he has a numeric value that is higher than read, but lower than update, then he gets read only access. If he has a higher value than read only and update, then he may execute update objects (programs) against the database files (tables), he has authority to access. All ADABAS security numbers for users and files are stored in the ADABAS security access control list. ORACLE security works in a similar fashion where users are granted permission to read, write, or update certain tables in the database. These security privileges are applied to the session of the end user and can be applied to certain PL/SQL commands similar to the newer ADABAS security

packages in NATURAL. Both hold profiles of the end user and compare his granted ability to the files or table security levels. Windows works similarly with attributes bits placed on files to protect certain commands from executing against the files. In Windows however, it does not distinguish who the user is nor does it compare authority levels. These security features are in addition to password login security. Deitel describes security kernels as so large that they inhibit good computer security. Highly survivable systems are now in use for increasing reliability and increasing computer security through redundancy. An example of this is the air traffic controller systems used by FAA. Objects in software allow for differentiation of computer security attributes to commands, executables, userids, tables, files, programs, sessions, and time frames. The operating system must keep track of all objects to avoid a lost object situation which would cause a system failure in the operating system and DBMS security. ORACLE grants security privileges to objects by the systems administrator or database administrator. One must ensure the system administrator id is not compromised to retain good security. The administrator can selectively revoke any users privileges to operate on data. Deitel then discusses cryptography and the problem of user authentication of messages transmitted to other operating systems. He says system should be designed to maintain cryptographic privacy in ciphertext using a plaintext as input from a sender to receiver. He describes the difference between a public key and private key encryption system. At the time of the writing in 1984, DES and RSA were

standard cryptography schemes in use. Mainframe operating systems use encryption and decryption as much as any other systems simply be a programmer setting a switch for encryption when messages are transmitted through the teleprocessor or stored in a database or tape. Penetration tests are test to ensure the system can stand up to an attack by would be intruders. He describes flaws in operating systems that allow operating system penetration. He next discusses Generic operating system attacks such as masquerade, operator spoofing, denial of access, browsing, piggyback, clandestine code, Trojan Horse, line disconnect, and "NAK" attack. Deitel discusses a penetration test managed by the University of Michigan which hired a company to attack it's computer and pinpoint computer security flaws to Michigan after the successful attack. This vulnerability testing is the type done by NSA for government agencies. Today, INTERNET has created a new level of concern for more smaller and more powerful computers and servers than ever was anticipated in 1984 when the "Operating Systems" was written by Mr. Deitel. Communications capabilities of America are much more diverse than ever before in the history of computing. The Deitel book was a landmark text used by many computer science departments in America and focused on making the highly technical world of Operating Systems easier to understand to the layman.

Database Systems Security

One of the best books on Relational Database Systems is CJ Date's "An Introduction to Database Systems" [Date, 1995]. This text is the mainstay of the University of Maryland University College Relational Database program as well as George Washington University. Date discusses computer security elements in one of the most interesting chapters of the text. He states that security and integrity are related in databases. Furthermore he states that there are two types of security in databases: discretionary control and mandatory control. Discretionary control involves giving the user different types of access privileges or authorities on the database tables and other objects. Mandatory control is rigid and a classification level is placed on every object with each user having a clearance level. Security rules are enforced in the DBMS where they are also known as authorization rules. The security subsystem of the DBMS implements checking routines of the objects. For example, ORACLE follows this type of computer security scheme. ORACLE has both object level security and user authorization levels that may be granted through SQL. Date discusses how discretionary access control can be placed on a users id through the creation of security rules in the SQL "CREATE SECURITY RULE " SQL command. The user is granted retrieval, insert, update, delete, or all command levels of operation while he/she is online with the database. Audit trails are important to the relational database operational security and are implement in the form of logs that record

when every action is do by any and all users. These logs can take up enormous space but are required to run an inspectable audit list of actions performed against data. Mandatory Access Control is the idea that each object has a classification level such as top secret, secret, confidential. In this scenario, each user has a clearance level with the same possibility levels as classifications. These classifications follow the Orange book and Lavender Book (discussed in the Orange Book Series reference) produced by the NSA for the federal government. The security classes in the Orange Book include four categories (D,C,B, and A). Class D is minimal protection and class A is maximum protection. Discretionary protection is afforded by subclass C1 and C2. Structured protection is subclass B1, B2, and B3. Class A requires a mathematical proof that the security mechanism is consistent and that it is adequate to support the specified security policy. Data encryption is the most effective countermeasure in database security as it falls into the class A realm. Date goes on to discuss plaintext, the encryption algorithm, the encryption key, and ciphertext. Date discusses the operation of the DES standard (figure 17) and Public-Key Encryption in very clear and concise manner. This may be because Date is a mathematician by education. The last points that Date discusses are the SQL supporting commands for security in a relational database. He describes how to use the grant and revoke commands from the system administrator levels of the database. Since SQL is a standard language the format of the commands is the same for any version of SQL that is

relational. Date summarizes each of the areas he discussed with excellent use of bold printed keywords and common sense language that is easily understood.

A wise systems administrator is always learning more about his software suites. The book “Oracle 8 DBA Handbook” has everything the new database administrator needs to explain Oracle 8 Database Security. [Loney, 1998] Chapter 9 focuses on Oracle 8 Database Security and Auditing. Accounts are created in Oracle databases by the System Administrator sometimes called the lead DBA. This DBA establishes ORACLE access accounts for all users and gives them a profile. Objects are also given privileges using the “grant” command. System level SQL functions such as “create table” and “drop table” are also given to trusted system users. The “SYSDBA” and “SYSOPER” userids are the most powerful in the ORACLE security scheme, usually reserved for the lead DBA. These can perform system management functions like shutdown, startup, and recover. Object management is done for all commands (objects) a user can perform in SQL or PL/SQL. Users are granted roles that have various levels of authority in the commands used. Every user has a profile in which puts limits on systems resources that can be used for each userid that is stored. Password management allows the lead DBA to determine the number of wrong attempts at login as well as the password. Reuse of passwords is prohibited by the Oracle 8 security software. Password complexity can be regulated also, where the system demands the user to enter certain types of characters in their passwords. The

object level privileges can be set on the select, insert, update, delete, alter, index, execute, and read commands (objects). This means that when that user runs an application with restricted passwords, he may not be able to perform all tasks of the application package in PL/SQL. This is a good way to shepherd the novice users and program security in applications. The data dictionary holds all the information about these Oracle privileges. The data dictionary views DBA_ROLEs, DBA_ROLE_PRIVS, DBA_SYS_PRIVS, DBA_TAB_PRIVS, and DBA-COL_PRIVS give information on the DBA privileges. These are the places where the SYSDBA and SYSOPER save data in Oracle system files when setting up security in a fresh database. This must be done before any users are allowed access to the data tables either through SQLPLUS, SQL, or applications. Oracle has the encryption capability for all passwords. Auditing in Oracle 8 is done on Login attempts of any client on the network. This Login Audit is stored and can be reviewed by the DBA on a regular basis for unusual activity. Oracle objects can be audited to categorize the information and make it easier to track bad attempts at certain commands.

Time Bomb Ticking

Ed Yourdon's book entitled "Time Bomb 2000" was excellent preparation for a person to become a computer disaster recovery expert [Yourdon, 1998]. The book describes the scope of the year 2000 problem and even successfully predicted the

electricity blackouts now occurring in California (January 2001). Although there were no major problems in year 2000 at the deepest end of the anarchy scale, there were smaller problems like the “denial of service” attacks on AOL and Amazon websites in February, 2000. Your does an excellent job covering the extent of computers and risks in the federal government on an agency by agency basis. He rated all agencies with grades on a report system in 1997 and found more than half the agencies with less than a C on preparedness for year 2000 defects in software and computer technologies. Some agencies were planning this moment in history as far back as 1989 in software at the Office of Personnel Management Retirement Systems Division. Financial calculations (interest rates) were extended into the new Century in an ADABAS NATURAL program core table that matched years with rates in the Automated Voluntary Contributions System. The array internal to NATURAL was extended to 2010. Before 2010 the calculations will have to be modified again. This was better than the modus operandi of the agency who had staff who changed the internal arrays similar to this one on an annual basis as needed every year as a part of the software maintenance cycle. One Orkand Corporation programming team completed these programming modifications in 1989. The value of Time Bomb 2000 is that it gets you to thinking about the possibilities of what can go wrong in our ever complex society. It’s the type of book that should catch the reader’s attention and make him slightly paranoid

about the US national computer infrastructure and energy infrastructure. If the US ever loses power, we become a dead society. President Bush appointed Vice President Richard Cheney to ensure we have power in all states at adequate levels in recognition of the threat to our nation. One can be sure that a hostile foreign nation would try to shut us down if they had the means to do such. This is where intrusion detection and penetration testing help us identify the areas of weaknesses similar to what the Yourdon book does for contingency planning and risk mitigation in the 21st century. Yourdon point out how we are so dependent on high energy consumption in our daily lives that it is our Achilles heel in the event of an electromagnetic- thermonuclear pulse (EMP) explosion in the atmosphere. In the case of the Y2K problem, the threat was the same in a worst case scenario. As we all know, embedded computer chips were fine and everything did not come to a standstill on New Years Eve 2000.

Network Intrusion Detection Analysis

Stephen Northcutt of the SANS institute is the premier expert on INTERNET Intrusion Detection and has taught courses in network intrusion detection [Northcutt, 2000] to the very best network administrators in the world. Network Intrusion Analysis describes the cases of incidences and appropriate responses by the network administrator. The book is mostly technical data on how to identify network intruders

and how to handle intrusions in certain operating systems (UNIX and Windows NT). Northcutt was previously assigned to the Navy Shadow group at Dalhgren NSWC and was interviewed at the Shadowcon 2000 conference at Dahlgren. He presented network intrusion as one of his life tasks and described how hackers can intrude on a network and compromise the root directory on servers among other things and cause havoc. Northcutt explained that he could teach more about network intrusion to interested students at his Intrusion Detection Courses at SANS group. Professor Randy Marchany from Virginia Tech presented after Northcutt and discussed computer network security and how important it is to all governments and large organizations. He was available for follow-up comments over the telephone when he recommended Northcutt's book from his course. Marchany teaches his own computer security course to undergraduates at Virginia Tech as well as speak at computer INFOSEC conferences. Marchany remains a resources for more information from his websites.

Biometrics

The Biometrics Consortium is a group of interested commercial and government parties who have come together to exchange information in the technology world to improve government security using biometrics devices. The NSA and NIST co-sponsor the annual event and the group is available online at www.biometrics.org. The

biometrics are concerned with identifying and authenticating people trying to obtain access to either buildings or computer and communications devices. This consortium is a very leading edge group and is based in the Baltimore-Washington DC Area. The number of devices to protect government assets is increasing every year. The "Biometrics Consortium Annual Proceedings for 2000" has papers on the current biometrics used in the government and for sale by various vendors. Many of the papers are very technical and target specific areas of vulnerabilities that need to be covered by Biometrics. An example of the type of Biometrics devices are fingerprint machines, voice print machines, facial thermal scanning, retina scanning, and smart cards. These devices are used on the front end of a system to deny access to unauthorized personnel. Most significant to government systems is the potential uses of biometrics as automated identification and authorization agents for military systems and computer network nodes used in the network centric battlefield. Information warfare has integrated with new weapons systems and authentication requires the proper personnel to use the weapons systems. The Army land warrior laser guided gun system is one that requires login by the soldier and his identification. This prevents theft of the system by an enemy on the battlefield and use against friendly forces. The authentication in biometrics can be done by any physical attribute of the soldier owner of the system. Biometrics can be applied to larger weapons systems

like tanks, aircraft, ship board firing systems (missiles and guns) and any other control systems (steering and helm, radar, etc) where there may be an embedded computer chip.

The Future of Computing Physics

Predicting the direction of computer sciences and especially computer security is a difficult, if not impossible, task. Professor Gerald Milburn of Australia attempts to explain the concept of the late Richard Feynman's quantum computer in the book "The Feynman Processor" [Milburn, 1998]. Feynman was a professor emeritus at California Tech University who work on the Manhattan Project when he was younger and was considered to be the best Physics Teacher of the 20th century. Both men are physicists who believe that light technology is the logical direction of computer chip manufacturing. Photons of light are the smallest possible atoms that can hold a digital state of 1 and 0. Light also is the fastest way to transmit data strings between computers. This is called quantum computer physics based on the theory of quantum entanglement explained by professor Milburn. Theoretically, this is the smallest and fastest we can expect any computer chip to process data. Fiber optic cable is one of the most secure mediums as any wiretapping can be monitored from the message sender. This book is important because it dares to bring forth a computer

manufacturing direction based on current day physics principles.

Executive View

It's hard to imagine any executive in the 21st century who does not understand the importance of computers to the company or government organization. Paul Strassman's book has been included in this literature review because of what he does not say about computer security [Strassman, 1984]. His book, "The Business Value of Computers" was written before he went to work for the DOD at the pentagon for President Bush, the elder. Everyone in government and military computer organizations read the book to understand where he was coming from. He uses rationalization about why computers help the business function, but never even talks about military intelligence or other clandestine uses of the computer as discussed here. The closest he comes to discussing computer security is to describe the risks of not using computer technology in a growing, thriving business. It is unfortunate to see that older people are slow to adapt and change to the new computer world, but a fact of life. This book is only recommended if you want to see why the SANS institute says top management makes 7 mistakes when it comes to computer security and the first is not recognizing that computer security is an important function of governments and companies everywhere. Strassman did discuss the CIO position in his 1991 book so it must have been his position that computer security is a highly delegable task which he had

no time to become familiar with. I am certain his years in the pentagon changed this perception. Future generations of executives will include CIO and computer experts who fully understand the importance on computer security to the business. Strassman talks about risk of loss of the computer function and this is the closest he comes to any type of positive notes on computer security. For his age group it may have been standard not to discuss computer security in the executive courses he took, but since the 1980's most masters degree programs and MBA's have at least a session on computer security. After the explosion of INTERNET in the 1990's computer security has really gotten fair treatment in government and businesses. The bottom line is that executives have to consider computer security at least as a risk factor in doing business today.

American Leadership Defined.

America has inherited a certain leadership style according to our form of democratic republic and the plans laid down by our founding fathers [Phillips, 1997]. The American Leadership style was used by such leaders as George Washington, Benjamin Franklin, and Thomas Jefferson. Phillips describes the American style of leadership to be one in which we build our vision, set goals, and involve everyone. American leadership is done with teamwork and is decisive. First the great American leader listens and then he communicates. This was the style of General Washington to use intelligence against the

British. The American commander travels with the troops. He also turns negatives into positives. He innovates and leverages all possible resources. The American leader attends to financial matters. He refuses to lose and continuously learns. He is a risk-taker. The American leader understands human nature. He has the ability to compromise and create a culture of compromise. Finally he can stick to and follow through on plans. These were the virtues of our forefathers and can be applied today to "Global Leadership in INFOSEC". Just because INFOSEC is a fairly 21st century innovation does not mean that we should avoid the time tested virtues of leadership shown by the great men of our early nation. Today we defend many of the constitutional rights they were wise enough to give us in operating our daily governments. Surely, they would have used the technologies of today to increase diplomacy and help other less fortunate countries survive critical acts of nature and war. Networking would have come under the innovative leadership of Doctor Benjamin Franklin who discovered and experimented with static electricity. He was an innovator and government minded ambassador to Paris in his lifetime. He would have ensured that we had qualified corps of information aged craftsmen to ensure domestic tranquility. General George Washington was a mater of understanding intelligence and verifying enemy positions during the Revolution. He ensured his troops were in the right place at the right time and as well equipped as they could be. He could have used network centric warfare or information warfare against our opponents to dominate battles of

that time. He had ill-equipped troops and many historians wonder at the amazing lengths Washington went to motivate his troops. He stayed with them in Valley Forge in 1776 and was a frequent visitor to the chapel to say a prayer over his troops. He listened to his men's needs for food, clothing, and war making goods and took action to procure them for the next spring of battle. He lost many men that winter and only God knows how General Washington felt about losing his men to the winter cold and diseases. Today, commanders who are effective in securing computer resources must not only be trained in the sciences but also in the humanities required of a good leader. The examples of Franklin and Washington give us something to build on in all levels of government today as we become more technologically advanced. The American Form of Leadership, 226 years old, should always be an internal working part of every leader's mind, heart, and soul as we enter the 21st century and become stewards of innovative computer security technologies and other areas such as biomedical, biometrics, command and control networks, and weapons platforms.

Articles

The best article on Encryption was entitled "Growing Development of Foreign Encryption Products in the Face of U.S. Export Regulations" from the Cyberspace Policy Institute at George Washington University. This article identified 805 hardware and

software products in 35 countries of the world that pose threats to the United States Leadership in cryptographic products. The foreign countries showed a 22% increase over a 1997 study in foreign encryption products. Some of the foreign encryption algorithms used were Triple DES, IDEA, BLOWFISH, RC5, or CAST-128. New cryptographic products appeared in 6 new countries since the 1997 report. A total of 512 countries either manufactured or distributed cryptographic products in about 67 countries outside the United States. The report further stated that the quality between American cryptography products and foreign products is comparable. Global economic growth parallels growth in the foreign encryption products arena. U.S. restrictions on encryption algorithm exports has actually increased the international encryption market. Another study in 2002 would help determine if the trends noted between 1997 and 1999 are continuing to grow in the foreign encryption products. Link this with the U.S. search for algorithms at NIST and the United States may be in the unenviable position of standardizing on some other countries product if it is of high enough quality. The world standards for encryption products are being improved by all the products listed in this report. The United States must compete with the world for the best and brightest encryption algorithms.

Articles on network centric warfare are abundant on the pentagon and DOD websites. The digital briefing books on the NRO and NSA from the George Washington University National Security Archives were also excellent resources. The new military

archives at College Park, University of Maryland campus provides additional references resources. The CIA articles and speeches by George Tenet and others were available from the CIA website. INTERNET access allowed viewing of recently declassified information in these briefing books.

The Best Computer Security Websites

NIST Computer Security Laboratory (www.nist.csl.gov)

This website has all the Federal Information Processing Publications online and the Computer Security Lab Circulars and Special Publications. This is best used for details of computer security procedures and practices required by federal government contracts. Many of these publications have been downloaded over the years and the NIST List 91 is attached which shows the current FIP PUBs topics. The lab was created as a result of computer legislation which authorized them to write technical standards for computer security. Remember that NIST handles all government agencies including independent agencies and executive agencies (cabinet and non-cabinet level) computer security. Military agency computer security is advised mostly by internal service computer groups and NSA NCSC. The overlap ensures everyone has covered their mission capability computer systems and services. Federal Contractors are also allowed access to these resources for computer security.

SEI Computer Emergency Response Team (CERT) (www.sei.cmu.edu)

This website has been used in this study for some data research on the number of hacker attack incidences and hotline calls from 1988-2000. The CERT has listed the primary alerts it has published and described the nature of each alert. Some are virus alerts like the recent “Love Bug” virus. Another example is the “denial of service” attacks that occurred in private company networks and knocked out several company's networks. The countermeasures are described for all the CERT alerts. The SEI CERT was created by congress in 1984 and reports to them on national computer security issues.

Federal Bureau of Investigation (FBI) (www.fbi.gov)

This website is the best on white collar crime prevention involving computers. The FBI has the “Carnivore” system description and the Internet Computer Fraud Center. The White collar crimes division investigates computer fraud, financial fraud crimes, and others that may be done with computers. Additionally, the public can report identity theft to this FBI unit also. The FBI Computer Laboratory is used by the nation to provide forensic computer evidence preservation for the courts systems in criminal computer cases. Finger print analysis (AFIS system) is done by computer algorithms in minutes instead of hours to identify criminals. The FBI also describes

probable “hacktivist” attacks (as political protests) on government and private computer systems during specific event dates like the Olympics, etc. The “new” FBI has the technical firepower to provide national foreign counterintelligence on a level unprecedented in past years.

SANS Institute (www.sans.org)

The SANS (System Administration Network Security) Institute has some of the best computer network security people in the nation who advise the NSA, National Security Council, and President. This website gives some great practical advice on computer network security like the top 7 mistakes management makes in computer security (Figure 20) and the top 10 ways a hacker attacks a network (Figure 19). Their staff is recognized throughout the country as “the” computer network security experts. They teach security methods to corporate network administrators as well as NSA and government staff members. They have “intrusion detection” tools, network authentication, firewalls, penetration testing, vulnerability detection, and other courses available to the public. Learning these tools prepares the best in the country to combat the myriad of computer hackers. White papers and posters are available from the company on various topics concerning computer network security.

Federation of American Scientists (www.fas.org)

This website is operated in Washington DC and describes a whole gamut of scientific concerns that the general scientist is concerned with like government secrets documents, countries who have developed nuclear capabilities, and some high level diagrams of a proposed nuclear defense missile system. There are also foreign country intelligence collection group links to websites all over the world. The political purpose of this website is not clear, but it was surely a place to learn some new information relating to the declassification executive order from president Clinton, the committee on government secrets, and foreign country intelligence agencies in developed nations of the world. This relates directly to the development of international computer security laws and global security as computers are used for command and control of firing nuclear weapons, radar detection, trajectory planning, and flight controls of most nuclear arsenals in the world. This was a sobering thought to see how much information was available from INTERNET without a current federal security clearance.

Department of Energy CIAC (www.ciac.gov)

This is the department of energy computer systems security website which was given by an interview with a member of NSA staff as a good reference for computer

security in the government. The website is rich with circulars and bulletins on computer security written by DOE employees. It is important to know that since computers were used in nuclear testing in Project Manhattan that DOE would have been an early user of supercomputers. In deed, they have some of the larger computers and networks in use today. The numbers of the bulletins on computer security are listed in the appropriate figure to compare consecutive series of years. The idea is that more circulars in certain years indicates higher levels of government concern for computer security in those calendar years.

George Washington University (**www.gwu.edu**)

Two websites were available at George Washington University. The CyberPolicy Institute and the National Security Archives were both great resources at GWU. They can also be accessed from other agency sources with web links to GWU. The Archives contained a number of briefing books on various previously top secret and secret programs such as the CIA CORONA program and other satellites to high level officials in the federal government.

Definition of Terms in Chapter 2

Chapter 2 contains many references from government and commercial sources and there were many acronyms used to digest the materials. Those acronyms are defined according to the normal usage of the word, phrase, or acronym in the environment of the government expert. The following terms were used in this chapter to explain the literature references researched:

1. AFCEA – Armed Forces Communications and Electronics Association located in Arlington, Virginia.
2. AFCERT – Air Force Computer Emergency Response Team.
3. NSA NCSC– National Security Agency National Computer Security Center, Ft. Meade, Maryland.
4. NIST FIP PUBS – National Institute of Standards and Technology Federal Information Processing Publications.
5. "Computer incidences" – a hacker attack or other computer network attack.
6. SEI CERT – Software Engineering Institute Computer Emergency Response Team.
7. SANS Institute – A company contracted to NSA for network and

information security (INFOSEC).

8. “Information Warfare” – The art of destroying an enemy command and control of computer networks and communications. Also protection of our computer resources from enemy attacks.
9. “Colossus” – The British computer systems used during WWII to decode German and Axis diplomatic and strategic messages.
10. “Clipper Chip” – A computer chip that contains the “Skipjack” algorithm in the computer security community.
11. PKI – Public Key Encryption
12. RSA – The algorithm named after the authors of this encryption algorithm whose patent becomes public domain in 2000. This means public companies can use the algorithm without having to pay royalties.
13. “Tempested computer” – A machine that is built with low radiation profiles for government agencies who want to protect information from detection through windows and buildings by enemy VDT radiation equipment.
14. “Trusted software” – Software that has encryption software and is built to government intelligence specifications.
15. “Orange Book” or “Rainbow” Series – The series that describes the

classification requirements for secured federal computer facilities.

16. "Manhattan Project" – The United States project during world war II to build an atomic bomb to end the war early.
17. "Cryptanalysis" – the act of analyzing messages and decoding crypto-codes.
18. ADP - Automatic Data Processing, today called Information Technology (IT).
19. CIA – Central Intelligence Agency at Langley, Virginia.
20. NATO – North Atlantic Treaty Organization
21. DOD – Department of Defense
22. CDROM – Compact Disk Read Only Memory
23. WTO – World Trade Organizations
24. FCC – Federal Communication Commission
25. UK – United Kingdom of England, Scotland, Wales and Ireland
26. G8 countries – European countries organization.
27. "Carnivore" System – FBI system to intercept telecommunications messages selectively.
28. CERT – Computer Emergency Response Team.
29. ADABAS – "Adaptable database" proprietary database used by US

Armed Forces.

30. AT&T – American Telephone and Telegraph Company.

31. CSPAN – Cable TV network of US congress.

32. "Crack" – To break a code and disable it from hiding the real message meaning.

33. RPC – Remote Procedure Calls (a C-like computer language that allows the programmer to bind two machines together using a protocol and bypass security at the higher level of the ISO model, AKA tunneling at the data layer of the ISO model).

34. SEI CERT – Software Engineering Institute Computer Emergency Response Team.

35. "Forensic Computer Evidence" – a computer after a crime has been committed. Blank sectors on the hard drive that may be revived by the forensic computer specialist of the FBI.

36. Trojan Horse – A type of computer security program left to activate that appears harmless. Similar to Greek gift left for Trojans to gain access to sack the city of Troy during Trojan war.

37. Audit log – A list of userids and commands issued in an operating system or database system designed for tracing system activity and computer

security.

38. Security kernel – a small set of operating system commands that secure a system.
39. Object – any single type of software artifact used in an operating system or database management system to perform actions or hold information about the system (meta-data). Objects are sued in object-oriented and events-oriented systems and networks.
40. System Penetration Testing – testing done to try to penetrate into an operating system software from outside the software.
41. Vulnerability Testing – testing to find the flaws and correct them in a computer operating system or network operating system.
42. DES – Data Encryption Standard
43. Encryption – the special coding of a message, letter, word, sentence, paragraph or other communication into a ciphered form that is unreadable without the decryption or cipher key.
44. Masquerade – a penetrator assumes the identity of a legitimate use after having obtained the proper identification through clandestine means.
45. Operator spoof – a clever penetrator who fools a computer operator into performing an action that compromises the system.

46. Piggybacking – the penetrator uses a special terminal to tap a communication line.
47. Clandestine code – A patch is made under the guise of correcting a bug in the operating system.
48. NAK – Negative acknowledgement.
49. NRO – National Reconnaissance Office
50. CORONA – An early U.S. satellite program by the CIA to film photographs from space returned in a canister.
51. SAMOS – Air Force Project Office who controlled satellite development.
52. GRAB – Navy Galactic Radiation and Background satellite.
53. KGB – Internal Soviet Union Intelligence Agency
54. GRU – External Soviet Union Intelligence Agency
55. GWU – George Washington University

Research Methods

Chapter 3

Introduction

The purpose of this chapter is to discuss data gathering methods and validity of the data. Data limitations are also discussed in detail. The chapter will outline the statistical method as the primary means of obtaining data and applying it to the basic hypothesis that computer security is becoming more and more needed as the nation continues to build the National Information Infrastructure. Data sources are well known secondary sources who have collected their own data such as the Carnegie-Mellon SEI CERT group and the FBI white collar crime unit. Data from the president's office website shows the U.S. is exposed to more technology discussions from the White House in 2000 than in 1992. The wild list from May 2000 shows the many more computer viruses in today's computer world than ever before [Appendix D].

The primary hypothesis data then leads to the fact that many organizations need to have computer security staff trained in the recommended solutions to deal with the increase in computer security breeches. There are certain recommendations to network and database managers that will help with improving organizational computer security in the government and private industry. This is not a panacea to all computer

crime and abuse, but recognizes the limitations of the data used. Attacks on network that are military based are ever more important to counter. Classified military attacks are not included in this study.

America has many technical weapons systems which implies more automated command and control using computer systems. These types of systems often are required to use cryptologic techniques of encoding data and databases before, during, and after transmission.

The Approach

The principles used in statistical analysis lend a good amount logical deduction whenever talking about security issues and technology. Measures of central tendency are useful in determining the increases in national computer security threats over the last 10 years. These numbers are simple, yet represent how much more complex the U.S. distributed computer network infrastructure has become. Averages and changes in the mean, median, and mode are useful to this analysis. The number of computers used by the US government would be as meaningless as the number of nuclear warheads produced. The numbers collected by certain sources can indicate areas of concern to government and corporate management. One of these areas is computer security. In many places this study uses top 10 lists to describe a point in statistical

analysis. Bar charts and pie charts are also included.

What Statistics?

This study does not use a normal distribution curve or other normative statistics because the data on computer crime should not be considered normative. In fact, the data and statistics can be extrapolated and analyzed in terms of predicted increasing trends from websites. In this way one can estimate what future computer security laws, attacks, viruses, and antidotes should focus upon. Statistics are objective and observed by organizations who may be biased towards proving there is a security problem to maintain their status as a security solution agency. The correlation was calculated for SEI Incidences and various other time-series variables in this study. The problem with this rationale is that many organizations are coming to the same conclusions based on separate data observed from the same population. Behavior patterns can be determined from the statistics gathered by the agencies. Best practices can also be prioritized based on the statistical data about computer crimes and security as observed by the SEI or FBI. The best practices used by 9 computer facilities plus 3 college computer facilities are use as observations of how to implement computer security. The World Almanac gives data on computer usage from 1991, 1993, 1994, and 1998.

Data Gathering Method

The method used in this study was the statistical analysis method. The method enabled the investigator to make rational observations and develop solutions and recommendations based on the findings. The data for the case was gathered over a period of six months, and it included data from agencies that have INTERNET websites and public data on the INTERNET. Actual full-blown computer crime data was not available directly form the agencies. Government computer executive published some of the data on computer contractors in the federal government and relate to percentages of the dollar amounts expended on computer security. The White House website was another source of data on technology press releases to the US for the past 7 years. A next step would be to gather data after 3-5 more years to validate or nullify the findings in this research.

Databases of the Study

The databases used in this study include the following organizational databases available to the public. Note that some are INTERNET resources and some are periodic publications. The best databases used in this study are:

1. Government Printing Office Access United States Code database
2. The FBI White Collar Crime Unit database
3. The SEI CERT Computer Security Reported Data from 1988-1999 database
4. SANS Institute Database and Education Programs in Computer Security
5. The Government Computer Executive Magazine “Top Government Contractors” issues.
6. The White House Press Releases on Technology for 1993-2000 database.
7. The NIST Computer Security Lab publications since 1960 database.
8. The Federation of American Scientists databases.
9. The US and foreign Computer Laws since 1900 database.
10. The Computer Virus Wild List of May 2000 database.
11. George Washington University Cyber Policy Institute and National Security Archive documents databases.
12. CIA online website of documents and mission.
13. The World Almanac 1993 and 2001 for demographic data on computer users, INTERNET, and cellular telephone usage in the world and U.S.

Due to the national security nature of this study, data from top secret and classified sources were not available, nor requested. The documents from the George

Washington University National Security Archives were marked unclassified on the web. The US Navy was helpful in directing the researcher to the user conference called “ShadowCon” with joint unclassified and classified attendees.

Analyzing the Available Data

Each of the 13 data sources used in this study is analyzed using various techniques available on microcomputers. In some cases a graph or chart was created and in others a list was created with the ten or top most cases listed. In comparing data from two sources for computer laws, the two lists were compared for title and type of laws as well as total number of laws. Some of the was presented in time series format and did not require manipulation.

METHOD I

Data collection by reading books, texts, magazines and other printed materials from organizations involved in computer security, computer laws, and countermeasures is prudent in any scientific effort to proof current computer security procedures and best practices. This includes comparisons and contrasts of computer laws in the US and UK. Also, top companies who contract in computer hardware, computer software, telecommunications, weapons systems, and IT are used here. Filtering of the

information was done by manual means in this case. The most advanced technology used for this was a word processor to transcribe the lists onto the research paper medium for the reader's evaluation and understanding. No surveys were done as part of this study. Method II used the INTERNET and search capabilities.

METHOD II

Data collection using online websites statistical research and automated search engines for search phrases and keywords related to computer security, computer laws, and countermeasures. This data is analyzed to prove the computer security crisis is numerically real and that the countermeasures are needed to help end users mitigate the risks of operating in an insecure computer security network environment. Where possible summary information has been transferred to computer spreadsheets to make numerical points of comparison. At times, lists have been used to show the basic relationships between technology business in the federal government and the inferred increase in computer security funding which should have taken place as a result of this investment in systems. Websites were especially good at providing up to date statistics on the SEI and FBI numbers of incidences in computer security. The Government Printing Office and White House websites allowed online searching and querying for data that the researcher needed to prove that technology has become

more prevalent in the US Code and White House Press Releases each successive year. Data collection was easier through automated means using INTERNET. It should be noted that the websites accessed are listed in an appendix to this study and that they are dynamically changing over time as a function of the webmaster and sysop changes to each website. As databases they serve as snapshots to the public for that specific timeframe.

METHOD III

Experiential subjective assessments of Ft. Meade student experiences in computer security and first hand knowledge as a professional computer systems programmer, applications developer, supervisor, and manager were used here. Additionally, best practices at the many computer facility assignments are used as a benchmark for better procedures that can be improved. This method helps determine what computer security actions are practical and cost effective to implement. This method of collecting my data has been most heuristic. I have experienced a variety of 9 government agencies computer networks environments and each had various computer security requirements and levels of secrecy required according to the mission of that agency. The agencies were US Air Force Academy, Bethesda Navy Medical Data Services Center, US Army Intelligence - CalTech Jet Propulsion Lab, US Navy

Ordnance Center at Indian Head, The Pentagon, Office of Personnel Management, The Federal Bureau of Investigation Headquarters, General Services Administration Central Office, Marine Corps Systems Development at Quantico, and Maryland State Highway Administration. The tasks at each installation included systems management and software and hardware engineering and development. Some of the tasks were completed as a contractor and others as a government civil servant. The university systems the researcher has been familiar with include St. Mary's College Univac mainframe timesharing to Towson State University in the mid 1970's using card punched programs, University of Maryland Univac 1108 mainframe card punch processor in the late 1970's, American University mainframe and microcomputer labs in the 1980's, client-server at Catonsville Community College and University of Maryland University College client-server workstation computer labs and open networks of the 1990's. The researcher has used best practices that have evolved over time as these systems have evolved. The computer security on each of these systems was different according to the methods employed at that time. General observations of the computer security procedures in each facility were very different and have contributed to the researcher's practical education in computer security management. Method III also included attending several conferences related to computer security and interviewing several of the nations best known security experts

in person and on the telephone.

Limitations of the Study

Data and statistics are limited by the fact that they are objective measures only. Any subjective observations may be discounted by many studies using statistics. The best study uses both subjective and objective statistical measures. Statistics can also be misinterpreted. Another problem is the amount of data in the sample population. There has to be enough trial cases to be valid for the overall population if one is to draw conclusions from the sample population. This study uses all national data from the entire population of computers and computer networks. Missing data is another problem with statistics. These data values must be represented in the data somehow as “no data”, “unknown”, or “not available” data values. All surveys that are used in statistics must have these values to be valid. The researcher has never managed work on a Cray computer system (or other Supercomputer) but has been exposed to market data and the COS (Cray Operating System). There exist many of these “supercomputers” which support operations such as the National Laboratory at Los Alamos, NSA, Cheyenne Mountain NORAD Complex, and some research universities. It has always been the researcher’s intention to “fly” as many computer systems as

possible during his career.

Validity and Uniqueness (Originality) of the Data

"There are lies, damned lies, and statistics." [Mark Twain]. The data in this paper may well be cynically viewed as propaganda designed to keep the agencies and companies perpetually funded to employ more computer people to fight computer hackers and attacks. However, this assertion must also be proven with public data and private (top-secret) data that are for the most part, unpublishable. The researcher's experience and current news events of the day seem to support the data from the FBI SEI, SANS group and others that suggest there are more computer security breeches today than ever before due to the large numbers of computer used in the government and industry. As a society, America is evermore dependent on computer processes and systems even in embedded military weapons and intelligence surveillance systems. The US government has been transforming systems technology from military and space usage into general business computers and technologies for several decades as a policy. Responsible systems managers and chief executives need to review their internal MIS organizations and ensure they are fully staffed with qualified Computer Security analysts. In deed, with the explosion of hacker attacks

worldwide, more laws, algorithms, encryption methods, standards, and guidelines must accompany the basic technology to ensure education and awareness of the general public to good computer security practices. Behavior modification at a young age when students first use INTERNET may be the new way to ensure computer security is a seriously studied discipline. The U.S. may soon see university computer sciences departments create new academic programs in computer security just as law schools have developed computer law courses. There is great congruence between computer law and computer security. National information and computer security improvement depends on the vigilance of life long computer security experts. The military has led in this area in the past and it is time to expand the role of the computer security officer from intelligence to best business practices.

Summary of Chapter 3

Chapter 3 discusses the research methodology used in this paper which is primarily statistical gathering from online databases. Additional data was obtained from source magazines, textbooks, and other printed media. The US Code CDROM was also consulted for data on the implementation of computer security related laws in the United States Congress. The research methodology of statistics points to the fact that since the early 1980's when small personal computers became mass-produced,

computer crimes have mushroomed in government and private networks. The SEI and FBI data shows this to be true. The number of computer security and computer related laws enacted and NIST standards published has increased faster in the United States than in Great Britain and has contributed to public awareness of both the problem and solutions. The number of congress people who served in the military and may have had early experiences with technical systems has gone down as veterans of WWII decreases due to natural causes. Many veterans used analog weapons systems, which were replaced by newer computer-controlled systems. Those who are elected now may not even know the difference as baby-boomers have always lived with the nuclear and computer sciences as part of everyday life. Surely, the US economy has recently benefited from computer and communications technology advancements in public corporations. The data shows that computer security attacks have been more frequent in 2000 that in 1988. What are the best practices to help a computer security or information security officer do his job better in today's world? Once the open minded MIS manager sees the trends in this data, they should advance to adopt as many of the recommendations outlined in the recommendations of this report.

Definition of Terms in Chapter 3

The research methodology of this paper is basically statistical where statistics

are available for computer security incidences nationwide. The paper does not focus in on any one company or agency but leans toward a macro-security view of the entire nation. This was possible because the FBI and SEI have published incident data online. The general terms and acronyms are outlined in the definition and acronyms section. These definitions may not be well known in other area of the computer sciences and military as the subject is most prudently approached conservatively with great disdain for white collar crime and misdemeanor behavior of a small group of computer programmers who give all programmers a bad name. Following is a brief summary of defined terms for the chapter:

1. FBI – Federal Bureau of Investigation white-collar crime unit.
2. SEI CERT – Software Engineering Institute Computer Emergency Response Team.
3. INTERNET – Global network available through personal computers linked to telecommunications devices.
4. CDROM – Compact Disk Read Only Memory.
5. NIST – National Institute of Standards and Technology.
6. Cryptology – the field of coded secret writings.
7. “Computer security incidence” – an attack on a computer system or network by malicious software such as Trojan Horse, logic bomb, virus, or macro-virus.
8. SANS Group – a company who specializes in computer network security on

contract to the federal government.

9. SAS – Statistical package on computer.

10. SPSS – Statistical Package for Social Sciences (computer based correlation, et al)

11. MIS – Management Information Systems (Sciences)

12. NORAD – North American Air Defense located at Cheyenne Mountain Complex, Colorado Springs, Colorado.

13. US Code – United States Code of Federal Regulations

14. COS – Cray Operating System

15. CIA – Central Intelligence Agency

Data Analysis

Chapter 4

Introduction

This chapter describes the data available from the literature and websites researched for this dissertation. In each case, conclusions have been drawn from the data based on experience and a conservative approach to computer security management where more protection is better than less and expenditures should be spent wisely. There are many things that can be included in the security program that are not expensive. However, upper management needs to fund a comprehensive computer security plan for maximum effectiveness. The security of government and private company data is equally important in all countries of the world. We should afford recognition to the data presented in this report as proof of the need for more computer security that is comprehensive and mature in nature. Global security depends on the abilities of countries to keep secrets during diplomatic discussions and meetings. In fact, this was the original intention of encryption in Ancient Egypt and Rome.

President Clinton's Data (Figure 1)

President Clinton has been one of the most proactive presidents in technology. Since

his inauguration he has made speeches that included the term “Technology” in more and more speeches over his 8 years in office. The data was acquired by searching his website under the press releases. The data shows a linear relationship over time with a positive slope. The correlation between SEI incidences and the president's press releases the over time frame from 1993 to 1999 was 0.8817 which is significantly positive. Why did this happen? The president always has claimed that he has kept the economy going strong and expansive. Maybe he assumed as others have that technology was driving the expansion of private firms the same way it helps government.

Congressional Leadership (Figure 2)

Leadership is key in any government organization. Figure 2 shows that the U.S. is seeing diminishing participation in the military by elected officials. This trend could be very good for businesses as elected officials are drawn from this pool of people. However, they may not be trained in military tactics and technologies. If this becomes the rule, instead of the exception, then America must face the fact that fewer veterans are aspiring to top elected positions. This curiously coincides with the deaths of many World War II veterans who had no choice in being conscripted into federal military service. Does it say that today’s adults who were mostly Vietnam age are not willing to fight for America’s freedom? Or is it that our society and nuclear détente are enough to keep America free? It is clear

that a military career is no longer a requirement for a congressional career as it once was. The number of congressmen with military experience further decreases from 205 in 1993 to 61 in 2007 when the data point is extrapolated. In fact, the correlation between the decrease in military experience and the increase in SEI hacker incidences reported is -0.9858. This indicates a strong inverse relationship between the two time series data. In other words, the less military experience in congress, the higher the number of SEI incidences from 1993 to 2007. However, there are more computer laws created during the 1990's to stop computer crime and hacker incidences.

Laws Comparison and Contrast (Appendix A & B, Figure 3)

Man is a being with laws. Since the Magna Carta, there have been hundreds of laws that describe good conduct by man in democracy. In recent times, America created the Declaration of Independence, Bill of Rights, and various federal and state Constitutions. It should be of no surprise those federal computer security laws and laws relating to computers have increased as the U.S. leads the Information Revolution. The British have created similar computer related laws, but created some of them (Patents and Trademarks) earlier than the U.S. It is interesting that other countries do not have significant computer related laws. The computer seems to be a real copyright of the democratic society. Figure 3 shows the number of U.S. laws and U.K. laws are 4-5 times more prevalent in the 1990's

than in the 1940's. The library of congress has volumes of international laws to assist congressional researchers in this area. The Bainbridge book describes how advanced British laws have become in the area of computer crime and computer security. U.S. law schools have been teaching computer law for several years as a specialty. Figure 3 shows that the trend in computer related laws are increasing since the 1940's in both the United State and the United Kingdom. This can be seen as a response to the increase in computer related "white collar" crime in the developing nations with advanced computer systems. The number of computer related laws in the 1940's was one fifth of the computer laws passed into legislation in the 1990's. As dependency on computers in our communications infrastructure increases, this trend will increase as shown in Figure 3 with a high correlation between laws enacted and hacker incidences.

OMB Funding of Computer Technology (Figure 4)

The Office of Management and Budget reports directly to the president. This office has directed the U.S. government to acquire and build information infrastructures over the past years administrations regardless of president. The fact that OMB directs policy towards hiring government computer contractors and systems management principles indicates strongly that the U.S. government is dependent on computers today and tomorrow. OMB Circulars are regulatory policy that describes how the government should

operate and manage computer resources. The major policies are listed in figure 3. Specifically, OMB A-130 section III discusses Computer Security in government systems. This guidance is used by all agencies with major computer systems acquisitions. This is proof that the U.S. government is very concerned about computer security in the last 25 years. Circular A-130 has been rewritten several times to cover new computer technology.

FBI and SEI CERT Incidences (Figures 5-7)

The FBI just opened a new White Collar Crime Unit that deals with computer crimes and other types of fraudulent behaviors. The data from the FBI shows that Incidences of Computer Crime are up between 1998 and 1999 according to alerts, advisories, and assessments issued by the FBI. The SEI data in figure 5 shows that since 1988 the number of computer security incidences nationwide have risen drastically from 6 to 12,000 incidences in 2000. This data is troubling. The SEI incidences in figure 5 were correlated with many other time-series trends in this report with positive values. This trend in increasing number of hacker incidences will probably increase as other variables also increase. The SEI hotline calls in figure 6 shows a sinosoidal wave. The next data point for 2000 may be up or down following the sine curve pattern. The FBI and SEI have resources to train professional organizations in computer security. They also are using the network infrastructure to warn the country's organizations of network threats to computer

security. They type and describe the threat as it was reported. Being on the email listserv of these computer security groups is not enough. Computer staff members who write source code and work on networks every day require additional training. SEI offers this type of training.

Higher Education (Figure 8 & 9)

MIT, Carnegie-Mellon, and Minnesota are the top 3 schools with Ph.D. programs in Management Information Systems or Computer Sciences. This data was aggregated from U.S. News and World Report. All of these schools should have computer security coursework as part of computer sciences, but few have a computer security major. In the future, U.S. schools will have a computer security major as another sub-discipline of computer sciences. The top 10 schools without Ph.D. programs include two military academies. These schools may graduate officers who specialize in computer security during their careers at military computer security schools. The military leads in this area, as use of computers for Information Warfare has become an accepted reality of the new battleground. Many of the systems created for the government are built by contractors.

DOD Systems Contractors (Figure 10-14)

Contractors usually accept higher risks on government projects to obtain a long-range business relationship with the government. DOD embedded computers is funded through long range appropriations. Figure 10 shows the amounts of funding for specific companies are very large for 1999 according to Government Executive Magazine.
The average amount of IT contract award for each company in the top 10 in figure 10 was $1.031 billion dollars. If only 1% of this is earmarked for computer security, then 10.31 million dollars would be budgeted for each of the ten IT companies listed. Figures 12-15 show the leading IT companies and services with the highest amount of embedded systems. The Army has the top funded Information Technology.

NIST Publications (Appendix C)

NIST publications describe the types of computer security standards required on federal contracts. NIST has the authority to publish federal computer security standards and examine standards at the computer security laboratory. The publications in Appendix C show how many of the standards are available over the INTERNET to the public. When developing computer systems, vendors should use these standards as a guideline. Military and DOD projects should also consult the NSA standards for computer security known as the “Rainbow Series”. NIST is a very useful source for both government and contractor people who have the task of implementing computer security. NIST helps agencies

understand the role of computer security in electronics security of federal civilian and military agencies. The individual military agencies have their own computer security functions and they all contribute to the NSA functions of providing distinct computer security functions for hire. Of course, NSA also works with the CIA to track global signals by listening in on potentially dangerous electronic messages. NIST publications are well known on government contracts where they are required viewing by the vendor before he can complete his mission. Contract requirements are the agreement that includes NIST computer security requirements and many other federal and state requirements. NIST publications become late night reading for the many contractors who support government computer work.

Foreign Encryption Products (Figure 16)

Figure 15 shows the development of foreign country encryption products. The highest percentage of new product come from the United Kingdom (17%). The U.K. has extensive resources in computer security and military intelligence of interest to the U.S. Other countries with significant encryption products developed are Canada (13%) and Germany (13%). This is evidence that high technology economies can afford the

investments in computer security and understand the role it plays in national and international security. It is interesting that of all the countries listed above, 10% are democracies who began building networks and infrastructures after WWII ended.

The correlation between SEI Incidences and number of new encryption products and companies between 1993 and 1999 was .9605. This suggests more foreign products were created to help stop the rise in computer crime incidences between 1993 and 1999.

DES 64 Algorithm (Figure 19)

The DES 64 algorithm in figure 19 is psuedocode from a computer networks text [Tannenbaum, 1984]. The algorithm is relatively short and concise as presented in figure 19. There are basically three parts to the algorithm. The algorithm works by taking a key and applying to the cipher text using 64 bits of information in each message part that is encrypted. Today, the RSA and other algorithms are much more reliable than the DES 64 algorithm. That is, they take much longer to be cracked by outsiders, even when they use computers.

Encryption Algorithms (Figure 20)

The major encryption algorithms used in computer security of data are listed in figure 20. These were obtained from the NIST and NSA documentation for unclassified algorithms. Some of the algorithms have longer crack times than others. That is, it takes longer for a computer to decipher an RSA code than and DES 64 code. Tests have shown this to be true. NIST has a competition to find the next most unbreakable algorithm. An algorithm that takes a thousand years for a computer to resolve is certainly secure (for a thousand years). What you have to remember is that computers tomorrow will be more powerful than today and will resolve these algorithms faster. New hardware always causes problems with software and new software must catch up to the hardware. The Escrowed Encryption Standard is a fairly new NIST algorithm for encryption. PGP stands for "Pretty Good Privacy" and covers emails and other message traffic that can be encrypted. PKI stands for Public Key Infrastructure and uses a public and private key plus the encryption algorithm to secure communications. Note that these algorithms are the most common encryption algorithms and that foreign nations have created their own encryption products in the wake of United States Export controls on encryption products (figure 15).

SANS Institute Network Top 10 Vulnerabilities (Figure 21).

Network systems vulnerabilities are organized in a priority listing by the SANS institute to tell the U.S. computer public which threats are the top 10. Then a company can buy products which address detecting and repairing the top ten vulnerabilities. Many of the vulnerabilities are only applied to UNIX, LINUX, or Windows NT operating systems. The computer security officer can obtain this ongoing list from SANS institute. They also do training in the local Washington Metropolitan and Baltimore Areas. Stephen Northcutt (SANS) and Randy Marchany (Virginia Tech) are excellent resources on this subject and both spoke at Shadowcon 2000 at Dahlgren NSWC. Data on US Navy Intrusion Detection incidences was not available for the public. Dr. Marchany helped develop the top ten list of network vulnerabilities. Organizations must test vulnerabilities in their own systems to ensure they are immune to the known attacks on networks. The original list also has the solutions to fixing the top ten vulnerabilities and these are available from SANS institute. Some examples of the types of security cracks are denial of service, Trojan horse, back door, and password guessing. These are a direct result of some of the top 10 vulnerabilities in computer networks. It is recommended that a full time computer security officer become very familiar with these 10 vulnerabilities and have an assessment done on his organization every six months to determine where the 'hot spots' in his network architecture may be compromised. Running an intrusion detection software will also help identify these vulnerabilities.

SANS Top 7 Mistakes by Top Management (Figure 22)

The top 7 mistakes made by senior management could be eliminated by the next few decades when there will no longer be any "analog" executives. Figure 20 shows the top 7 management mistakes according to the SANS Institute. The new digital executives who came up through the management information systems and Information technology ranks will forever change the way senior managers look at computer systems. One could hypothesize that senior executives of today are smarter than in previous generations about technology and computer security. It is possible for executives to be pro-computer security without having to know all the details. An executive who delegates authority may well want to only be kept abreast of major problems and may wish to be kept in the loop on financial decisions only. A good CIO should make the complex world of technology seem easy to the outsider and to upper management when required to do such. But he must also know the technical details of the job when asked. One of these details includes ensuring the budget for computer security and ensuring the proper hardware and software tools are acquired to get the job of computer security done. Thus the CIO shields senior management from mistakes is the MIS manager's job one. Still senior managers have authority to make decisions and thus make mistakes without knowing all ramifications. Communications up and down the chain of command is paramount to avoid as many

mistaken decisions as possible by everyone in the process of computer and information security.

Employed Mathematicians and Computer Scientists (Figure 23)

Figure 23 shows fast the increase in the number of employed mathematicians and computer scientists from 1991 to 1999 of 113% from 866 thousand to 1847 thousands. If one considers that the internal employee is the greatest risk for computer crime then the increase in the number of employed mathematicians and computer scientists sets a riskier precedent for computer crime then ever before. A high correlation of .9942 exists between the increasing number of computer experts and the increase in SEI incidences reported over the same time period. This threat assumes internal disgruntled mathematicians and computer scientists are suspect of committing computer crimes. The internal threat was documented by every author in computer security.

US Households Using INTERNET (Figures 24 & 25)

Figures 24 and 25 shows the number of US households using INTERNET by region and education level. The west uses INTERNET the most at 31.3% of population. This may be due to the increased mileage between cities in the western part of the United States and the connectivity that INTERNET offers. The south uses INTERNET the least at 25.4% of total population. This means there are more users of INTERNET in the west than in other parts of the United States and potentially more computer crime in the west also. 48.9% of INTERNET users were College educated. 16.3% were High School educated. Only 3.1% were elementary school level. This means that there is more chance of college educated peoples committing computer crimes. This was certainly a fact in the "Love Bug" virus case where a Phillipines college student created a virus for a college project. His instructor knew about his intent to cause computer crime according to Time magazine. The Morris vs. NSA case was about a masters degree student who let the INTERNET worm loose on government networks as a masters project to see if it would work as destroying computer network nodes.

US Households with Computers (Figures 26 & 27)

The number of US Households with computers has increased greatly since 1994 and 1999. Figures 26 and 27 show the increases between 1994 and 1998 of computers in US households. 48.4% of college educated people had personal computers in 1994 and

this increased by 20.3% in 4 years to 68.7% of college educated people in 1998. At this rate, by 2002 there would be 88.7% of college educated people with computers in the home. We are truly a digital society that will be 100% wired some day. High school educated people with computers increased from 14.8% in 1994 to 31.2% in 1998. This was an increase of 16.4% in this education level group. The smallest increase was the elementary school increase from 2.6% in 1994 to 7.9% in 1998. This was a 5.3% increase in the elementary school group. The significance of this growth in computers at home is again the increase in the number of chances for hacking and other crimes to take place where people have modems and advanced communications software from home.

Figure 27 shows the increase in number of computers used in households in various regions of the United States. The west had the highest percentage at 48.9% of households with computers in 1998. This increased 18.4% from 30.5% in 1994. The South again had the lowest percentage in computers in the households at 38% in 1998, up from 20.9% in 1994. These data are very similar to the INTERNET usage figures by region of the United States. It would seem to say that computers are more accepted by households in the west than other areas of the country. Again this may also indicate more chances for hacker attacks from this region of the country.

Increase in Cellular Telephone Subscriptions 1985-1999 (Figure 28)

Figure 28 shows the increase in cellular phone subscriptions between 1985 and 1999. In 1985 there were 340,213 cellular phone subscribers. In 1999, there were 86,047,003 cellular phone subscribers in the United States, the most of any country in the world. This was an incredible increase in cellular phone subscribers of 25,192% between 1985 and 1999. Surely this indicates the trends in mobile computing that affects all computer users. Denial of service attacks can use cellular phone lines to transmit data. The mobile INTERNET on telephone and Personal Data devices is becoming a reality. More people today are communicating in digital mode than ever before. This again is an indicator of the possible chances for abuse within the United States. An adversary could easily use this fact against us by infiltrating cellular phone usage and using this media as access to INTERNET hacking attacks. Other countries with significant cellular phone usage are Japan (48.4 million), Italy (30.2 million), and South Korea (23.4 million). This all falls well short of the 86.1 million in the United States [WAEG, 2001].

The "White" Rich Criminal Profile

More "white" people have computers and use INTERNET than any other race in the United States by a percentage (46.6% in 1999). There are also more people in the $50,000 and up income range who own computers (39.3%). [WAEG, 2001, p 571] This gives a profile of the computer hacker as being a "white" wealthy person. This is typical of

what is taught in computer security courses. Since there is more opportunity for hacking activities among this group, one would not expect the typical computer criminal to be of other races or outside this wealth status. Additionally, 35-50 year olds use the computer the most (54% each). This further stratifies the profile of the would be computer criminal here in the United States from within our society. Other parts of this paper have discussed foreign sources of computer crime.

Viruses (Wild List) (Appendix D)

Another threat to organizations network security is the macro virus and other types of computer viruses that can enter the system from outside sources. The list of viruses presented in this research is from May 2000. Whenever a virus is encountered, network anti-virus software should be run in "Detect and Clean" mode. The companies who create virus protection software allow new upgrades every six months to handle new viruses. MacAffee is one of the most popular virus scanners and repair software. Shareware is not recommended for virus detector software as there is no guarantee of covering most viruses. The Melissa virus was one that hit networks during 1999. The Michaelangelo virus is one that is suspected to hit on the same date every year like a time bomb. The "Love You" virus was launched in 2000 and the hacker found to be a 22 year old student in the Phillipines. Any virus is dangerous and can be found on the Wild List once found by the

public. With as many viruses as are listed on the Wild List, it is easy to see why computer security is becoming a big business in today's technology society. Few people are well trained in detecting and cleaning viruses properly. One of the best deterrents is to keep a good back up of your data. Viruses can not harm your data that is backed up if it is not on the hard disk at the time of the attack. A professional computer expert always operates with a backup of his data periodically.

Summary of Chapter 4

Chapter 4 describes some of the data in the figures researched for this paper. The president has issued more and more technology briefs from his White House position since 1992. They climbed from 200 to over 800 in 8 years. Congress is becoming less technically sophisticated as pointed out by the lack of military experience in new members in the class of 1999 compared to 1993. More data points to increased computer incidences occurring in the year 2000 than in any year past. Both SEI and the FBI data on incidences confirm this trend. OMB circulars are revised every few years to direct federal spending on computers and computer security systems. Military weapons systems have a large portion of embedded computer systems that are vulnerable to hacker attacks. The top military embedded computer systems and IT contractors are listed with the amounts of business in the billion dollar range. The portions of the military IT funding pie are shown in one of the

figures. Lockheed-Martin leads in this category. The Army has the top military systems spending according to Government Executive. The Navy and Air Force are next. The major systems that men and women of the military depend on for securing the nation are required to maintain out technological edge on foreign threats to U.S. security as a force multiplier. Computer and network Information security is required on these systems to ensure non-compromise in the current and future world theatres of operation. NIST publications help contractors and government secures computer systems they build by describing algorithms and standards. Foreign countries who have spending on encryption products most similar to the United States are the United Kingdom, Germany, and Canada. The list of six basic encryption algorithms is listed in this chapter. The top 10 vulnerabilities of network computing require closer examination by the serious computer security expert and organizations requiring more security analysis. No Company or agency should overlook computer security as an important element of corporate data security. This chapter has shown that there is both the need for more security and the means to achieve the computer security in all systems (embedded and un-embedded) through intrusion detection, network intrusion analysis, and virus scanning and repair.

Definition of Terms in Chapter 4

The following definition of terms apply to chapter 4. Many of the terms are used

in previous chapters and further discussed as results of data findings herein.

1. DES – Digital Encryption Standard
2. FBI – Federal Bureau of Investigation
3. INFOSEC – Information Security
4. NIPC – National Infrastructure Protection Center at the FBI
5. NIST – National Institutes of Standards and Technology, Gaithersburg, Md.
6. NSWC – Naval Surface Warfare Center, Dahlgren, Virginia.
7. OMB – Office of Management and Budget, Federal government, Washington DC.
8. SEI – Software Engineering Institute at Carnegie-Mellon University, Pittsburgh, Pa.
9. SHADOWCON 2000 – A conference held at Dalhgren NSWC, Virginia to improve computer network security.
10. IT – Information Technology

Summary, Findings, and Recommendations

Chapter 5

Summary

This section will summarize the findings in figures 1-19 where there is data and statistics from other sources. Collecting survey data was done on INTERNET and using publications available to the researching in hard copy from book publishers and federal agencies since 1977. There are common themes for the potential computer security officer to absorb before taking a position with a company or agency. Some of these were taken from the literature search. This chapter is a primer for the new computer security officer and gives him some ammunition to fight the common problems in computer security in organizations. Much of this chapter was gained as a computer security officer at the Navy Medical Data Services Center from 1977-1981 and other organizational assignments and texts read since then. Computer security can basically be viewed as a collateral duty of all technology staff and managers or as a primary duty assigned to a person for a duration of time with specific goals and results in mind.

Common Theme Findings

This will discuss the common themes in the paper across the literature review of military intelligence, computer security, and national computer policies and in the data

found. Some findings may not have been expected but are recorded here. It is common theme that there are computers (combat and non-combat) there are security compromise possibilities. All computer systems need computer security assessment testing and vulnerabilities analysis completed in government. There is not one but many areas where government data that is classified as secret can be compromised to outside sources. Another common theme is that the United States is not going to reduce the amount of technology used to protect our freedom any time in the near future. The military policy of leveraging technology to create force multiplier will be necessary as fewer and fewer people wish to have military careers in the United States. The real security in computer systems comes from testing systems to ensure that they are un-compromised by unwanted intruders. Large U.S. companies and foreign countries have the budgeted IT dollars to ensure global dominance of computer security by free countries. The United States has been unofficially asked to lead this sector of economy for the last 40 years and will continue to lead into the future. The creation of encryption standards helps companies and countries play on a level field with the United States. The U.S. can reap the same rewards in openness from other countries sharing programs. U.S. and British laws protect the citizens of these countries from having intellectual property stolen by others, inside and outside the countries. U.S. and British laws also punish computer crimes that were once non-felonies in the early days of computing. This is a good trend aimed at the protecting

the honest citizen and punishing intentional wrong-doings. There is a positive correlation between SEI incidences and independent variables of presidential press releases with technology, computer laws by decade, FBI alerts, foreign encryption products and companies, employed mathematicians and computer scientists, and increases in cellular phone subscriptions.

Specific Findings

Some of the specific findings follow in the sections below and will help the practitioner in his computer security planning and written documentation. These findings are aggregated from the data in figures in this paper and the real operational security policies of the U.S. Navy. Many of the findings below are developed upon the readings in literature and some on the data found online and in textbooks researched in this paper. Some of the findings are useful in developing operational policies and others are useful in developing a computer and information security policy in an organization.

Privacy Rights and Security Laws

The Privacy Act in America was signed into law in 1974. This was the official recognition of the arrival of “Big Brother” and designed to protect individuals data rights to protection. Today we are coping with identity theft and illegal use of personal data gained

from electronic media and other sources. Computer security began with the Privacy Act but was embedded in password authorizations long before the Privacy Act. The Privacy Act calmed the masses that feared technology and still do. The Electronic Communications Privacy Act is the 1990's version of the Privacy Act of 1974 in that it protects online communications privacy of INTERNET users in a computing world vastly improved from the 70's. Although Mr. Gore did not create INTERNET, he did help fund it when it was known as ARPANET. America is not alone when computer security algorithms are written by computer scientists. Foreign countries are able to export far more algorithms today than ever before. Export controls by America have actually spawned more algorithms and creativity by other nation-states to be self-dependent on encryption algorithms. American sensitive computer encryption algorithms are not for sale on the open world market and the world has responded in kind by producing more algorithms and products than ever before. Now the United States has to know how to use our algorithms and those of foreign countries. Some will be willing to share information with us as our allies (NATO). Others like IRAQ, IRAN and others may not be so willing to share anything with the west. America should continue encryption product moratoriums but should also be out in the marketplace testing foreign computer encryption products for the best available to use in our systems. Who says that other countries can not compete when National Defense depends on it? We must be forward thinking as we overtly and covertly assess the potency

of foreign encryption algorithms through academic consortiums with our allies. The George Washington Cyber Policy Institute study tells us that we have to be open and willing to exchange ideas with foreign countries when it comes to all encryption technologies. The computer security laws of tomorrow must protect America from foreign attacks and point us towards a new world of enabling everyone in society through technology. Too many laws and we will kill the imagination that creates great algorithms. Too much regulation defies the competitive nature of the American Programmer. Only sensible computer security laws should be put in place. It's hard to imagine that a congress with only a handful of experienced computer programmers could achieve this goal under the stress of producing legislation.

Funding INFOSEC

Funding for computer security and network security should be rising with the rising costs of computer systems and contractor fees in the government. Funding is definitely a part of contractor funding, but may not be earmarked for every product that is a deliverable to the U.S. military. Funding may be allocated for the NIPC and SEI operations to tell society about CERT alerts and what's out there. More funding is required to teach new computer scientists about good computer security in their programs and hardware. This is an area where a survey would be good. INFOSEC will be funded as long as government is

so dependent on technology as it is today. Penetration testing and vulnerability tests are now being done on a cost reimbursable basis and should be standard practice at mature IT organizations. If the NSA can not perform some of these tests into an organization's network then they need to perform the test themselves or get an out-sourced company to help with the analysis on a profit basis. The cost of funding the computer security function is well worth the US government's time and the Patent and Trademark Office for securing corporate secrets. Many companies chose to keep their secrets out of the patent offices even though they are protected for 17 years. 17 years can pass by very quickly.

Calculating Data Resource Value

The key to obtaining funding is to calculate the value of lost data. Lost data opportunity is also a calculation that can help managers understand the real value of data as a corporate asset. The corporation ceases to function when the data is taken away or data security is compromised. Data destruction has to be considered also. Un-recoverable scenarios are the most devastating to the organization. Data systems have to be recoverable to retain residual values. The data is the life blood of the organization and needs to be treated with numeric precision when a value is placed on it. Senior executives are used to calculating risks and values of tangibles and may find "data value" an abstract

term. It is abstract and it will kill the organization that does not know it's monetary value to business or military intelligence.

Threats Probability Matrix

The most effective annual review (and minimal) a manager can do is to create a threats matrix with factor weighted probabilities of certain events occurring in the organization (and facility) to destroy data and operation of computer systems. This is a common known technique done at Navy installations in a computer security installation review. It primarily covers the outside events that can affect a computing system or systems. Outside events that would terminate computer services are all considered threats in a military or non-military environment. The documentation is turned in as a report to the operations manager of a computer facility or kept on file and revised every year with new events and risks occurring that year.

Implementing the Security "Onion" Layers

The security "onion" layers as depicted in figure 17 show how layers can delay the cracker from intruding into your computer network. The sum of the layers creates so many layers of deflection that the would be criminal decides to give up on compromising the government or corporate system. When the effort is too much to be done by normal

means, the hacker will give up on the intrusion attempt. The outer layer is always physical protection of the system. The next few interior layers of security are procedural, hardware, firmware, software, and password security. All too often, password security is the only type of security on given computer systems. Passwords must be hard to guess and have some random characters or numbers in them to be effective. The DES 64 standard password is one which has random characters in it. This is usually a good default password. A weak password is “password” or any word that allows easy guessing. Passwords should be augmented by the outer layers of security to enhance overall computer security. In some cases, a SCIF, Secured Computer Information Facility, must be built that will prevent electronic emanations from penetrating the walls and windows of the computer room. This type of facility is built when the information is classified as top secret. Access to these areas is strictly limited on a need to know basis. The rooms can be like a vault which protects the computer hardware from theft or tampering. Procedures require signing in and out and only a few people have pass-codes for the door. This is the ultimate type of secure facility.

Secured Database Transactions

Every database transaction needs to be secured in the operating system or network operating system between end users and distributed databases. [Date, 1997] Security

classifications for every user must match that user's need to know or have the privilege instructions of read, update, delete, add, and write capability. Relational databases give the systems administrator a wealth of ways to secure the system. The responsibility must not be taken lightly or surely there will be a security breech. Hot and cold system backups must be generated on regular intervals to ensure backup and recovery. Every transaction on the network gets backed up when it acts on a database. This feature should be preset so that the DBA can work safely without putting out fires.

Secured Operating Systems

Operating systems provide many types of computer security in the hardware and software. Systems Programmers are a key link in securing a major computing facility in the government. A young programmer in this environment would be wise to study the protected area instructions of the computer systems and look for work on the access control lists and password lists. Encryption of these files would be advised so no one else could access them. Mainframe computers have similar data structures to many of today's microcomputers but are not accessible without proper authority. Physical and procedural security is more stringent in the mainframe world where you may be escorted out of the building if you learn too much. In these situations an expert could use a good lawyer who

understands how computer security is handled in the federal government. The local union representative will not know how to handle these cases.

Telecommunications Security in OSI Layers

Telecommunications security is inherent in the I*SO* OSI Telecommunications Standards model.[Tanenbaum, 1984] The security in messages using this standard comes in the form of applying an encryption standard to the body (text) of the message. Messages are surrounded by frames of routing data for the message in a packet switching network. The text (plain text) message is coded with an encryption key and an algorithm produces a cipher text. The receiver of the message is delivered the cipher text and key for decrypting the message through the application layer of the OSI model. Each layer of the OSI model has it's own additions to the frames (headers and trailers) of the individual messages sent along the data communications channel from the source to the target.

Optical Technologies and Security

Fiber optic channels are one of the most secure. Wiring tapping can be done to other channels of communication easier than fiber. Fiber cable can detect anyone tapping in or eves-dropping. Signals sent through microwave and satellite signals must be scrambled due to the possibility of interception. The light technology products offer greater

security throughout the systems used in telecommunications. One day light technologies will be the standard for communications media rather than the exception. The transatlantic cable is now fiber optic at 1/10 of the weight. Fiber optic cable easily converts to satellite channel through special hardware connectors. Fiber channels are easy to work with and will someday be the standard for cable transmission and security will be thus improved globally.

Network Intrusion Analysis

Systems administrators should be required to study computer security as part of their educational programs in colleges. Northcutt believes that Network Intrusion Analysis is a basic function that can be mastered by the computer security specialist to become familiar with the tools used in hacking and the methods used by hackers. For example, Northcutt teaches how the hacker attempts a “denial of service attack” by controlling two computers at once at intercepting the TCP/IP signals of one sender and sending it’s own message to the receiver node. Clearly, understanding the underlying technologies and how computers hand shake to connect are also required. It may be that the masters level technologist is a better candidate for network intrusion detection analysis, but as computer scientists we must push the knowledge to the undergraduate level to the fresh minds of those who might well become hackers if not fully indoctrinated into the computer security

field. Thus it is more difficult to regulate honest use of the gained network detection analysis techniques than it is to teach the material itself. Network intrusion analysis is a tool to combat illegal hackers in INTERNET and should be part of the overall education of the vigilant systems administrator. Tools can be purchased to add to the network administrators toolkit to help ensure network intruders are scanned. This is usually third party software that collects INTERNET messages and analysis the detailed data messages, frames, headers, and trailers on the information packet. The FBI “Carnivore” system has this ability to sniff packets on the wire and analyze information in the message before tagging the message to complete delivery to the receiver. Another technique called a “Honeypot” is used to assist with intrusion detection by offering an interesting fake server for the curious hacker and deterring him from altering code or destroying anything of value on the network. The Air Force CERT also uses an Intrusion Device on its INTERNET connection to intercept hackers. This technique is common among the various computer security units at federal agencies. State agencies could also use network intrusion detection analysis devices on INTERNET as they move towards putting more business on INTERNET. In fact, the Governor of Maryland has requested that 80% of all external business processes be automated on INTERNET websites by 2003. The state is moving towards this goal, but clearly INTERNET security through Intrusion Detection Analysis will be needed as the business volume grows on INTERNET and the agencies are exposed to

the same level of hacking that federal agencies who are ahead in technology development on INTERNET.

Biometrics Security

Biometrics systems stand between the physical security external to the computer systems and the access to the computer facility. This would be in the physical and procedural controls area of the Computer Security "Onion" layers. Biometrics have become very sophisticated and are at use in some of the very secure buildings in Washington DC such as the FBI Headquarters (J. Edgar Hoover Building). Biometrics link something personal about the person to his identity and authentication code. This can be facial thermal scans, fingerprints, voice print, or any other unique identifier of that person. They can be implemented on a smart card or other electronic device. The ability of non-replication of the Biometrics is important to protecting the identity of the person. The Biometrics Consortium Conference is held every year and is sponsored by NIST, NSA, GSA, and the US Army. Biometrics is a layer of security that must be used in real time high security government application areas. The annual Biometrics Conference held by NSA and NIST is an excellent resource for learning more about Biometrics contractors and devices that run software algorithms for this type of physical and access security controls.

Agencies needing an improved computer security function would be wise to attend this meeting held in the Washington D.C. metropolitan area.

Database Systems Redundancy

Database designers must be concerned with the security of data in electronic databases when the need exists for the data to be secured. Top secret data can be wrapped in relational databases like ORACLE or stored in an encrypted mode in other databases like ADABAS and DBASE. There has to be consideration for total database security, which mandates a backup copy or redundant copy of the database being available for cross over from the 'hot' database in event of a crash. Databases frequently encounter head crashes and other hardware problems that require new system hardware. Redundancy is a security method in database architectures. In fact, NASA uses redundant computer systems on the space shuttle to ensure computer security on the flight. This is a type of operational security that maintains 100% availability of the systems resources. In critical computer operations, redundant systems are a must to maintain low failure rates and times to repair existing hardware and software failures. Failures will occur in every system if it has enough time to run online. Figure 16 shows a possible configuration of redundant databases and redundant processors.

Access Control Lists

Today the system administrator is entrusted with access control lists that read into the operating system or database system and must be changed automatically by the end user when 90 days is up. Novell requires the end user to change his password every 90 days. This is good control of passwords to access control lists in the operating system. The system administrator is the only person who should have access to this list with update authority and rights. This file should be encrypted and backed up in a special place in case of system disaster. The best access lists can be cracked by hackers. A screen that allows the user to try more than three times to enter a proper userid and password is a bad security screen. A hacker could try hundreds of combinations in an automated software utility until it finds the right access userid and password. Most databases use access control lists and security schemes that are relative to the users rights and the table he wishes to access. These are the most sacred of tables in the database and also have only one system administrator who has the master update control of all userids and passwords. For example, ORACLE, DB2, and ADABAS all have access control tables with userids and passwords encrypted. Novell has an access control list that is kept on the server. These are highly protected and the master password and userid should be kept secret. The

systems programmer is very powerful when it comes to protecting the userids and passwords on the system.

New Encryption Algorithms

The best of encryption algorithm can be cracked when enough time is given to the task. NIST has contests for new encryption algorithms to replace the old algorithms. Figure 17 shows the DES algorithm from a telecommunication college text book [Tannenbaum, 1984]. The RSA algorithm is another good algorithm for encrypting messages. The algorithms in figure 20 are the best algorithms on the market at this time. Any of these algorithms will give the desired effect of software security in message sending. NIST is constantly looking for algorithms that are patented and can replace current encryption algorithms through annual contests. The United States should continue to create the best software in the world and search for the best methods in the world, regardless of the originator of the encryption algorithm. We are truly a leader and can not afford to be arrogant when it comes to recognizing new algorithms worldwide. We should embrace the new algorithms that win in NIST competitions from US and foreign countries that are legally exchanging software and hardware.

Annual Information Technology Contingency Plan

An effective IT manager will update an annual contingency plan that includes threats analysis of the computing environment and discusses some of the aspects of maintaining good computer security in the data processing facility. This annual IT plan can be published for others to view the best practices currently being used. The format of the document would look something like this:

1. Background
2. Purpose of Plan
3. Business and Technical Environment
4. Threats Matrix (numeration and documentation of problems from observations of environment)

Threat	Probability of Occurrence (0-1.0)	Priority Factor (5=high 1 = low)	Weighted Rank (higher more critical)
Water	.01	3	.03
Fire	.03	4	.12
Smoke Damage	.01	2	.02
Computer Viruses	.20	1	.20
Electrical Brown Out	.15	2	.30

Network Intrusion	.12	2	.24
Insider Attack (Disgruntled)	.15	3	.45
Accidental Erasure	.05	5	.25

(sample data for probabilities, factors, and weighted rankings)

5. Analysis and discussion of threats matrix (varies for every installation)
6. Countermeasures for Threats Matrix
7. Recommendations and conclusions summary

The annual IT contingency plan should be updated to reflect the current threats and probabilities of threats occurring based on the immediately previous year experience in the organization. For instance, if an organization experiences a power failure once a year then the availability of the system may be affected and a probability can be assigned. The more days the power is out the higher the probability of failure and thus the threat probability increases for electrical failure.

Measuring More Reliable Systems

System reliability was taught in a Real Time systems course at American University with chapters on availability and reliability of computer systems [Tebbs, 1977]. Reliability engineering is the discipline that covers this type of calculation as well as the Mean Time to Repair (MTTR) and Mean Time Between Failure (MTBF). A lower MTTR is desirable in

highly reliable systems. Likewise, a higher MTBF is better for higher reliability systems. Overall availability is calculated:

$$\text{Availability } A = \frac{MTBF}{MTBF + MTTR}$$

According to Tebbs and Collins, the overall system availability is enhanced by building serial or parallel machine circuits. Figure 16 shows how the redundancy in processors and databases are enhanced through parallel circuited machine units and a serial circuit. Serial circuits are less reliable than parallel circuits. For serial circuits and parallel circuits the calculations are :

Serial Availability = A1 x A2 x A3 x A4 x……xAn

Parallel Availability = 1-(1-A1)(1-A2)(1-A3) or 1-(1-A)**n

The real world solutions may require both serial and parallel circuits between network machine units (Servers, Modem pools, UPS, Client PCs) which requires a combination of the serial and parallel calculations done to determine the system probability. Tebbs and Collins also discussed security and integrity in mainframe computers of the 1970's. They discuss physical security and password security as main components of an overall plan. Integrity is the ability to keep the data and information accurate. Accidental corruption from chance coincidences in the operating system occur due to mainframe time

shared approach to memory management. The deadly embrace can easily occur when multiple users are accessing data online and in batch mode in mainframes. The deadly embrace is when two users are each waiting for the other user to free up the same data resources.

Engineering Calculations

The Engineer-In-Training Reference Manual has an entire section devoted to reliability and availability of systems calculations [Lindenburg, 1998]. Sometimes this is also called System Failure Analysis. There are a plethora of other calculations that are useful to the reasoned person in studying system operations research. The key is that a mathematical minded person can convey the mathematical representation of a systems reliability and availability to managers and staff when required. All these calculations may become part of the annual IT Contingency plan when discussing all units of an evolving computer system or embedded computer in a weapons system.

Backup the Backup

Every systems manager knows his first responsibility is to bring up a dead system from scratch in event of a problem with the computer facility. A good systems manager always has a current backup to the next previous week or day. A good backup is

described as a real-time recovery to operational capability. This includes storage of the backup data off-site in case of total destruction of the primary computer facility. The off site storage is then available to bring up the backup site which becomes the primary computing site. Network and database server backups should be run incrementally (nightly) and periodically full (monthly and/or weekly) for most facilities. The failure to take any backups is planning to fail when the system has a problem. Backups should also be tested for recovery procedures working properly. Backups are useless if they can not be recovered or they are not documented properly. There are current software and hardware dedicated to backing up the networks of organizations. Streaming tape drives and network backup software is recommended to build this capability and keep it on schedule. Automated backup software may allow for unattended backups of servers. Sometimes "hot" or "cold" backups are needed based on a database server operational status. "Hot" backups are taken when the system is up and running in ORACLE terminology. "Cold" backups are taken when the system is down. Both run from ORACLE backup scripts. ORACLE also has an export function that allows the administrator to create an "Export" file from any ORACLE set of tables. There are many contractors and vendors of these types of backups. It is wise to choose a highly reliable backup system that has an independent power supply to operate in times of distress on the computer center electric supply. This greatly improves computer security of the facility by having contingency routines and

support hardware and software in place to augment the systems programmer oversight of the backup processes.

Return on Investment in Risk Mitigation

Each of the elements of the threats matrix must be mitigated in order to proof that the system threats have been countered. Risk mitigation may require a person to be hired to ensure backups and recovery procedures are in place. It may also be required to ensure operation at a high availability rate. The return on investment in risk mitigation will be the successful operation of the corporation and corporate databases where the value has been calculated. A corporation or business with no data value has no business value. Data equals the resource that a company must have to continue to operate. The CSO must ensure that the company can survive any disaster involving the computer resources. This sometimes may fall into the lap of the computer network administrator and manager as he produces system backups and a contingency plan that is an ongoing model for computer health. Some authors discuss a risk mitigation management plan in systems development processes to avoid a failed system build [Pressman, 1999]. Pressman suggests that this RMM plan is useful for systems builders in determining what threats in the computer development environment might cause havoc to the system development process. Some type of threats include systems engineers leaving the project, passwords being

compromised, source code be left half complete, project planning left incomplete, and poor project management and supervision on the systems development task. Pressman is unique in his recommendation of a series of systems documents that can be used at every phase of the systems development life cycle by even non-technical people. The documents keep the thoughts on paper and save money that would be spent somewhere else. Indeed a good strategic IT plan contains many long term elements of migrating to a new a computer environment in organizations. This provides a measure of increased security in that a written technical plan should discuss security and integrity issues of data, software, equipment, and procedures.

The New Computer Security Officer Role

The organizations without computer security officers will soon be in the minority. Many organizations have various managers and administrative people doing computer security officer duties, but this is probably less effective than hiring a computer scientist who may know more on the technical side of the business and network information security. Definitely a person with great mathematical abilities and the ability to play out scenarios is required for the position. The person must also have knowledge specific to general security and computer security training and experience. Organizations who fail to have this

responsibility with high visibility run a risk of losing operational and strategic data across all organization boundaries when and if they have a catastrophe or computer network failure.

Organizational Security Mindset

The organization must be sensitized to computer security for there to exist a feeling of security by the computer users. Typically, computer users who know there is a security officer online are more cautious about how they use the computer resources. This is the only way to monitor system insiders. Privacy Act requires security officers to let it be known that users are being monitored and should contact the computer security person if there is a breech of security such as a virus found. Many organizations allow the systems administration staff also perform computer security since that person handles user-ids and sign-ins to the network. This works well if the systems administrator has the training and knowledge about the other areas of computer security also. A computer security course is recommended for organizations who wish to take this part-time approach to the problem.

The CIO and Computer Security

The CIO is sometimes the person who the computer security officer reports to. In some cases the CIO **is** the computer security officer. This places the computer security function above many other line functions in the organization with due authority over

computer users who might otherwise violate the computer security rules. The computer security person needs the cooperation of the staff and the network administrator to be successful. The CIO or CEO give the authority to the computer security officer to engage in investigations involving computer resources abuses or intrusions. The Computer security person should have intrusion detection training for network environments and should work with the systems administrator. The CIO must also have analysis and managerial sensibility so the company does not lose any value on computer security that may be outdated. The computer security awareness must grow with the technology of the company or nation. A good CIO can make employees aware on the needs for computer security in subtle tactful means without firing talented staff. The CIO in the federal government is the CIA head and FBI head for the most part. Military agencies have their own CIO's with just as much knowledge and experience, sometimes more than the civilian counterpart. It is never recommended to allow a person into this role with less than college or post bachelor's work in computer technology or engineering. CIO's have come from accounting and psychology backgrounds in state and federal agencies. They have no operational experience in computer security but are asked to perform this as one of their functions. If the CIO is not the computer security expert than the organization suffers and the reputation of the agency suffers with the image of a square peg in a round hole. CEO's who appoint CIO's should take past experience in computing into consideration, but one

does not see this in today's government. Technical ability and knowledge are not pre-requisites for good executives with the exception of the CIO. The same is true for a Chief Knowledge Officer (CKO) position. How could a CKO be a person with a psychology degree and friends in high places? This person should have the right mix of computer knowledge including computer security and artificial intelligence and human resources management skills. Too many senior appointments are made on the basis of friendships and political alliances rather than the best person for the job by background and past job experience.

Computer Security Outsourcing

There are companies who specialize in computer security and who have staff who is trained in computer security. This would be wise for a short turn improvement in data processing systems environments. The bigger companies can hire a sub-contractor or may have someone on staff who is capable of handling computer security tasks and responsibilities. More and more government organizations are out-sourcing all computer work including computer security. In years past, government agencies would not out-source computer security as it is a main function crossing organizational lines. For example, NSA has recently out-sourced 1000 computer security jobs to the private sector.

Teams in today's working environments require out-sourcing for critical skills (such as someone with a particular programming language knowledge on one project) when they are not available in-house.

Computer Security Education Revolution

Computer security education will undergo a revolution when computer security becomes such a large subspecialty that in depth training in computer security is required for positions. The U.S. colleges will create new disciplines to encompass computer security as a special topic within computer sciences. This may already be a reality in some technical schools. The federal government has special computer security training at schools that can be attended by security agency personnel. This specialized training will continue. The private sector also has computer training through organizations like SANS institute who also have computer security certificate programs in general security, network intrusion, et al. The future is bright for those who are willing to invest resources in training in computer security beyond the limited college courses of today. The colleges of tomorrow will have the education that responds to the need for more people of specific caliber to attack and prevent computer hackers from ransacking government and private computer networks and database resources. It is predicted this revolution will occur in the next few years prior to year 2010. The education of new computer network security officers at the

junior college and undergraduate levels will be welcomed by the current practitioners of computer information sciences, management information systems, computer scientists, and telecommunications specialists. Currently the federal government (NSA) send it's systems administrators and security specialists to the SANS institute and Naval Postgraduate Computer Security School and other military computer schools. Universities need to catch up to the hands-on approaches used in these courses to maximize student knowledge gains.

Strategies through Written Policies

Organizations should have computer security policies written down to be able to prosecute those who do not comply as a condition of working for the firm. The government computers in the military almost always have a giant page disclaimer stating that a system has classified data and is considered sensitive and that intruders will be prosecuted. This may warn off some hackers, but it may also signal the beginning of an attack against a website or database that continues until breached. The abysmal failure of such warnings should drive organizations to more passive methods of capturing violators. A written policy only helps when the attacker may be an insider and gives legal premises for dismissal. It is a must when an organization is serious about computer security. Fortunately, congress has given more legal authority to prosecute computer criminals in recent years. Congress

needs to stay on the vigil for nuances of any technology where National Security is involved. This is becoming increasingly more difficult when fewer and fewer congress people who are elected have deep technology backgrounds. The days of Congress having John Glenn type senators who are real technology heroes may be vanishing with the "greatest generation". At last count there was only 1 congressman who listed computer programming as a previous profession in the CSPAN directory for 1999. This is the sad state of affairs in our country and education system. The best and brightest never make it to the top in a system corrupted by money and outside influences as suggested by Arizona Senator John McCain and his campaign finance reform. Thank god we have a few heroes left from the Vietnam generation who understand computer security, intelligence, and technology.

Keeping Government Secrets

NSA and NIST have federal government authority to keep the nation's cryptographic secrets. NIST secrets can be compromised by a simple phone call. Thank goodness NSA doesn't bend that easy. One of the country's greatest secrets is that if one tries hard enough there are no secrets. Holding a top secret clearance does not hold the weight in government that it once did. The intent of the computer security agencies to keep our secrets safe is a prudent policy stance. Foreign countries have been trying to steal

technology secrets for years. The former Soviet Union paid $50,000 for a copy of ADABAS which is used by the Marines. NATO allies found out and foiled the sale. It is an oxymoron of governing by democracy that the freedoms we fight for are the same ones that open us to foreign intelligence agents here in the states. The Federation of American Scientists believe in openly discussing all technologies. It is the stance of this paper that more discretion in protecting algorithms is better than less. We can not give away any of the standards in encryption. Like many ANSI standards which cost upwards of $150.00, NIST standards can be downloaded. These include encryption standards and are provided to stimulate the economy of smaller more competitive companies. It would be wise to force a registration by the NIST whenever any standards involving encryption methods and algorithms are downloaded via INTERNET. This type of protection can be subverted by anyone but is a minimal. The FBI forensic computer evidence lab has the capability to track and record any clandestine computer activity by foreign nationals here in America.

Data from the SEI shows that more intrusion incidences are occurring on INTERNET and thus we need to protect INTERNET resources. The best kept secrets are the ones we keep on our own agencies. We should constantly be doing vulnerability analysis on our own networks in organizations. NSA is meeting this challenge. The Dahlgren Navy Weapons Test Center is home of the Navy's Shadowcon group who provide electronic network security for the Navy. The Air Force has the AFCERT. The FBI covers many of

the executive and independent agencies. Be assured, we are becoming more ready as a nation to win the network and information wars.

Solutions Looking for Problems

This is a common situation in the computing industry where people have solutions and know how to stop computer hackers, but are not playing the role of computer security officer in any organization. With only a small fraction of the computer industry trained in the specialty of computer security, it turns out that those few people are looking for most of the problems to solve. They may be vulnerability assessors or intrusion detectors. The technology is so specific and fast evolving that it has the appearance of people with solutions looking for problems. This can be solved by cross training computer security staff in more areas to broaden their backgrounds and reap the returns on investment in human intelligence and human capital. "Human intelligence" is leverage on most technology problems and helps us as humans deal with the myriad of technology we are asked to master in a single lifetime according to the president of AFCEA.

Demographics of Change

The demographics of computer, INTERNET, and cellular telephones increases in the

United States all indicate a society that is more and more dependent on computers, INTERNET, and cellular phones during the last 6-15 years. Computer systems are no longer just the providence of the governments and states in America. We have saturated our very homes with electronic communications devices. The market saturation point may not have been reached yet and we can expect further market penetration in the coming years. Truly the "Bull" market of the 1990's was spearheaded by the technology stocks and sector which would include products that fueled this change. More people than ever are computer scientists and hobbyist computer novices. Even education has began teaching computer sciences as a secondary skill to the many sciences and business skills. There is no longer a mystic about being a computer programmer as there was in the pre-1980's. Everyone thinks they can handle the complex programs written on mainframes such as assembler language macros and sysgens (system generations). This is just not true. The computer programmer of yesteryear and more full control of every aspect of computer rather than sharing it with other sub-specialties in computer sciences and Information Technology. Computer security was always the domain of the applications programmer and the systems programmer and today has become the domain of anyone using a computer. The most popular business software in 1999 was the Anti-Virus programs. This shows the awareness of the public to the issue of computer security at the PC level. Higher income people in the United States also had more computer systems. Surely, the

demographics will change in the next ten years towards more varied types of computer systems and security that the public can utilize on home computers. Government agencies will have to absolve themselves of the all-knowing and continue to develop computer security programs that help the very people who might be committing the computer crimes and hacker attacks. Government must also keep an eye on the demographic trends to provide better regulation of the computer industry and the nation's direction towards a safer computer environment on the entire planet. The data in this research suggests we are seeing more of everything in technology: computer users, computer scientists, INTERNET users, and computer crime and abuse.

Recommendations for Further Research

Recommendations for further research focuses on two areas. One area is going deeper into the executive views computer security. A survey of executives concerning computer security factors in their business risk mitigation planning would help quantify how many organizations are lacking in good computer security due to top management mistakes about INFOSEC and it's costs. This paper has attempted to explore the question of computer security leadership in the United States as a part of the new technology economy. The computer security and information security

defenses of corporations and agencies depends on developing new people to replace retiring personnel and staff. Any research that helps the public understand the new threats and potential threats to organizational data security and intelligence gathering are a welcome addition to the professional computer community. America is the best free country in the world and needs to maintain her lead in all technology categories and not just computer security and information security. This paper presupposes that America will always be a country smart enough and bright enough to stay ahead of other countries in the world through diplomacy and preparation for information warfare and future conflicts that will be fought before any bodies are at risk on the battlefield.

Definitions of Terms in Chapter 5.

The following terms and abbreviations apply to chapter 5. Some of these terms were used in previous chapters also. These terms are also included in the glossary of terms and acronyms at the end of this paper.

1. CEO – Chief Executive Officer
2. CERT – Computer Emergency Response Team
3. CIO – Chief Information Officer
4. CSO – Chief Security Officer

5. FBI – Federal Bureau of Investigation
6. ISO OSI – International Standards Organization Open Systems Interconnection
7. NIPC – National Infrastructure Protection Center
8. NIST – National Institute of Standards and Technology, once was called National Bureau of Standards (NBS)
9. NSA – National Security Agency
10. SEI – Software Engineering Institute
11. CKO – Chief Knowledge Officer
12. Intrusion detector – A person or software finding unauthorized incoming packets or code on the computer network.
13. Hacker – any user attempting to cause malicious damage to the software assets of an organization.
14. Vulnerability Analysis – a test to ensure the system vulnerabilities are discovered before a security violation occurs.
15. Penetration testing – the act of trying to get into (or penetrate) a computer system from outside the organization.
16. NASA – National Aeronautical and Space Administration
17. ORACLE – A proprietary relational database management system used by NSA and many other government agencies including Navy, and Maryland DOT.

19. DES – Data Encryption Standard for 64 bit encryption.
20. RSA – A newer algorithm named after the three authors' last names.
21. ADABAS – Adaptable Database by Software AG (linked list database although the company has claimed to follow some of the EF Codd's 12 rules of a relational databases).
22. SCIF – Secure Computer Information Facility (military term).
23. DBASE – a microcomputer relational database system that started as a file manager.
24. SEI – Software Engineering Institute (at Carnegie Mellon University in Pittsburgh) created by act of congress in 1988.
25. Access Control List – a list of system userids and passwords in an operating system, database, or network that require user inputs to access resources.
26. Novell Netware – A Network operating system used by many agencies to link personal computers together on a network.
27. Windows NT – A network operating file system by Microsoft.
28. Utility – A computer program designed to perform a single function very well without being in an entire application.
29. AFCERT – Air Force Computer Emergency Response Team.
30. Human Intelligence – The human resources value to the system of collecting data

and military intelligence.

31. Shadowcon – The NSWC Dahlgren, Virginia conference on computer and network security.
32. NSWC – Naval Surface Weapons Center.
33. NATO – North Atlantic Treaty Organization
34. ANSI – American National Standards Institute
35. INFOSEC – Information Security
36. GSA – General Services Administration
37. AFCEA – Armed Forces Communications and Electronics Association
38. Reliability – The amount of time a computer system is operating with failure.
39. Availability – A calculation that determines the uptime of the computer system in a probability. (e.g. 99% availability)
40. MTBF - Mean Time Between Failures
41. MTTR – Mean Time to Repair
42. Serial Circuit – A circuit where all nodes are dependent on previous nodes for electronic signal and voltage to operate.
43. Parallel Circuit – A circuit where nodes operate non-dependent on each other usually side by side with electronic signal split into N nodes that operate simultaneously.

44. Mixed Circuit – A circuit that contains both serial and parallel circuits for any computer machine equipment and flow of electrical current through those devices.
45. Cellular Subscription – A monthly fee for cellular phone services by any of the companies.

Figures

Figure 1

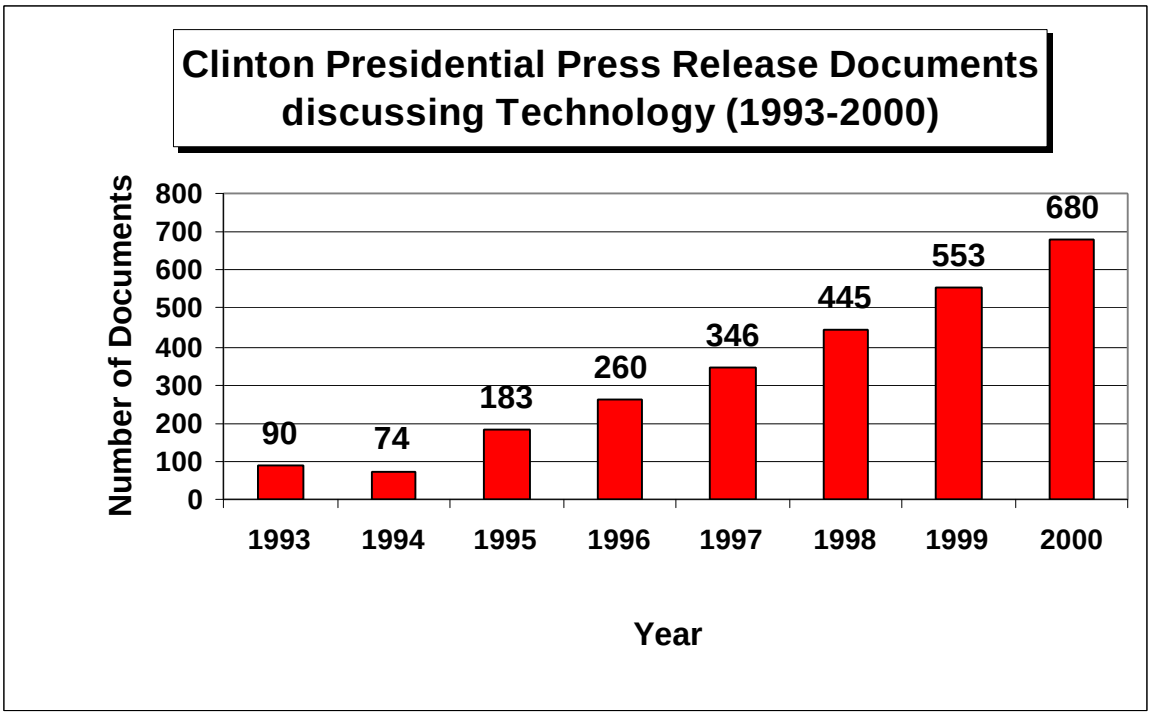


Figure 2

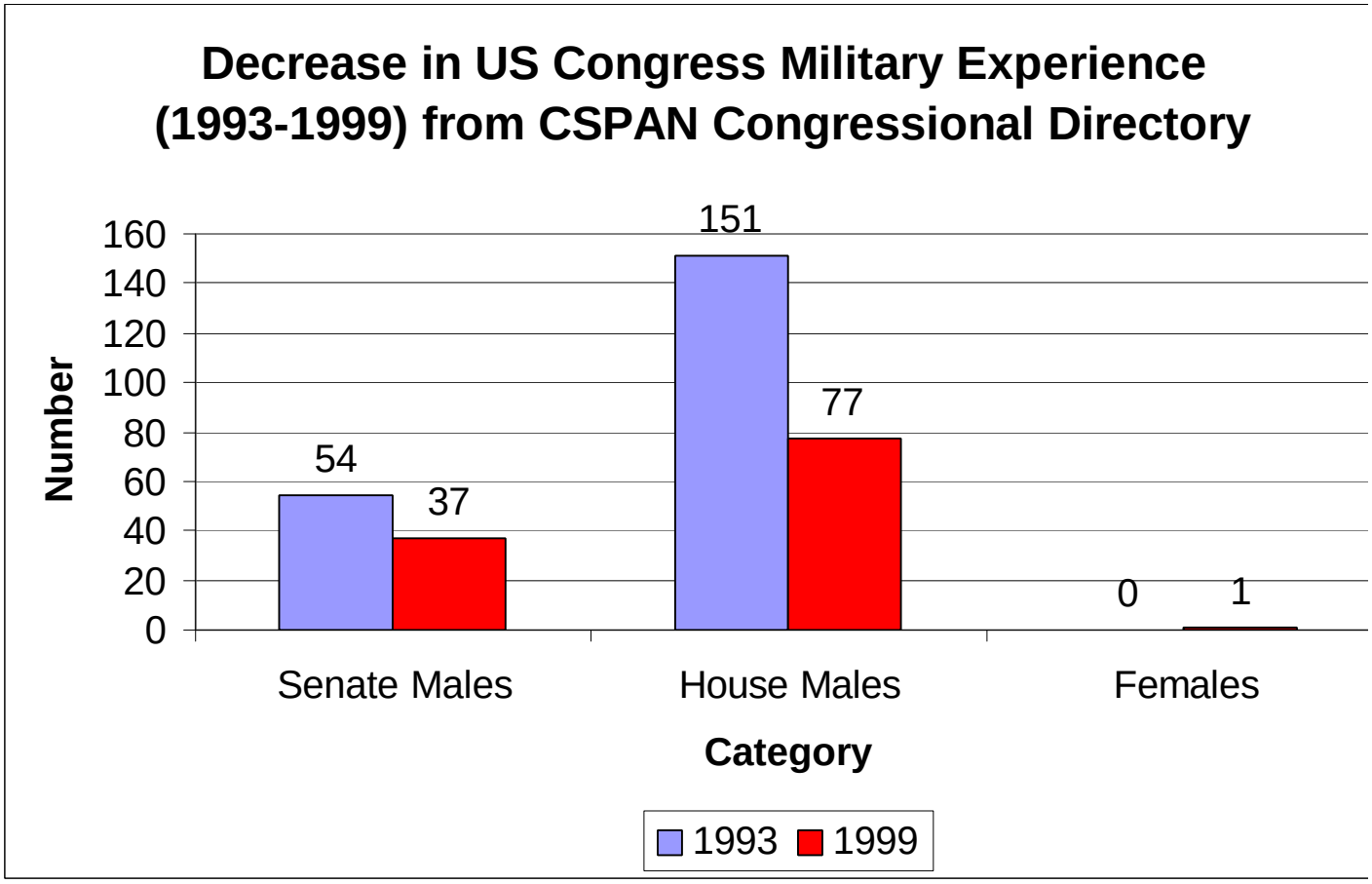

Decrease in US Congress Military Experience
(1993-1999) from CSPAN Congressional Directory
Number
160
140
120
100
80
60
40
20
0
54
37
151
77
0
1
Senate Males
House Males
Females
Category
1993
1999

Figure 3

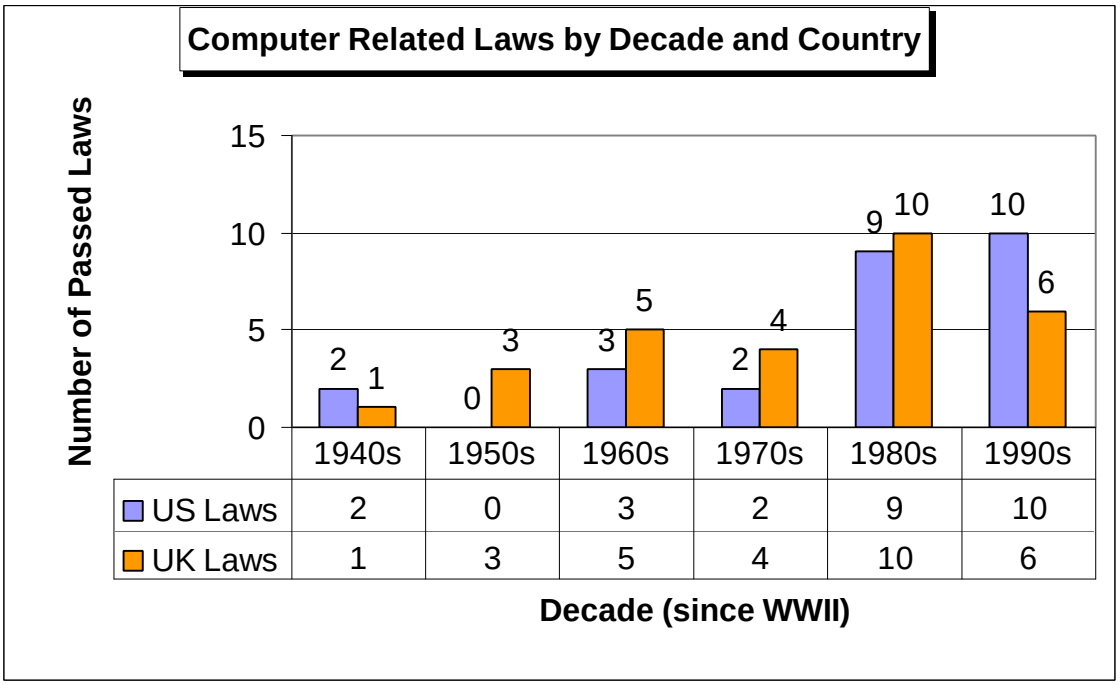

Computer Related Laws by Decade and Country
Number of Passed Laws
15
10
5
0
2
1
0
3
3
5
2
4
9
10
10
6
1940s
1950s
1960s
1970s
1980s
1990s
US Laws 2 0 3 2 9 10
UK Laws 1 3 5 4 10 6
Decade (since WWII)

Figure 4

OMB Circulars Related to Computer Security and Management

	Publication Name	Description
1.	OMB Circular A-76	Requires DOD and other agencies to compete all computer work before sole sourcing
2.	OMB Circular A-109	Major DOD Systems Management
3.	OMB Circular A-127	Financial Management and Systems
4.	OMB Circular A-130	Information Resources Management Guidelines

Source: Whitehouse Website (www.whitehouse,gov/omb) – September 2000

Figure 5

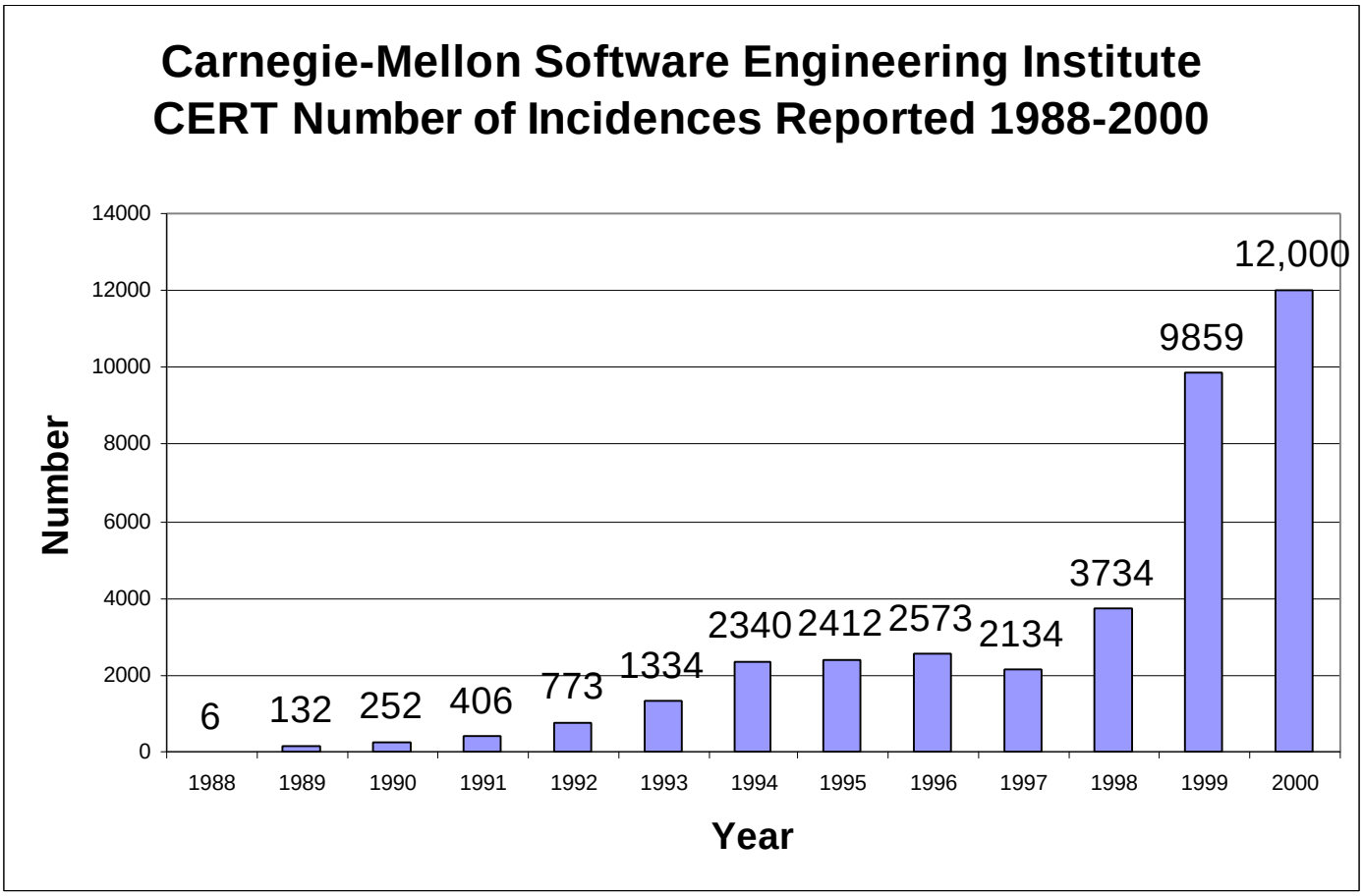

Carnegie-Mellon Software Engineering Institute
CERT Number of Incidences Reported 1988-2000
Number
Year
14000
12000
10000
8000
6000
4000
2000
0
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
6
132
252
406
773
1334
2340
2412
2573
2134
3734
9859
12,000

Figure 6

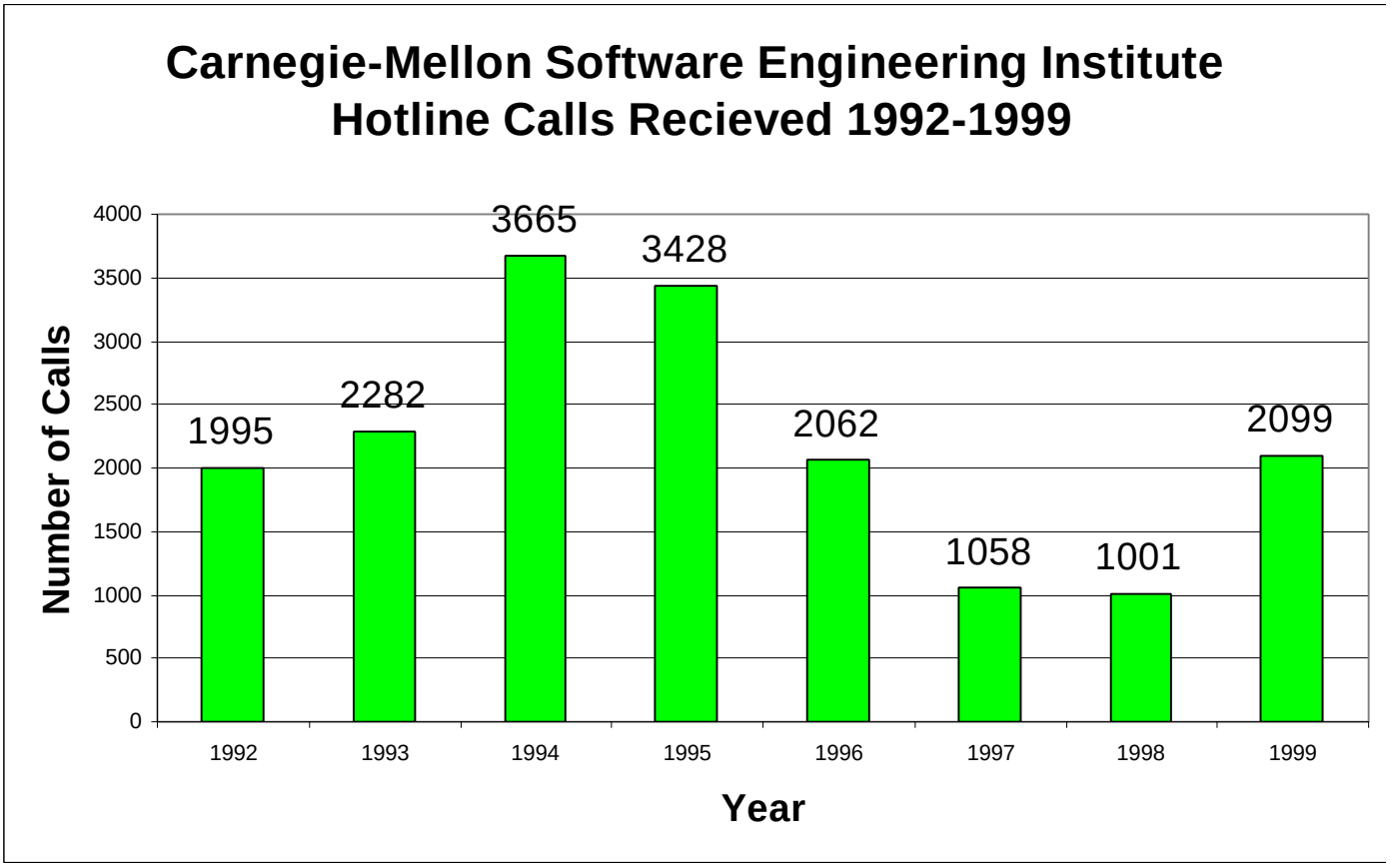

Carnegie-Mellon Software Engineering Institute
Hotline Calls Recieved 1992-1999
Number of Calls
4000
3500
3000
2500
2000
1500
1000
500
0
1995
2282
3665
3428
2062
1058
1001
2099
1992
1993
1994
1995
1996
1997
1998
1999
Year

Figure 7

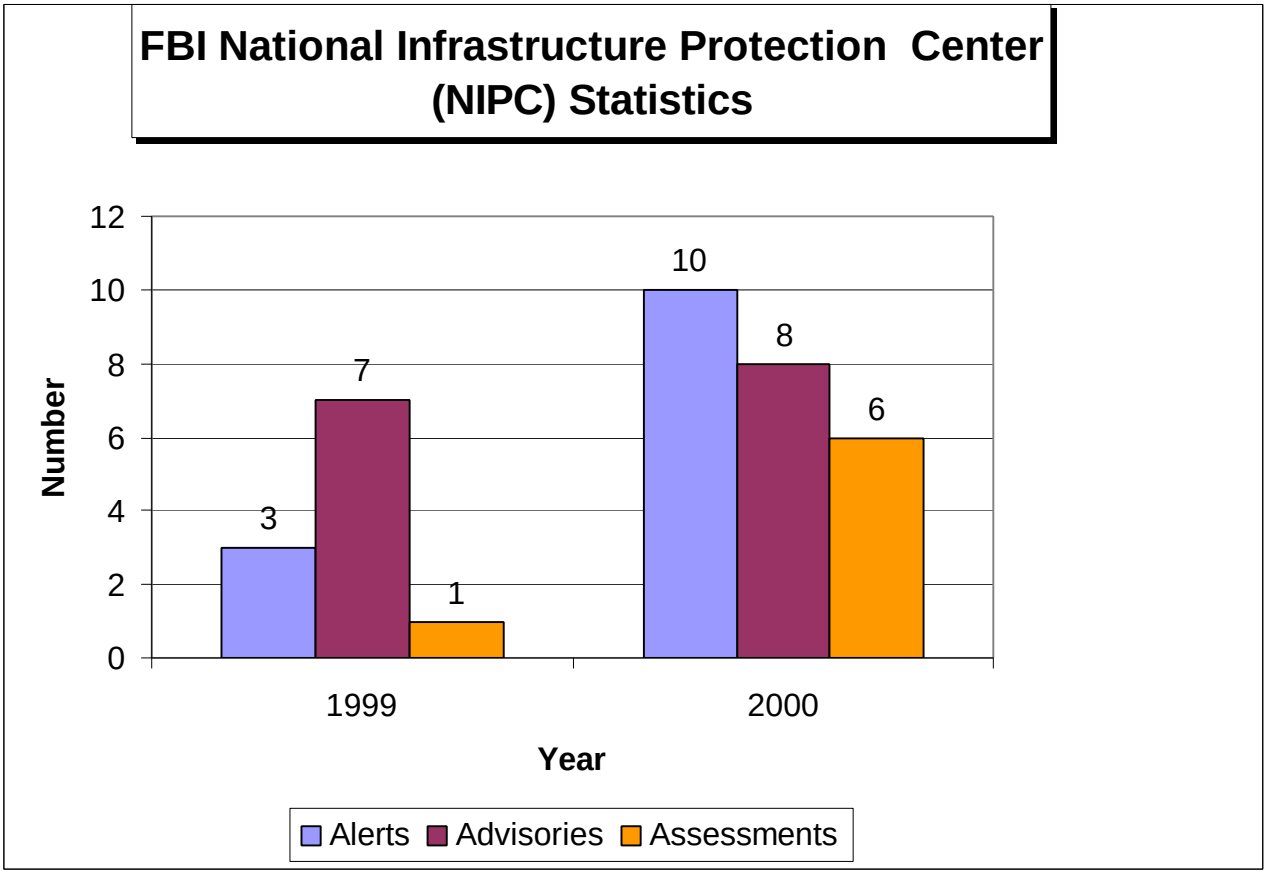

FBI National Infrastructure Protection Center (NIPC) Statistics
Number
12
10
8
6
4
2
0
3
7
1
10
8
6
1999
2000
Year
Alerts
Advisories
Assessments

Figure 8

Top 10 Management Information Systems

Educational Programs in the United States with a PhD

School Name	Location
1. MIT (Sloan School)	Massachusetts
2. Carnegie Mellon University	Pennsylvania
3. University of Minnesota	Minnesota
4. University of Texas (Austin)	Texas
5. University of Arizona (Eller)	Arizona
6. University of Pennsylvania (Wharton)	Pennsylvania
7. New York University (Stern)	New York
8. University of Maryland (Smith School)	Maryland
9. Indiana University - Bloomington (Kelley)	Indiana
10. University of California Berkley (Haas)	California

Source: US News and World Report, 2000

Figure 9

Top 10 Electrical/Communications Engineering

Educational Programs in the United States without a PhD

	School Name	Location
1.	Rose-Hulman Institute of Technology	Indiana
2.	Harvey Mudd College	California
3.	Cal Poly – San Luis	California
4.	Cooper Union	New York
5.	Rochester Institute of Technology	New York
6.	United States Air Force Academy	Colorado
7.	United States Naval Academy	Maryland
8.	Bucknell University	Pennsylvania
9.	Kettering University	Michigan
10.	United States Military Academy	New York

Source: US News and World Report, 2000

Figure 10

Top 10 Federal Government IT Contractors

	IT Contractor	Est. Annual Business
1.	Lockheed-Martin Corporation	$1.942 Billion
2.	Raytheon	$1.934 Billion
3.	Northrop Grumman Corporation	$1.197 Billion
4.	Computer Sciences Corporation	$1.079 Billion
5.	General Dynamics Corporation	$ .996 Billion
6.	Science Applications International Corp.	$ .678 Billion
7.	AT & T	$ .671 Billion
8.	TRW Incorporated	$ .627 Billion
9.	Unisys Corporation	$ .613 Billion
10.	Electronic Data Systems Corporation	$ .568 Billion

Source: Government Executive Magazine, Procurement Review, 2000

Figure 11

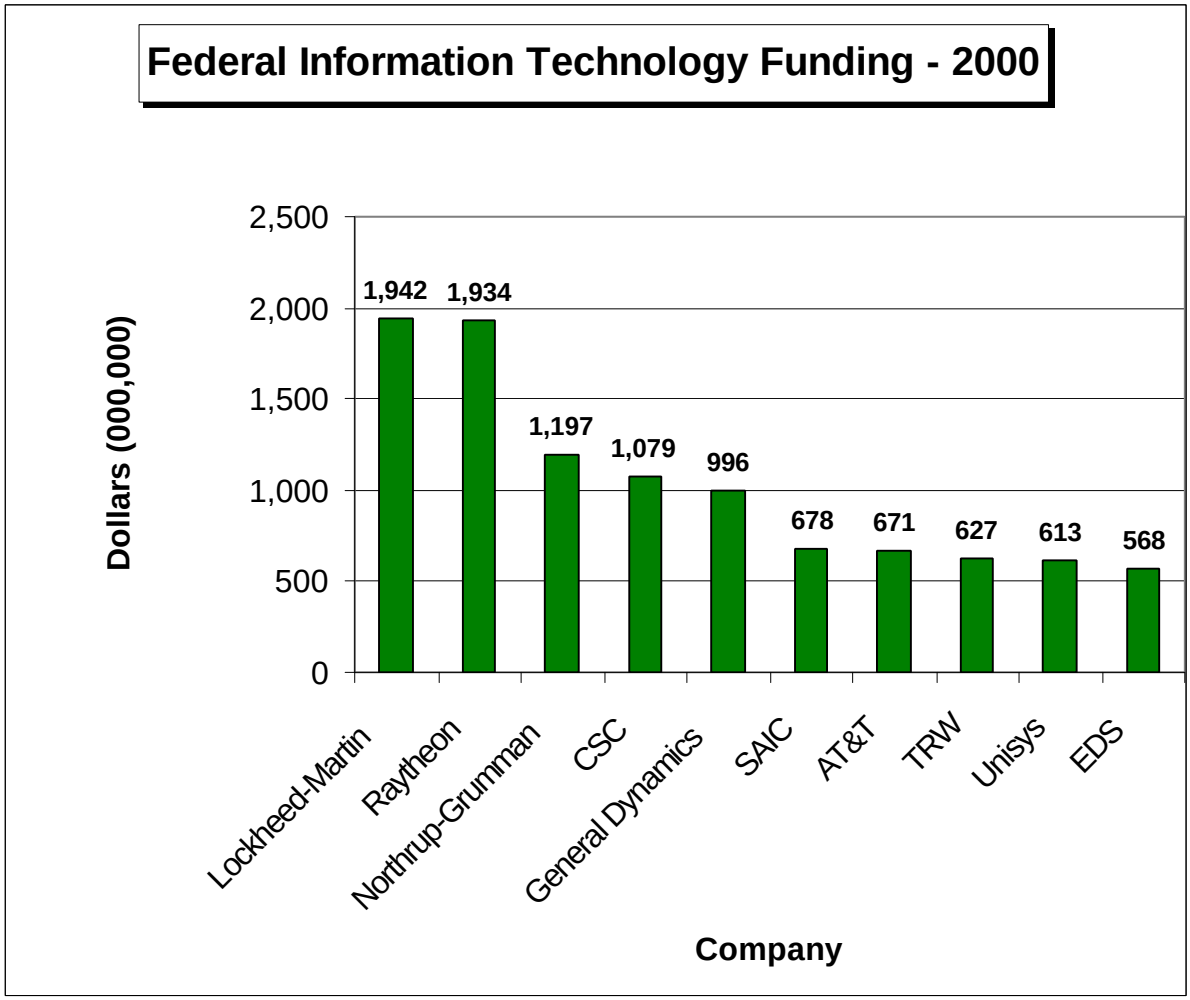

Federal Information Technology Funding - 2000
Dollars (000,000)
2,500
2,000
1,500
1,000
500
0
1,942
1,934
1,197
1,079
996
678
671
627
613
568
Lockheed-Martin
Raytheon
Northrup-Grumman
CSC
General Dynamics
SAIC
AT&T
TRW
Unisys
EDS
Company

Figure 12

Top Congressionally Funded Embedded Computer

Weapons Systems under new Pilot Contracts

For Maintenance of Production Systems

	System Name	Service
1.	M-1 Abrams Tank	Army
2.	AH-64 Apache Helicopter	Army
3.	RAH-66 Comanche Helicopter	Army
4.	CH-47 Chinook Helicopter	Army
5.	Crusader Artillery System	Army
6.	Fire Support Command and Control	Army
7.	Guardrail Common Sensor	Army
8.	High Mobility Artillery Rocket System	Army
9.	H-60 Multi-mission Helicopter	Navy
10.	EA-6B Prowler Aircraft	Navy
11.	Standoff Land Attack Missile (SLAM)	Navy
12.	Advanced Amphibious Assault Ship	Navy
13.	CG-47 Class Cruiser (Aegis – Smart Ship)	Navy
14.	Airborne Warning and Control System	Air Force

15.	Cheyenne Mountain Complex C2 Upgrade	Air Force
16.	F-16 Fighting Falcon	Air Force
17.	C-17 GlobeMaster III	Air Force
18.	Joint Surveillance and Target Attack Radar System (JSTARS)	Air Force
19.	B-1 Lancer Bomber	Air Force
20.	F-117A Nighthawk	Air Force
21.	C/KC 135 Stratolifter/Stratotanker	Air Force
22.	Space Based Infrared System	Air Force

Note: 60 Billion dollars annually is spent to maintain these systems and others not listed above. DOD hopes to save system maintenance dollars under new pilot contracts with risks shifted to contractors for performance.

Source: “Roadblock” Article in Government Executive Magazine, September 2000.

Figure 13

Top 10 Federal Government Computer Hardware Contractors

	Contractor	Est. Annual Business
1.	Dell Corporation	$347 Million
2.	Unisys Corporation	$321 Million
3.	Lockheed-Martin Corporation	$312 Million
4.	IBM Corporation	$308 Million
5.	General Dynamics Corporation	$280 Million
6.	GTSI	$237 Million
7.	Litton Industries	$231 Million
8.	Electronic Data Systems Corporation	$209 Million
9.	Carlyle Group	$199 Million
10.	Compaq Computer Corporation	$172 Million

Source: Government Executive Magazine, Procurement Review, 2000

Figure 14

Top 10 Federal Government Computer Service and Software Contractors

	Contractor	Est. Annual Business
1.	Lockheed-Martin	$1.204 Billion
2.	Computer Services Corporation	$1.025 Billion
3.	Science Applications International Corp.	$657 Million
4.	Unisys Corporation	$524 Million
5.	Electronic Data Systems Corporation	$497 Million
6.	Northrop Grumman Corporation	$480 Million
7.	Raytheon Corporation	$448 Million
8.	TRW Incorporated	$372 Million
9.	IBM Corporation	$351 Million
10.	General Dynamic Corporation	$334 Million

Source: Government Executive Magazine, Procurement Review, 2000

Figure 15

Top 10 Federal Government Telecommunications Contractors

	Contractor	Est. Annual Business
1.	Raytheon Corporation	$1.671 Billion
2.	Northrop Grumman Corporation	$843 Million
3.	Lockheed Martin Corporation	$773 Million
4.	AT&T	$661 Million
5.	General Dynamics Corporation	$548 Million
6.	Motorola Incorporated	$323 Million
7.	Bell Atlantic Corporation	$279 Million
8.	Boeing Corporation	$254 Million
9.	TRW Incorporated	$220 Million
10.	Litton Industries Incorporated	$214 Million

Source: Government Executive Magazine, Procurement Review, 2000

Figure 16

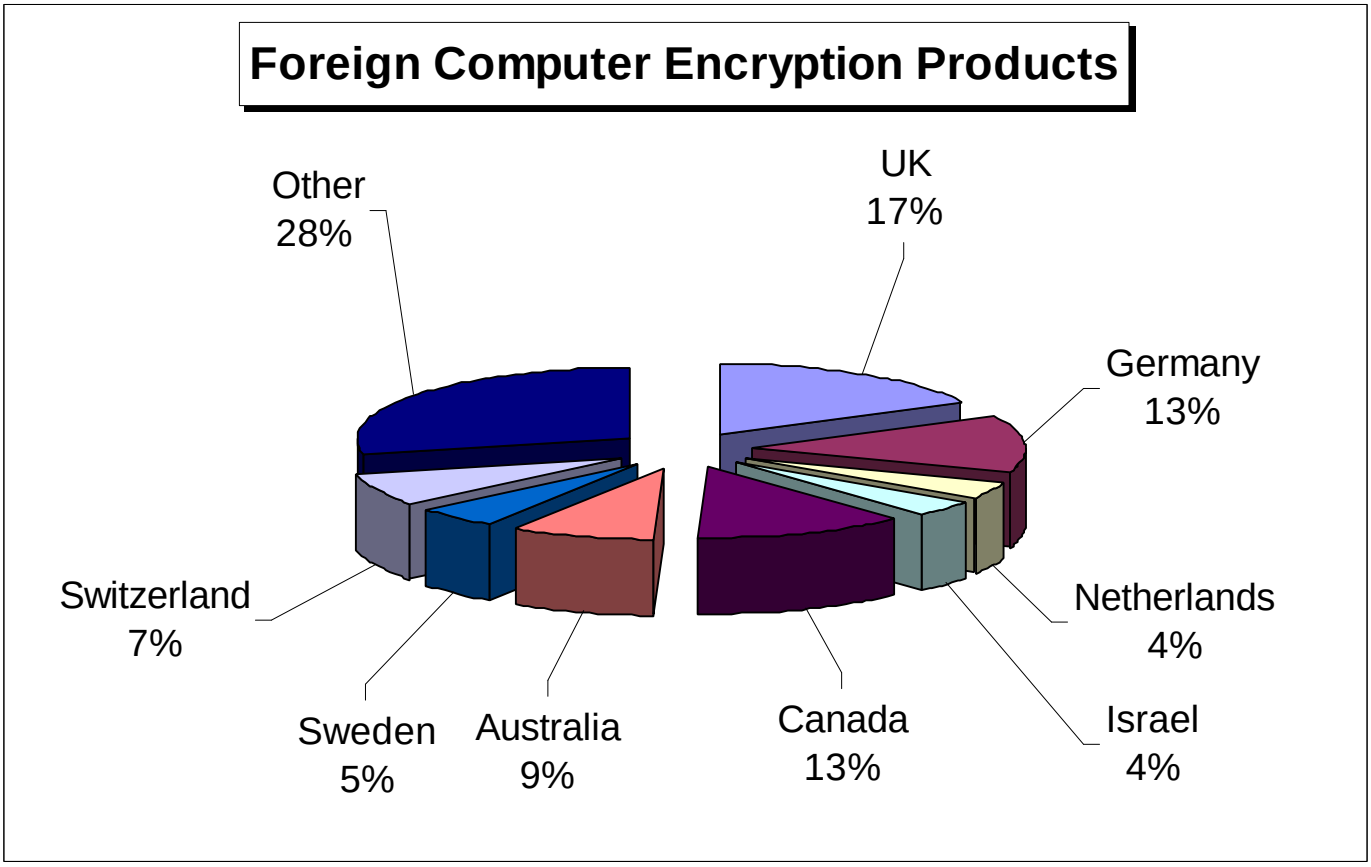
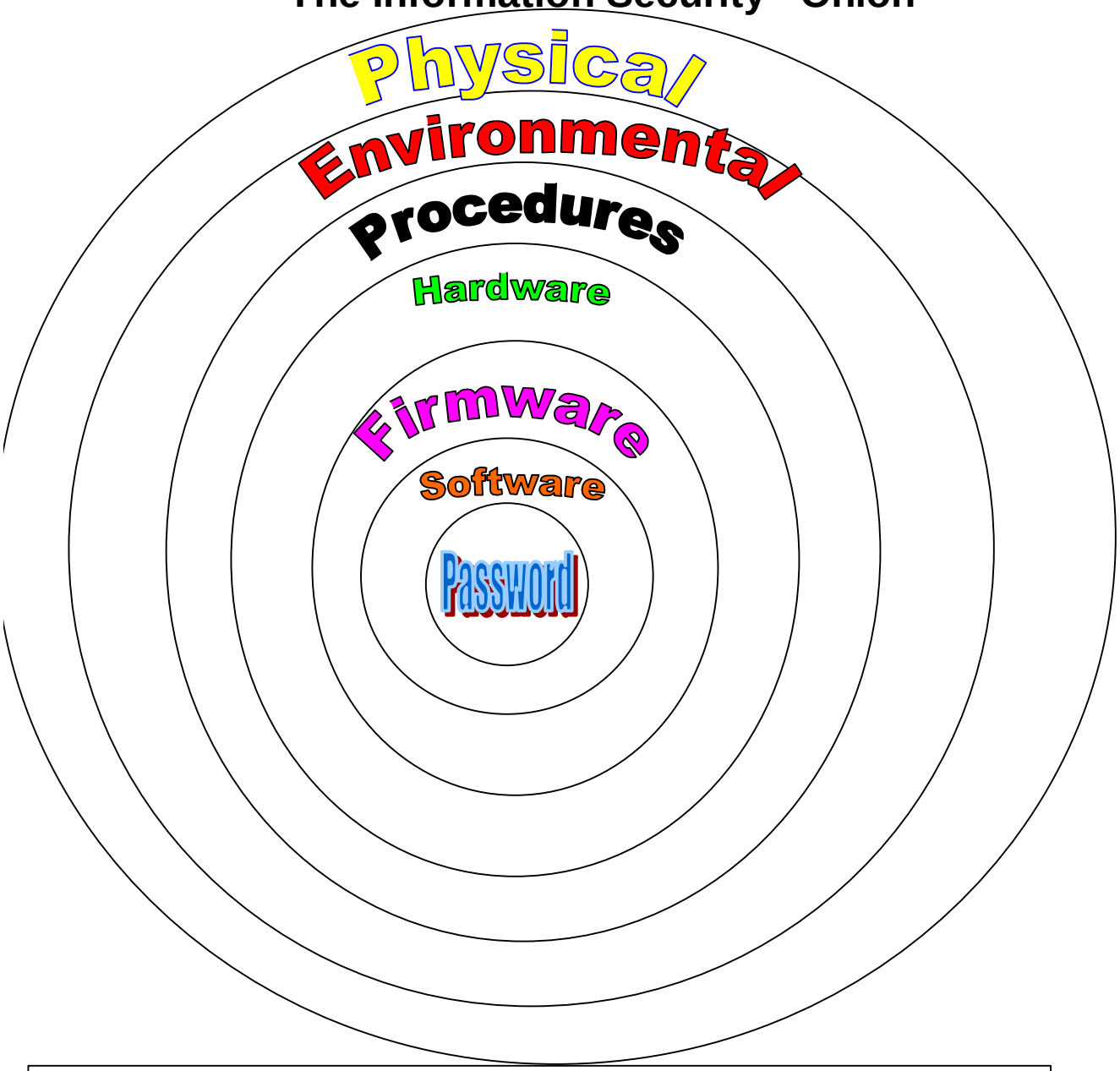

Foreign Computer Encryption Products
Other
28%
UK
17%
Germany
13%
Switzerland
7%
Netherlands
4%
Sweden
5%
Australia
9%
Canada
13%
Israel
4%

Figure 17

The Information Security "Onion"



Note: Adapted from James Martin book "Computer Security and Privacy", 1984. Applied with modification to 9 layers adding Legislative and Political layers to the outermost layers here.

Figure 18

Redundant Processors and Backup DB

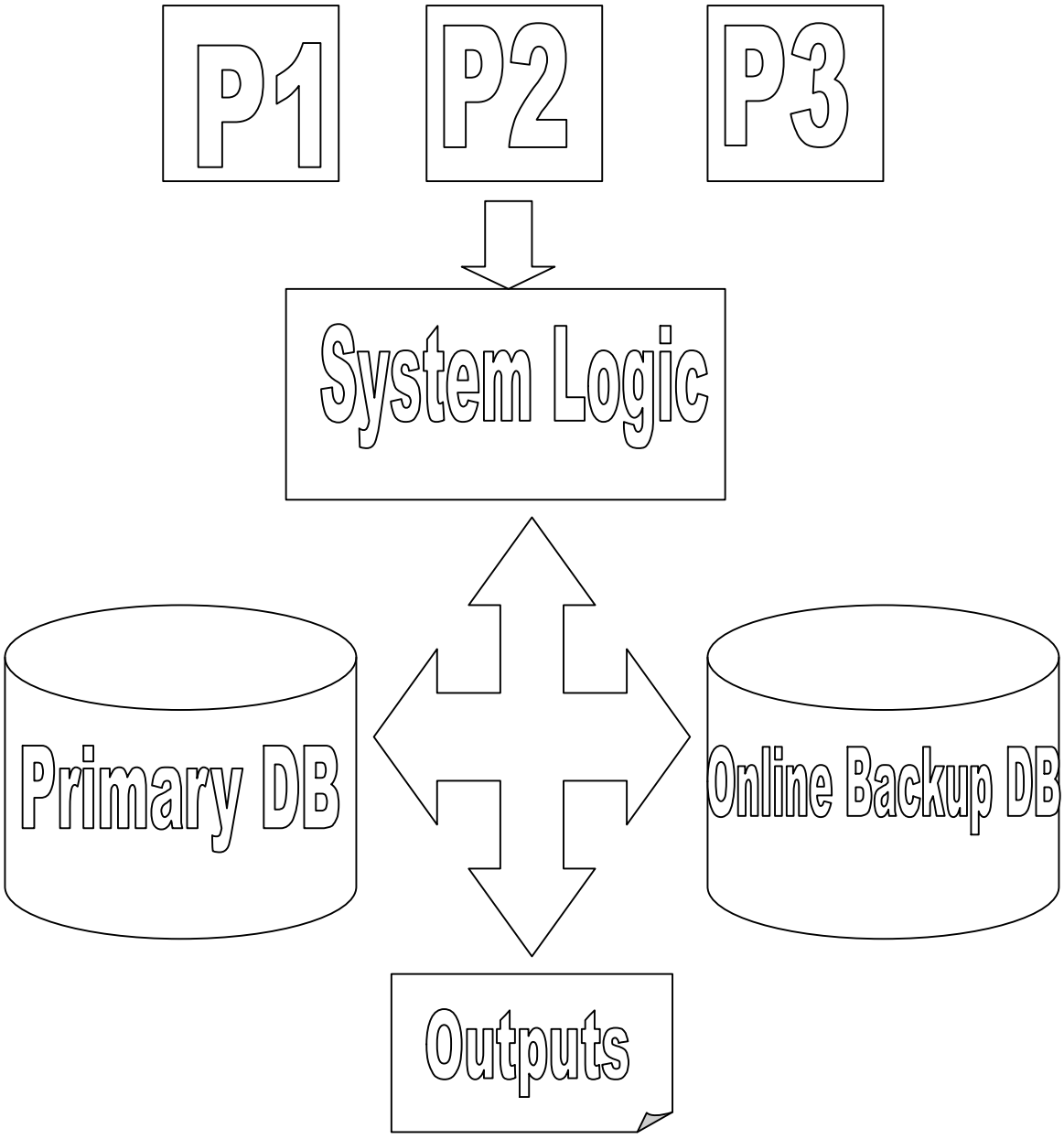


Figure 19

The DES Algorithm

```
type block = array[1…64] of 0….1                    {64 bit vector}
        ordering = array[1…64] of 1…64              {defines transposition}

var InitialTr, FinalTr, swap, KeyTr1, KeyTr2, etr, ptr: ordering
        s: array[1…8, 1…64] of 0…15;
        rots: array[1..16] of 1...2;

procedure transpose (var data: block; t: ordering; n: integer);
var x: block; i: 1…64
begin x:= data; for I:= 1 to n do data [I] := x[t[I]] end;  {transpose}

procedure rotate (var key: block);      {1 bit left rotate on two 28 bit units}
var i:1…55;  x: block;
begin x:= key;
      for i:= 1 to 55 do x[i] := x[i+1];
        x[28] := key[1]; x[56]:= key[29];  key:= x
end;    {rotate}

procedure f(i: integer; var key a, x: block);
var e, ikey, y, block;  r:0…64; k: 1….8;  j: 1…48;
begin e:= a;
       transpose (e, etr, 48);                  {expand e to 48 bits}
     for j:= 1 to rots [I]  do rotate (key);
       ikey:= key; transpose (ikey, KeyTr2, 48);
     for j:= 1 to 48 do if e[j]+ikey[j]=1 then y[I]:= 1 else y[j]:= 0;
     for k:= 1 to 8 do                          {substitute part}
          begin r:=32*y[6*k-5]+ 16*y[6*k] + 8*y[6*k-4]+4*y[6*k-3] +
                2*y[6*k-2] + y(6*k-1] + 1;
            if odd(s[k,r] div 8) then x[4*k-3]:= 1 else x[4*k-3]:=0;
            if odd(s[k,r] div 4) then x[4*k-2]:= 1 else x[4*k-2]:=0;
            if odd(s[k,r] div 2) then x[4*k-1}:=1 else x[ 4*k-1]:=0;
            if odd(s[k,r]) then x[4*k]:= 1 else x[4*k]:= 0
          end;
     transpose (x, ptr, 32)
end; {f}

procedure des(plaintext, key: block; var ciphertext: block);
var I:1…16;  j: 1…32;  a,b,x: block;
begin  a:=plaintext                     {copy plaintext to a}
   transpose (a, InitialTr, 64);        {Initial Transposition}
   transpose (key, KeyTr, 56);          {mix up key and reduce to 56 bits}
for I := 1 to 16 do                     {here come 16 iterations}
    begin b:= a;                        {a contains current ciphertext}
```

```
        for j:=1 to 32 do a[j] := b [j + 32];  {current left taken from old right}
            f(I, key, a, x);                    {compute x=f(r[I-1], k[I])}
          for j:= 1 to 32 do if b[j] + x[j]=1 then a[j+32]:=1 else a[j+32] :=0;
      end;
      transpose (a, swap, 64);              {swap left and right halves}
      transpose (a, FinalTr, 64);           {final transposition}
     ciphertext := a;
end: {des}
```

Source: Tanenbaum, (1984, p. 398)

Figure 20

List of Encryption Algorithms

1. DES (Data Encryption Standard) 64 bit Algorithm
2. RSA Algorithm (named for founders)
3. Escrowed Encryption Standard (EES)
4. PGP (Pretty Good Protection)
5. PKI (Public Key Authentication)
6. Skipjack Algorithm (Clipper Chip)

Note: NIST conducts new algorithm contests to replace older algorithms.

Figure 21

SANS Institute Top 10 Most Critical Internet Security Threats

1. BIND weaknesses: nxt, qinv and in.named allow immediate root compromise.

2. Vulnerable CGI programs and application extensions (e.g. ColdFusion) installed on web servers.

3. Remote Procedure Call (RPC) weaknesses in rpc.ttdbserverd (ToolTalk), rpc.cmsd (Calendar Manager), and rpc.statd that allow immediate root compromise.

4. RDS security hole in the Microsoft Internet Information Server (IIS).

5. Sendmail and MIME buffer overflows as well as pipe attacks that allow immediate root compromise.

6. Sadmin and mountd

7. Global file sharing and inappropriate information sharing via NetBIOS and Windows NT ports 135-139 (445 in Windows 2000), or UNIX NFS exports on port 2049, or MacIntosh Web Sharing or AppleShare/IP on ports 80,427,and 548.

8. Userids, especially root/administrator with no passwords or weak passwords.

9. IMAP and POP buffer overflow vulnerabilities or incorrect configuration.

10. Default SNMP community strings set to ‘public’ and ‘private’.

Source: SANS Institute – How to eliminate the Ten Most Critical Internet Security Threats, 17 November, 2000.

Figure 22

SANS Institute Top 7 Senior Management Mistakes

1. Assigning untrained people to maintain security and providing neither the training nor the time to make it possible to learn and do the job.

2. Failing to understand the relationship of information security to the business problem – they understand physical security but do not see the consequences of poor information security.

3. Failing to deal with the operational aspects of security: making few fixes and then not allowing the follow through necessary to ensure the problems stay fixed.

4. Relying primarily on the firewall.

5. Failing to realize how much money their information and organizational reputations are worth.

6. Authorizing reactive, short term fixes so problems re-emerge rapidly.

7. Pretending the problem will go away if they ignore it.

Figure 23

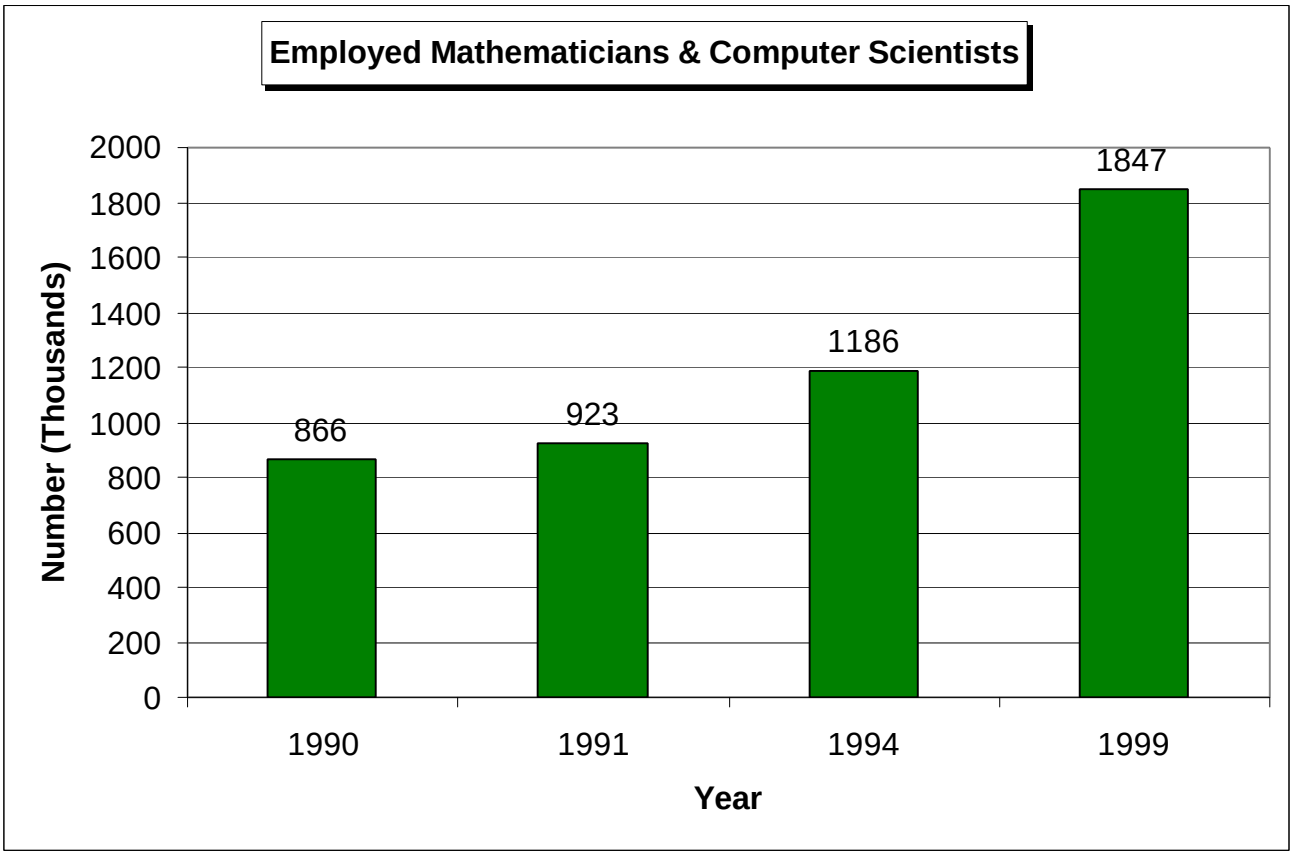

Employed Mathematicians & Computer Scientists
Number (Thousands)
2000
1800
1600
1400
1200
1000
800
600
400
200
0
866
923
1186
1847
1990
1991
1994
1999
Year

Figure 24

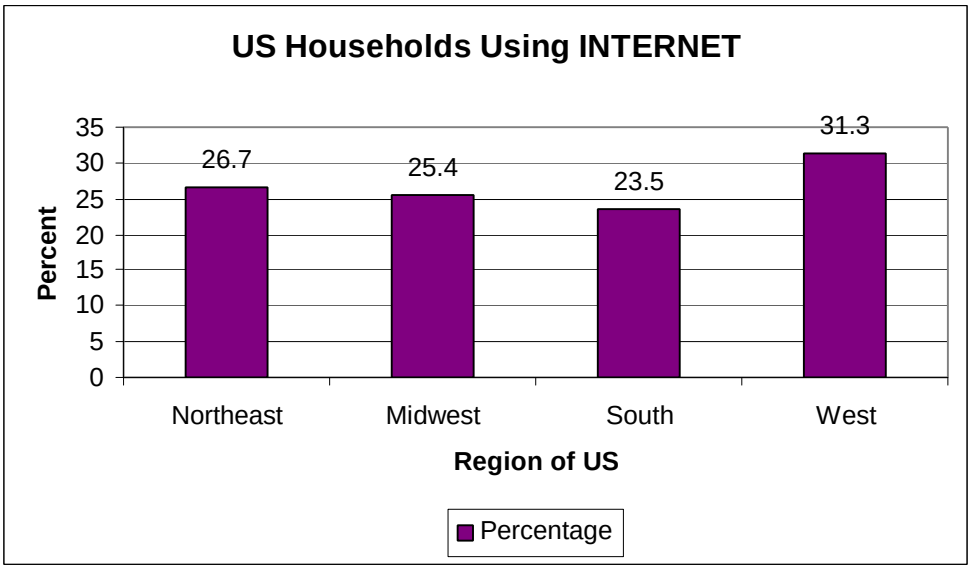

US Households Using INTERNET
Percent
35
30
25
20
15
10
5
0
26.7
25.4
23.5
31.3
Northeast
Midwest
South
West
Region of US
Percentage

Figure 25

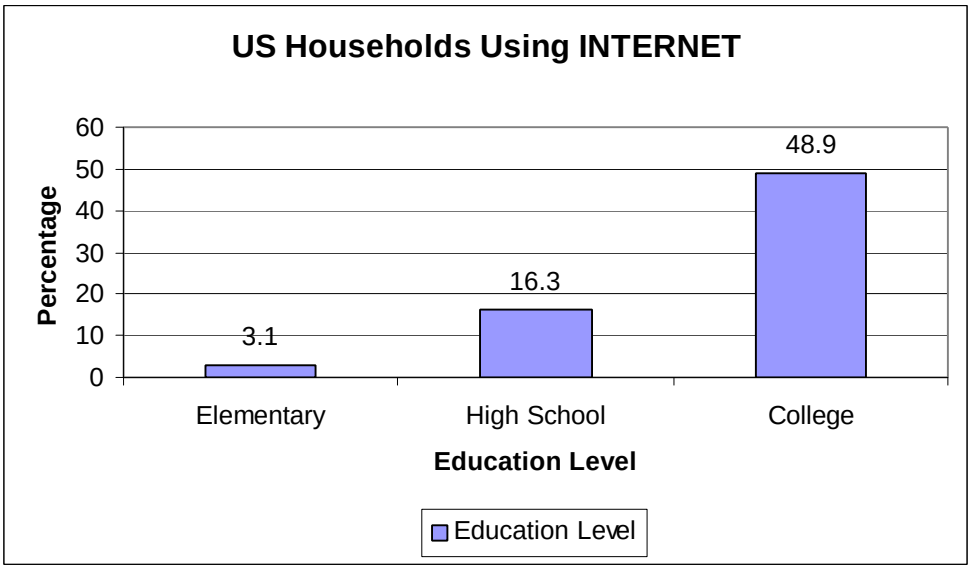

US Households Using INTERNET
Percentage
60
50
40
30
20
10
0
3.1
16.3
48.9
Elementary
High School
College
Education Level
Education Level

Figure 26

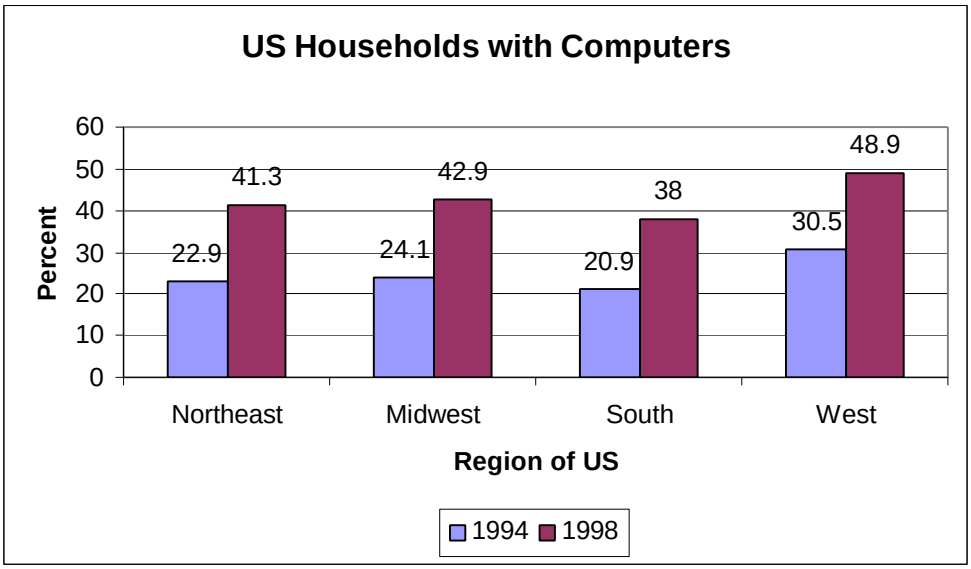

US Households with Computers
Percent
60
50
40
30
20
10
0
22.9
41.3
24.1
42.9
20.9
38
30.5
48.9
Northeast
Midwest
South
West
Region of US
1994
1998

Figure 27

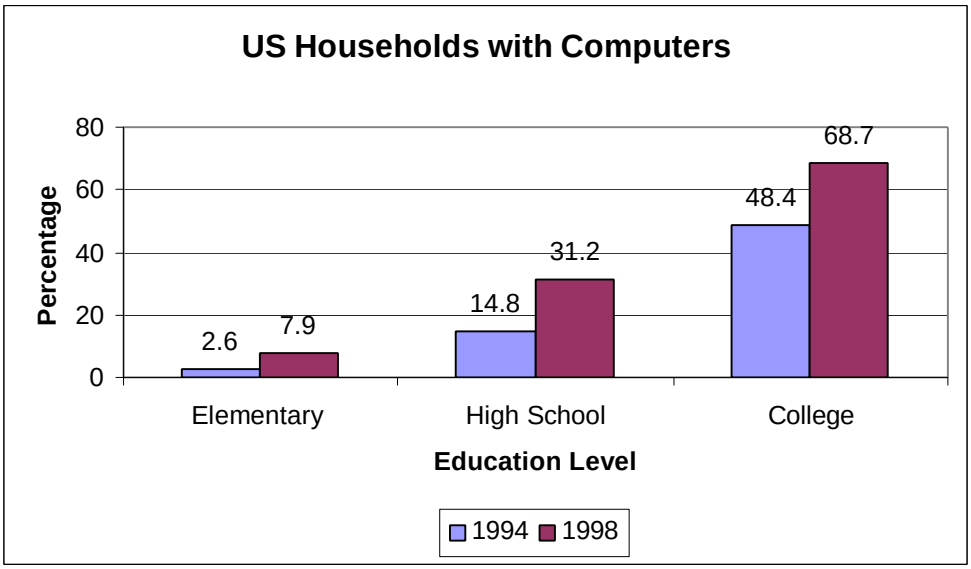
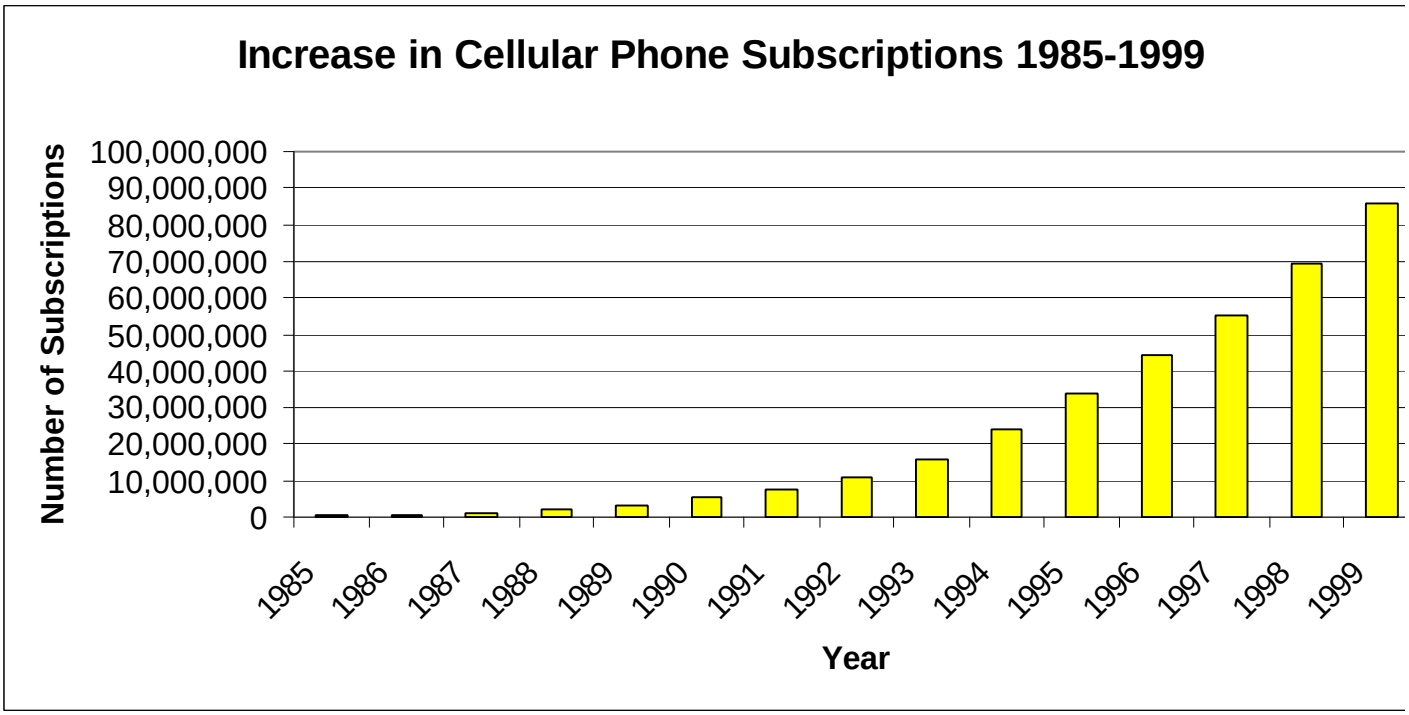

US Households with Computers
Percentage
80
60
40
20
0
2.6
7.9
14.8
31.2
48.4
68.7
Elementary
High School
College
Education Level
1994
1998

Figure 28


Increase in Cellular Phone Subscriptions 1985-1999
Number of Subscriptions
100,000,000
90,000,000
80,000,000
70,000,000
60,000,000
50,000,000
40,000,000
30,000,000
20,000,000
10,000,000
0
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
Year

References

Books

[ACM, 2000] ACM, Intellectual Property in the Age of Universal Access, ACM Press, 2000.

[Bainbridge, 1996] Bainbridge, David, Introduction to Computer Law, Pittman Publishing, 1996.

[Barrack, 1988] Barrack, Martin K., How We Communicate: The Most Vital Skill, Glenbridge Publishing Ltd., 1988.

[Bauer, 1997] Bauer, F.L., Decrypted Secrets: Methods and Maxims of Cryptology, Springer, 1997.

[Bittman, 1985] Bittman, Ladislav, The KGB and Soviet Disinformation: An Insider's View, Pergamon-Brassey's, 1985.

[Bloomer, 1992] Bloomer, John, Power Programming with RPC, O'Reilly & Associates, Inc., 1992.

[Buchannan, 1992] Buchannan, William, Virus, Random House, 1992.

[Bushkin, 1976] Bushkin, A.A. and Schaen, S.I., The Privacy Act of 1974: A Reference Manual for Compliance, System Development Corporation, 1976.

[Campen, 1998] Campen, Alan and Dearth, Douglas, Cyberwar 2.0: Myths, Mysteries, and Reality, AFCEA International Press, 1998.

[Chiarella, 1992] Chiarella, Donald and Oleynick, Nicholas , Prototyping in NATURAL II, WH&O Press, 1992.

[Clawson, 1994] Clawson, Patrick, Iran's Strategic Intentions and Capabilities, Institute for National Strategic Studies, National Defense University, 1994.

[Coulouris, 1994] Coulouris, Dollimore, & Kindberg, Distributed Systems: Concepts and Design, Addison-Wesley, 1994.

[Date, 1995] Date, Chris J., The Systems Programming Series: An Introduction to Database Systems, Addison-Wesley, 1995.

[Deitel, 1984] Deitel, Harvey M., An Introduction to Operating Systems: Including Case Studies in: UNIX, VAX, CP/M, MVS, VM, ADA, Addison -Wesley, 1984.

[NSA, 1985] DOD Std 5200.28, Department of Defense Trusted Computer System Evaluation Criteria, NSA - NCSC , December 1985.

[Graf, 1995] Graf, Rudolf F., & Sheets, William, Encyclopedia of Electronic Circuits, Volume 5, McGraw-Hill, 1995.

[Kahn, 1968] Kahn, David, The Codebreakers: The Story of Secret Writing, The MacMillan Company, 1968.

[Klevinsky, 2000] Klevinsky, T.J. and Scambray, Joel, Contemporary Hacking Tools and Penetration Testing, Ernst & Young, 2000.

[Lindeburg, 1998] Lindeburg, Michael, Engineer-in-Training Reference Manual, 8th Edition, Professional Publications, 1998.

[Loney, 1998] Loney, Kevin, ORACLE 8 DBA Handbook, Oracle Press, 1998.

[Luger, 1998] Luger & Stubblefield, Artificial Intelligence, Addison Wesley Longman, 1998.

[Lusk, 1978] Lusk, Hewitt, Donnell, and Barnes, Business Law: Principles and Cases, Fourth UCC Edition, Irwin, 1978.

[Martin, 1988] Martin, James, and Oxman, Steven, Building Expert Systems: A Tutorial, Prentice-Hall, 1988.

[Martin, 1989] Martin, James; Chapman, Kathleen, and Leben, Joe, DB2: Concepts, Design, and Programming, Prentice-Hall, 1989.

[Martin, 1970] Martin, James and Norman, Adrian, The Computerized Society, Prentice-Hall, 1970.

[Martin, 1986] Martin, James, The Information Manifesto, Prentice-Hall, 1986.

[Martin, 1983] Martin, James, Managing the Data-Base Environment, Prentice-Hall,1983.

[Martin, 1984] Martin, James, Security, Accuracy, and Privacy in Computer Systems, Prentice-Hall, 1984.

[McChristian, 1974] McChristian, Joseph A., Maj. Gen., Vietnam Studies: The Role of Military Intelligence 1965-1967, Department of the Army, 1974.

[Meisner, 1996] Meisner, Maurice, Quotations from Chairman Mao Tse-Tung, Easton Press, 1996.

[Milburn, 1998] Milburn, Gerald J., Quantum Entanglement and The Computing Revolution: The Feynman Processor, Perseus Books, 1998.

[Nagle, 1992] Nagle, James F., The History of Government Contracting, The George Washington University, 1992.

[Nash, 1993] Nash, Ralph C. Jr & Cibinic, John Jr., Competitive Negotiation: The Source Selection Process, The George Washington University, 1993.

[NSA 1991] National Computer Security Center, Trusted Database Management System Interpretation of the Trusted Computer System Evaluation Criteria, NSA-NCSC, April 1991.

[NSA, 1987J] National Computer Security Center, Trusted Network Interpretation,NSA-NCSC, July 1987.

[NSA, 1987S] National Computer Security Center, A Guide to Understanding Discretionary Access Control in Trusted Systems, NSA-NCSC, Sept 1987.

[NSA, 1988] National Computer Security Center, Glossary of Computer Security Terms, NSA-NCSC, Oct 1988.

[NIST, 2000] National Institute of Standards and Technology, Federal Information Processing Publications and Special Publications, NIST, 2000.

[Newton, 1997] Newton, David, Encyclopedia of Cryptology, ABC-CLIO, 1997.

[Northcutt, 2000] Northcutt, Stephen, SANS 2000 Coursebook: Network Intrusion Analysis, Wednesday March 22, 2000, Ninth Annual Systems Administration, Networking and Security Conference, Orlando, Florida, SANS Institute.

[Oleszek, 1989] Oleszek, Walter J., Congressional Procedures and the Policy Process, 3rd Edition, Congressional Quarterly Press, 1989.

[Pfleeger, 1989] Pfleeger, Charles P., Security in Computing, Prentice-Hall, 1989.

[Phillips, 1997] Phillips, Donald T., The Founding Fathers on Leadership: Classic Teamwork in Changing Times, Warner Books, 1997.

[Pressman, 1998] Pressman, Roger, Software Engineering Principles: A Practitioner's Approach, Prentice Hall, 1998.

[Sapronov, 1988] Sapronov, Walter, Telecommunications and the Law, Computer

Science Press, 1988.

[Strassman, 1990] Strassman, Paul A., The Business Value of Computers: An Executive's Guide, The Information Economics Press, 1990.

[Suvorov, 1984] Suvorov, Viktor, Inside Soviet Military Intelligence, MacMillan Publishing, 1984.

[Tanenbaum, 1981] Tanenbaum, Andrew S., Computer Networks, McGraw-Hill, 1981.

[Tebbs, 1977] Tebbs, David and Collins, Garfield, Real Time Systems: Management and Design, McGraw-Hill, 1977.

[WAEG, 1993] World Almanac Education Group, 1993: The World Almanac and Book of Facts, World Almanac Education Group, 1993.

[WAEG, 2001] World Almanac Education Group, 2001: The World Almanac and Book of Facts, World Almanac Education Group, 2001.

[Yourdon, 1998] Yourdon, Edward and Jennifer, Time Bomb 2000, Prentice-Hall PTR, 1998.

Articles and White Papers

[AFCEA, 2000] Armed Forces Communications an Electronics Association (AFCEA), Selected Articles, SIGNAL Magazine, AFCEA International Press, 2000.

[ACM, 2000] Association of Computing Machinery (ACM), Selected Articles in Communications of the ACM Magazine, ACM Press, Jan-August 2000.

[Cebrowski, 1998] Cebrowski, Admiral and Garstka, John J.; "Network-Centric Warfare: Its Origins and Future", in Naval Institute Proceedings,

1998.

[Chiarella, 1999] Chiarella, Donald, “Computer Security Undergraduate Course Syllabus,
”University of Maryland University College, 1999.

[Chiarella, 1991] Chiarella, Donald, General Services Administration Federal Information Resources Management Regulation Bulletin C-27, “Obsolete ADP Equipment”, GSA, 1991.

[Chiarella, 2000] Chiarella, Donald, “Office of Traffic and Safety (OOTS) Strategic IT Plan”, Maryland Department of Transportation, 2000.

[Chiarella, 1997] Chiarella, Donald, “TSAD Annual IT Contingency Plan”, Maryland Department of Transportation, 1997-2000.

[DOD, 2000] Department of Defense, Selected Articles in Crosstalk Magazine: The Journal of Defense Software Engineering, Hill AFB Utah, 2000.

[Hancock, 1999] Hancock, William, Embedded Firewalls: Defending Windows NT Servers from Network Attacks: A Security White Paper, Network – 1 Security Solutions, Inc., 1999.

[Hekimian, 2000] Hekimian, Chris, “Encrypted Denial of Service Attack Tool,” The George Washington University Cyberspace Policy Institute, September, 2000.

[Hekimian, 2000S] Hekimian, Chris, “Handbook for Cyber Snoops”, The George Washington University Cyberspace Policy Institute, September, 2000.

[McAfee, 1996] McAfee Associates Inc., “Current Computer Virus Threats, Countermeasures and Strategic Solutions,” White Paper, 1996.

[McAfee, 1996] McAfee Associates Inc., “Customer Case Study: Lyondell Petrochemical,” White Paper, 1996.

[McAfee, 1995] McAfee Associates Inc., "Evaluating Anti-Virus Solutions Within Distributed Environments," White Paper, 1995.

[McAfee, 1997] McAfee Associates Inc., "Protecting Networks and PCs from Hostile Java and ActiveX Applications: A White Paper on New Trends in Internet and Intranet Security", McAfee, 1997.

[NIST, 2000] NIST and NSA, "The Biometric Consortium 2000 Conference" Proceedings, NIST and NSA, September 13-14, 2000

[McAfee, 2000] Network Associates, "Anti-Virus Software Distribution: Managing the Distribution of Anti-Virus Upgrades and Updates Across the Enterprise", McAfee White Paper, 2000.

[Richelson, 1999] Richelson, Jeffrey T., "U.S. Satellite Imagery, 1960-69", in National Security Archive Electronic Briefing Book No. 13, George Washington University website, February 26, 2001

[Richelson, 2000] Richelson, Jeffry T., "The NRO Declassified," in National Security Archive Electronic Briefing Book No. 35, George Washington University website, February 26, 2001.

[Stein, 2000] Stein, Fred P., "Observations on the Emergence of Network Centric Warfare", on DOD CCRP website, 27 February 2001.

[Tenet, 2001] Tenet, George J., Statement to Senate Select Committee on Intelligence: "Worldwide Threat 2001: National Security in A Changing World", CIA website, 2001.

[USNI, 2000] Proceedings Magazine, Navy Technology Leadership Articles and Columns, US Naval Institute Press, 2000.

[Wells, 2000] Wells, Joe, "WildList – May 2000", 2000 Virus Bulletin Ltd., 2000

Reports

[FBI, 1999] FBI Laboratory, "FBI Laboratory Annual Report 1999", U.S. Department of Justice, 1999.

[GWU,1999] GWU Report GWU-CPI-1999-02, "Growing Development of Foreign Encryption Products in the Face of U.S. Export Regulations," Cyberspace Policy Institute, The George Washington University, 1999.

[SANS, 2000] SANS Institute, "SANS Security Alert", SANS Institute, 2000.

[SEI, 2000] Software Engineering Institute, "CERT Coordination Center 1999 Annual Report (Summary)", Carnegie Mellon University, 2000.

[US GPO, 1994] US House of Representatives, "Hearings on Electronic Communications Privacy Act", GPO, 1994.

GLOSSARY OF TERMS AND ACRONYMS

Term/Acronym	Meaning
ADP / IT	Automated Data Processing / Information Technology
AFCEA	Armed Forces Communications and Electronics Association
Bacteria	Programs that replicate themselves within a computer using up memory resources
Biometrics	Personalized medical traits used in

	computerized access equipment and algorithms.
CIA	Central Intelligence Agency
Cipher Key	A key word that is applied to the cipher text to decipher it to plain text
Cipher Text	A mathematical algorithmic coded message
C.F.R	Code of Federal Regulations (i.e. Title 41 CFR, Title 48 CFR, etc)
Classified System	A computer system that requires a classified, secret, or top secret security clearance by the programmer, analyst, or operator
Clipper Chip	Computer chip containing Skipjack Algorithm that implements the Escrowed Encryption Standard
COLLOSUS	British crypto-computer in WWII
ComInt	Communications Intelligence
ComSec	Communications Security

CompSec	Computer Security
Contract	A government agreement with a private company for computer, communications, or acquisition related services
CORONA	CIA intelligence satellite program in early 1960's
Crack	To decipher a code
Cracker	A Hacker or code cracker
Cryptology	Those arts and skills associated with cryptography and cryptanalysis
DARPA	Defense Advanced Research Projects Agency
DEA	Data Encryption Algorithm
DES-64	Data Encryption Standard 64 Bits
DIA	Defense Intelligence Agency
DISA	Defense Information Systems Agency
Distributed Denial of Service	Computer routines that can tie up the communications lines by replicating and initiating handshaking
DOD	Department of Defense

DODCI	Department of Defense Computer Institute at the Washington Navy Yard
EDI	Electronic Data Interchange
EES	Escrowed Encryption Standard as discussed in FIPS-185 using Skipjack algorithm. AKA Clipper.
FBI	Federal Bureau of Investigation (Also Fidelity, Bravery, Integrity – the virtues of the FBI)
FCI	Foreign Counter Intelligence
FIP PUBS	Federal Information Processing Publications
FORTEZZA	A PMCIA card that has the Skipjack algorithm, digital signature, and key exchange functions
KGB	Internal Intelligence Agency of Soviet Union
GAO	Government Accounting Office
GII	Global Information Infrastructure
GPO	Government Printing Office
GRU	External Intelligence Agency of Soviet Union

GSA	General Service Administration
Hacker	A person who uses a computer to intentionally commit crimes
Hacktivism	Political hacking as a means of activism during or near the time of a political event as a form of protest
Handshaking	Two computers setting up a telecommunications line to communicate digitally and verifying digital identities
HUMINT	Human Intelligence
Information Warfare	Computer controlled command and control
INFOSEC	Information Security
Intellectual Property	Ideas rather than physical property
Internet	A global network of computers created by the Defense Advanced Research Projects Agency (DARPA)
Intrusion Detection	Computer software that can detect an intruder on a communications line

ISO OSI	International Standards Organization Open Systems Interconnection
IW	Information Warfare
Life Cycle	The costs, time and events required to acquire and/or build computer/communications systems and operationally deploy them.
Logic Bomb	A program that at some given time in future sets off harmful computer instructions. May be dormant for years.
Macro Virus	A computer virus that lives in email word processor documents
Masquerade	The penetrator assumes the identity of a legitimate user after having obtained the proper identification through clandestine means.
MI8	British Cryptanalysis group in WWII
MID	Military Intelligence Division
MTBF	Mean Time Between Failure
MTTR	Mean Time To Repair
NAK Attack	Negative Acknowledgement Attack

NBS	National Bureau of Standards. Name of NIST from 1901-1988.
NCSC	National Computer Security Center
NDU	National Defense University at Fort McNair, Washington DC.
Network Centric Warfare	Network controlled battlefields
NIST	National Institute of Standards and Technology
NRO	National Reconnaissance Office
NSA	National Security Agency at Fort George G. Meade, Maryland
OMB	Office of Management and Budget
Operator Spoof	A clever penetrator can often fool a computer operator into performing an action that compromises computer security
Orange Book	"DOD Trusted Computer System Evaluation Criteria" series of guidance
OSI	Open System Interconnection
PAC	Personal Authentication Code
PCMCIA	Personal Computer Memory Card

	Industry Association
PEM	Privacy Enhanced Email
Penetration Attack	The attempts by a hacker to crack into a computer network undetected.
PGP	Pretty Good Privacy
Piggybacking	The penetrator uses a special terminal to tap a communication line.
PIN	Personal Identification Number
PK	Private Key or Public Key
PKI	Public Key Infrastructure
PKCS	Public Key Cryptography Standard
P.L.	Public Law
Plain text	A message after or before the process of cipher encoding
Protocol	A communication layer in the OSI model of data communication. 7 stacked layers comprise the OSI standard communications model.
RSA algorithm	Named for Ronald Rivest, Adi Shamir,

	and Leonard Adelman (RSA). Secure public key system based on prime numbers.
SIGINT	Signal Intelligence
SIS	Signal Intelligence Service – US Army
Skipjack	Encryption algorithm developed at NSA in the 1980's. AKA Clipper.
SPB	Security Policy Board created by President Clinton on 16 September 1994 in Presidential Decision Directive 29 (PDD-29).
Trojan Horse	Harmful computer Instructions included with valid instructions. Adapted from Trojan war when Greeks gave gift horse to Trojans to obtain access to city of Troy by soldiers waiting inside the horse. (Virgil, The Illiad)
U.C.C.	Uniform Commercial Code
U.S.C.	United States Code

Virus	A program that makes copies of itself and inserts them into other computer programs.
White-collar crime	Crimes committed by professionally educated people including fraud, forgery, and computer crimes.
Worm	A replicated bacteria that infects other computers or networks.
WWW	World Wide Web – Internet network of computer nodes (addresses).

APPENDIX A

LIST OF COMPUTER RELATED LAWS

United States Laws and Acts (in Chronological Order)

Cannonball Committee of 1776 – Gave congress the right to hire companies who could supply the Continental Army with cannonballs and other supplies. This formed the basis for current day computer and communications acquisition laws. (Nagle)

Communications Act of 1934 – Made AT&T the US Carrier and called for national telephone services coast to coast. (Sapronov)

Federal Property and Administrative Services Act of 1947 – Created GSA as government agency responsible for federal property (later to include computers) (Nash & Cibinic, p 400)

National Security Act of 1949 – Created NSA and military intelligence Agencies. (Kahn)

Satellite Communications Act of 1962 – Outlined US role in Satellite Communications.

Brooks Act of 1965 – Named after Texas Senator Jack Brooks who championed the federal computer acquisition laws assigned to GSA to match the development of large mainframe computers.

Brooks Act, Warner Amendment – Named after Senator John Warner of Virginia and designed to exclude embedded computers in military weapons systems from GSA acquisition authority and under the defense agency responsible for acquisition of the specific weapons system.

Privacy Act of 1974 – Discussed Information privacy accorded to people who were recorded government systems (Buskin & Schaen)

Copyright Act of 1976 – Described the "fair use" doctrine as applied to non-profit organizational uses of information that may be copied by Xerox machines, etc. (Lusk et al, pp. 1055-6)

Paperwork Reduction Act of 1980 – Mandated paperless offices and further usage of computers to ease the paper burden on agencies.

Telecommunications Deregulation Act of 1984 – Deregulated control of AT&T as national telecom carrier to local companies and other Competition (Sapronov).

Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 - Described fraudulent access devices and computer abuses.....

Small Business Computer Security and Education Act of 1984 – To proliferate educational resources on computer security in small businesses.

Computer Fraud and Abuse Act of 1986 – Outline computer crimes and abuses on government systems. Originated with Morris vs. NSA case on computer worm that destroyed NSA telecom network.

Paperwork Reduction Reauthorization Act of 1986 – Reauthorized business use of computers in government to reduce paperwork burdens.

Federal Technology Transfer Act of 1986 – Outlined rules for technology transfer from advanced technology agencies to less advanced agencies and the private sector.

Computer Security Act of 1987 – Defined federal government computer security in agencies and gave NIST responsibility under the Commerce department for non-military systems.

Computer Matching and Privacy Protection Act Amendments of 1989 – Rules and regulations on government use of computer name matching programs.

Computer Software Rental Amendments Act of 1990 – Discussed computer software rental agreements.

Computer Matching and Privacy Protection Act Amendments of 1990 – Authorized computer matching program in the federal government.

Small Business Technology Transfer Act of 1992 – Helped to transfer technology to small businesses.

Computer Abuse Amendments Act of 1994 – Reissued computer crime act with new details.

Paperwork Reduction Reauthorization Act of 1996 – Re-authorized paperless office in the federal government as a strategy to reduce agency paper burdens.

Electronic Communications Privacy Act of 1996 - Discussed extents and limitations on electronic communications privacy accorded to citizens using email, websites and other online materials. Defined software very broadly. Also discussed electronic intellectual property.

Information Technology Reform Act of 1996 – Outlined reforms in IT acquisitions to match the marketplace changes to smaller processor systems. Also gave NIST computer security for non-military systems.

Cyberspace and Electronic Security Act of 1999 – helps law enforcement obtain usable evidence as encryption becomes more sophisticated. (Proposed by FBI and US DOJ).

Communication Decency Act of 1999 – required decency in public US computer communications networks.

Digital Millennium Copyright Act of 1999 - Extended copy right laws to new electronic technologies.

Related Laws and Acts Without specific dates.

Armed Services Procurement Act – Authorized the Defense Department, NASA, and Coast Guard to procure needed weapons systems and supplies. These systems may include computer chips and processors. (Nash & Cibinic, p 400).

Trade Secrets - Regulated the dissemination of trade secrets, patents (17 years), and copyright infringements in companies. Also discussed patents which would have included those in computer sciences and communications industries (Lusk et al, pp 1054-56)

Freedom of Information Act (FOIA) – States that any citizen may write for information about certain topics that are unclassified and receive them from the agency who must provide a response at a small charge to the citizen for copies and labor time (Lusk, et al, p 1135).

Government in the Sunshine Act – Stated that government should operate more openly on certain subjects and hold public meetings and hearings at senior executive levels that were not considered classified. (Lusk et al, p 1136)

Sherman Anti-Trust Act – Anti-monopoly law as applied in recent Microsoft case and AT&T monopoly in 1984. This law prevents total domination of an industry by one company regardless of the industry. (Lusk et al, pp. 1066-7).

Federal Government Management Reform Act – Outlined how agencies should reform the way they do business from a management perspective which included IRM or Information Resources Management and contract management.

Uniformed Commercial Code – Provide mandates for all legal and illegal US commercial and business activities. This also covers computers and communications equipment and software used by federal agencies, if not specifically, then by fact that they are a business. (Lusk et al, pp. 1147-1259.)

- Note – There are many legal issues relating to intelligence use of computers which have been historically off-budget in congress and are only reported to committees as needed. National security itself is paid for off-budget. (Kahn, 1968)

APPENDIX B

LIST OF FOREIGN COMPUTER RELATED LAWS

Australian, British, and German Laws and Acts (Chronological Order)

Trademarks Registration Act of 1875 – Trademarks required registration on inventions.

Law of Property Act of 1925 – British law on property protection.

Trade Marks Act of 1938 – Trade marks were accepted as a means to protect property.

Registered Design Act of 1949 – Covered designs of engineers as well as the names of engineering products.

Copyright Act of 1956 – Copy right protection of intellectual property.

Treaty of Rome 1957 -

Obscene Publications Act of 1959 – Barred obscene publications.

Obscene Publications Act of 1964 – Revise obscene publications.

German Copyright Act of 1965 – Copy right protection in Germany.

Civil Evidence Act of 1968 –

Theft Act of 1968 -

Trade Descriptions Act of 1968 -

Criminal Damage Act of 1971 –

Consumer Credit Act of 1974 -

Patents Act of 1977 –

Unfair Contracts Terms Act of 1977 -

Criminal Attempts Act of 1981 –

Forgery and Counterfeiting Act of 1981 –

Australian Copyright Amendment Act of 1984 – Australia's copyright law.

Data Protection Act of 1984 –

Copyright (Computer Software) Amendments Act of 1985 –

Interception of Communications Act of 1985 –

Access to Personal Files Act of 1987 –

Consumer Protection Act of 1987 -

Semiconductor Products (Protection of Topography) Regulations 1987 –

Copyright, Designs, and Patents Act of 1988 –

(Amended by Copyright (Computer Programs) Regulations 1992)

Design Right (Semiconductor Regulations) 1989 –

Patent Rules 1990 -

Computer Misuse Act of 1990 –

Health and Safety (Display Screen Equipment) Regulations 1992 –

Trade Marks Act of 1994 -

Intelligence Services Act of 1994 –

Note: The above acts and laws are listed in the 1996 David Bainbridge book entitled “Introduction to Computer Law”.

APPENDIX C

LIST OF NIST COMPUTER PUBLICATIONS

(From NIST List 91)

1. Current NIST Information Technology Lab Circulars on Computer Security through the Computer Security Clearinghouse:

- **Securing Web Servers** - September 1999
- **The Advanced Encryption Standard: A Status Report,** - August 1999
- **Computer Attacks: What They Are and How to Defend Against Them** - May 1999
- **Guide for Developing Security Plans for Information Technology Systems** - April 1999
- **Measurement and Standards for Computational Science and Engineering** - March 1999
- **Enhancements to Data Encryption and Digital Signature Federal Standards** - February 1999
- **Secure Web-Based Access to High Performance Computing Resources** - January 1999
- **What is Year 2000 Compliance?** - December 1998
- **Common Criteria: Launching the International Standard** - November 1998
- **Management of Risks in Information Systems: Practices of Successful Organizations** - March 1998
- **Information Security and the World Wide Web (WWW)** - February 1998

- **Internet Electronic Mail** - November 1997
- **Public Key Infrastructure Technology** - July 1997
- **Security Considerations in Computer Support and Operations** - April 1997
- **Audit Trails** – March 1997
- **Advanced Encryption Standard** - February 1997
- **Security Issues for Telecommuting** - January 1997
- **Generally Accepted System Security Principles (GSSPs): Guidance on Securing Information Technology (IT) Systems** - October 1996
- **Implementation Issues for Cryptography** - August 1996
- **Information Security Policies for Changing Information Technology Environments** - June 1996
- **The World Wide Web: Managing Security Risks** - May 1996
- **Millenium Rollover: The Year 2000 Problem** - March 1996
- **Human-Computer Interface Security Issues** - February 1996
- **An Introduction to Role-Based Access Control** - December 1995
- **Preparing for Contingencies and Disasters** - September 1995
- **FIPS 140-1:A Framework for Cryptographic Standards** - August 1995
- **Standards for Open Systems: More Flexibility for Federal Users** - May 1995
- **Acquiring and Using Asynchronous Transfer Mode in the Workplace** - March 1995
- **Digital Signature Standard** - November 1994
- **Reducing the Risks of Internet Connection and Use** - May 1994
- **Threats to Computer Systems: An Overview** - March 1994
- **Computer Security Policy** - January 1994
- **People: An Important Asset in Computer Security** - October 1993
- **Security Program Management** - August 1993
- **Connecting to the Internet: Security Considerations** - July 1993
- **Security Issues in Public Access Systems** - May 1993
- **Guidance on the Legality of Keystroke Monitoring** - March 1993
- **Sensitivity of Information** - November 1992
- **Disposition of Sensitive Automated Information** - October 1992
- **An Introduction to Secure Telephone Terminals** - March 1992
- **Establishing a Computer Security Incident Response Capability** - February 1992
- **Advanced Authentication Technology** - November 1991

- **Computer Security Roles of NIST and NSA** - February 1991
- **Computer Viruses and Other Related Threats** - August 1990

2. SPECIAL PUBLICATIONS AND OTHER REPORTS
NIST Internal Reports (NISTIRs) describe research of a technical nature of interest to a specialized audience.

ACCESS CONTROL & AUTHENTICATION TECHNOLOGY
NISTIR 6192
A REVISED MODEL FOR ROLE BASED ACCESS CONTROL
By Wayne A. Jansen
July 1998

NIST SPEC PUB 500-157
SMART CARD TECHNOLOGY: NEW METHODS FOR COMPUTER ACCESS CONTROL
By Martha E. Haykin and Robert B. J. Warner
September 1988

NBS SPEC PUB 500-156
MESSAGE AUTHENTICATION CODE (MAC) VALIDATION SYSTEM: REQUIREMENTS AND PROCEDURES
By Miles Smid, Elaine Barker, David Balenson and Martha Haykin
May 1988

3. CRITERIA AND ASSURANCE
NISTIR 6068
REPORT ON THE TMACH EXPERIMENT
By Ellen Flahavin, Goswin Eisen, Steve Hill, Heribert Spindler, Julian Straw and Andy Webber
July 1997
This report documents the findings of a multi-national evaluation experiment, funded by the U.S. Advanced Research Projects Agency (ARPA), to explore alternative approaches to security evaluation.

NISTIR 5810
THE TMACH EXPERIMENT PHASE I - PRELIMINARY DEVELOPMENTAL EVALUATION
By Ellen Colvin Flahavin
June 1996
This document describes the multi-national evaluation experiment of the Trusted Mach system. The report focuses on Phase I - The Developmental Evaluation Phase.

NISTIR 5590
PROCEEDINGS REPORT OF THE INTERNATIONAL INVITATION WORKSHOP ON DEVELOPMENTAL ASSURANCE
By Patricia Toth
January 1995
This publication presents the proceedings of an invitational workshop on development assurance held in June 1994. Co-sponsors of the workshop were NIST, the National Security Agency, the Canadian Communications Security Establishment, and the European Commission.

NISTIR 5540
MULTI-AGENCY CERTIFICATION AND ACCREDITATION (C&A) PROCESS: A WORKED EXAMPLE
By Ellen Flahavin, Annabelle Lee, and Dawn Wolcott
December 1994
This document describes a worked example of a multi-agency certification and accreditation process. Although it focuses on the Mountain Pass Project implemented for the Drug Enforcement Administration, the document presents lessons learned and provides practical guidance to federal agencies that perform multi-agency C&A.

NISTIR 5472
A HEAD START ON ASSURANCE PROCEEDINGS OF AN INVITATIONAL WORKSHOP ON INFORMATION TECHNOLOGY (IT) ASSURANCE AND TRUSTWORTHINESS
Marshall D. Abrams and Patricia R. Toth, Editors
August 1994
This document presents the proceedings of a workshop held in March 1994 in Williamsburg, Virginia, to identify crucial issues on assurance in IT systems and to

provide input into the development of policy guidance on determining the type and level of assurance appropriate in a given environment.

NISTIR 5153
MINIMUM SECURITY REQUIREMENTS FOR MULTI-USER OPERATING SYSTEMS
By David Ferraiolo, Nickilyn Lynch, Patricia Toth, David Chizmadia, Michael Ressler, Roberta Medlock, and Sarah Weinberg
March 1993
This document provides basic commercial computer system security requirements applicable to both government and commercial organizations. These requirements form the basis for the commercially oriented protection profiles in Volume II of the draft Federal Criteria for Information Technology Security document (known as the Federal Criteria).

NISTIR 4774
A REVIEW OF U.S. AND EUROPEAN SECURITY EVALUATION CRITERIA
By Charles R. Dinkel
March 1992
This report reviews five U.S. and European documents which describe criteria for specifying and evaluating the trust of computer products and systems.

NBS SPEC PUB 500-153
GUIDE TO AUDITING FOR CONTROLS AND SECURITY: A SYSTEM DEVELOPMENT LIFE CYCLE APPROACH
Editors/Authors: Zella G. Ruthberg, Bonnie Fisher, William E. Perry, John W. Lainhart IV, James G. Cox, Mark Gillen, and Douglas B. Hunt
April 1988

4. CRYPTOGRAPHY
NIST SPEC PUB 800-17
MODES OF OPERATION VALIDATION SYSTEM (MOVS): REQUIREMENTS AND PROCEDURES
By Sharon Keller and Miles Smid
February 1998
The Modes of Operation Validation System (MOVS) specifies the procedures involved in validating implementations of the DES and Skipjack algorithms. It is designed to perform automated testing on Implementations Under Test (IUTs). The MOVS consists

of two categories of tests - Known Answer tests and Modes tests - which are detailed for each mode of operation. This publication also specifies the requirements and administrative procedures to be followed by those seeking formal NIST validation of an implementation of the DES or Skipjack algorithm.

NIST SPEC PUB 800-15
MINIMUM INTEROPERABILITY SPECIFICATION FOR PKI COMPONENTS (MISPC), VERSION 1
By William E. Burr, Donna F. Dodson, Noel A. Nazario, and William T. Polk
January 1998
The Minimum Interoperability Specification for PKI Components (MISPC) supports interoperability for a large-scale public key infrastructure (PKI) that issues, revokes, and manages X.509 version 3 digital signature public key certificates and version 2 certificate revocation lists (CRLs). The MISPC supports both hierarchical and network trust models.

NISTIR 5788
PUBLIC KEY INFRASTRUCTURE INVITATIONAL WORKSHOP SEPTEMBER 28, 1995, MITRE CORPORATION, MCLEAN, VIRGINIA
William E. Burr, Editor
November 1995
This report constitutes the proceedings of an invitational workshop cosponsored by NIST, the Security Infrastructure Program Management Office (SI-PMO), and the MITRE Corporation. Papers were presented on the current state of technology and standards for a Public Key Infrastructure, management and technical issues, escrowing keys used for confidentiality exchanges, and cost models.

NISTIR 5234
REPORT OF THE NIST WORKSHOP ON DIGITAL SIGNATURE CERTIFICATE MANAGEMENT, DECEMBER 10-11, 1992
Dennis K. Branstad, Editor
August 1993
This report summarizes the major topics of discussion at a workshop on Digital Signature Certificate Management held at NIST on December 10-11, 1992. The purpose of the workshop was to review existing and required technologies for digital signature certification and to develop recommendations for certificate contents and formats.

NIST SPEC PUB 800-2
PUBLIC-KEY CRYPTOGRAPHY
By James Nechvatal
April 1991
This publication surveys public-key cryptography, discussing the theory and examining examples of public-key cryptosystems. The related topics of digital signatures, hash functions, and zero-knowledge protocols are also covered.

NBS SPEC PUB 500-61
MAINTENANCE TESTING FOR THE DATA ENCRYPTION STANDARD
By Jason Gait
August 1980

5. ELECTRONIC COMMERCE
NIST SPEC PUB 800-9
GOOD SECURITY PRACTICES FOR ELECTRONIC COMMERCE, INCLUDING ELECTRONIC DATA INTERCHANGE
Roy G. Saltman, Editor
December 1993
This report presents security procedures and techniques, including internal controls and checks, that constitute good practice in the design, development, testing, and operation of electronic commerce systems. Security techniques considered include audit trails, contingency planning, use of acknowledgements, electronic document management, activities of support networks, user access controls to systems and networks, and cryptographic techniques for authentication and confidentiality.

6. GENERAL COMPUTER SECURITY
NIST SPEC PUB 800-18
GUIDE FOR DEVELOPING SECURITY PLANS FOR INFORMATION TECHNOLOGY SYSTEMS
By Marianne Swanson and Federal Computer Security Program Managers' Forum
December 1998
This guideline addresses the development of security plans that document the management, technical, and operational controls for federal automated information systems. Written primarily for federal agencies, the concepts are also valuable for industry organizations interested in establishing security plans.

NIST SPEC PUB 800-16
INFORMATION TECHNOLOGY SECURITY TRAINING REQUIREMENTS: A ROLE- AND PERFORMANCE-BASED MODEL (supersedes NIST Spec Pub 500-172)
Mark Wilson, Editor; Dorothea E. de Zafra, Sadie I. Pitcher, John D. Tressler, and John B. Ippolito
March 1998
This document is designed for use by federal agencies who develop security training and awareness courses, or for those personnel who develop information technology (IT) security training for government use. The document emphasizes training criterial or standards, rather than fixed content of specific courses and audiences. The emphasis on roles and results gives the training requirements flexibility, adaptability, and longevity.

NIST SPEC PUB 800-14
GENERALLY ACCEPTED PRINCIPLES AND PRACTICES FOR SECURING INFORMATION TECHNOLOGY SYSTEMS
By Marianne Swanson and Barbara Guttman
June 1996
This document provides a baseline that organizations can use to establish and review their information technology (IT) security programs. It presents a foundation of generally accepted system security principles and gives common practices that are used in securing IT systems. The guideline assists managers, internal auditors, users, system developers, and security professionals to gain an understanding of basic security requirements.

NIST SPEC PUB 800-12
AN INTRODUCTION TO COMPUTER SECURITY: THE NIST HANDBOOK
By Barbara Guttman and Edward Roback October 1995
This handbook provides assistance in securing computer-based resources (including hardware, software, and information) by explaining important concepts, cost considerations, and interrelationships of security controls. It gives a broad overview of computer security to help readers understand their computer security needs and to develop a sound approach in selecting appropriate security controls.

NISTIR 5308
GENERAL PROCEDURES FOR REGISTERING COMPUTER SECURITY OBJECTS

Noel A. Nazario, Editor
December 1993
This publication describes the object-independent procedures for operating the Computer Security Objects Register (CSOR) which services organizations and individuals seeking to use a common set of tools and techniques in computer security.

NIST SPEC PUB 800-6
AUTOMATED TOOLS FOR TESTING COMPUTER SYSTEM VULNERABILITY By W. Timothy Polk
December 1992
This document discusses the use of automated tools to perform system vulnerability tests. The tests examine a system for vulnerabilities that can result from improper use of controls or mismanagement, such as easily guessed passwords or improperly protected system files.

NIST SPEC PUB 800-5
A GUIDE TO THE SELECTION OF ANTI-VIRUS TOOLS AND TECHNIQUES
By W. Timothy Polk and Lawrence E. Bassham
December 1992
This guide gives criteria for judging the functionality, practicality, and convenience of anti-virus tools so that users can determine which tools are best suited to target environments.

NISTIR 4939
THREAT ASSESSMENT OF MALICIOUS CODE AND EXTERNAL ATTACKS
By Lawrence E. Bassham and W. Timothy Polk
October 1992
This report provides an assessment of the threats associated with malicious code and external attacks on systems using commercially available hardware and software.

NIST SPEC PUB 800-4
COMPUTER SECURITY CONSIDERATIONS IN FEDERAL PROCUREMENTS: A GUIDE FOR PROCUREMENT INITIATORS, CONTRACTING OFFICERS, AND COMPUTER SECURITY OFFICIALS
By Barbara Guttman
March 1992
This document assists federal agencies in selecting and acquiring cost-effective

computer security by explaining how to include computer security requirements in federal information processing procurements.

NISTIR 4749
SAMPLE STATEMENTS OF WORK FOR FEDERAL COMPUTER SECURITY SERVICES: FOR USE IN-HOUSE OR CONTRACTING OUT
Dennis M. Gilbert, Project Leader
Nickilyn Lynch, Editor
December 1991
This document presents a set of Statements of Work (SOWs) describing significant computer security activities. It assists federal agencies and government contractors in the acquisition of computer security services by standardizing the description of typical services available from within or outside of the organization.

NIST SPEC PUB 800-3
ESTABLISHING A COMPUTER SECURITY INCIDENT RESPONSE CAPABILITY (CSIRC)
By John Wack
November 1991
This publication describes increased computer security efforts, designated as Computer Security Incident Response Capabilities (CSIRC), which offer an efficient and cost-effective response to computer security threats. A CSIRC is a proactive approach to computer security, one that combines reactive capabilities with active steps to prevent future incidents.

NIST SPEC PUB 500-172
COMPUTER SECURITY TRAINING GUIDELINES
By Mary Anne Todd and Constance Guitian
November 1989
These guidelines provide a framework for determining the training needs of employees involved with computer systems. It describes the learning objectives of agency computer security training programs " what the employee should know and be able to direct or actually perform " so that agencies may use the guidance to develop or acquire training programs that fit the agency environment.

NIST SPEC PUB 500-166
COMPUTER VIRUSES AND RELATED THREATS: A MANAGEMENT GUIDE

By John P. Wack and Lisa J. Carnahan
August 1989
This document contains guidance for managing the threats of computer viruses and related software and unauthorized use. It is geared towards managers of end-user groups and managers dealing with multi-user systems, personal computers and networks. The guidance is general and addresses the vulnerabilities that are most likely to be exploited.

NBS SPEC PUB 500-134
GUIDE ON SELECTING ADP BACKUP PROCESS ALTERNATIVES
By Irene Isaac
November 1985

NBS SPEC PUB 500-133
TECHNOLOGY ASSESSMENT: METHODS FOR MEASURING THE LEVEL OF COMPUTER SECURITY
By William Neugent, John Gilligan, Lance Hoffman, and Zella G. Ruthberg
October 1985

NBS SPEC PUB 500-120
SECURITY OF PERSONAL COMPUTER SYSTEMS - A MANAGEMENT GUIDE
By Dennis D. Steinauer
January 1985

7. NETWORK SECURITY
NIST SPEC PUB 800-10
KEEPING YOUR SITE COMFORTABLY SECURE: AN INTRODUCTION TO INTERNET FIREWALLS
By John P. Wack and Lisa J. Carnahan
December 1994
This publication provides an overview of the Internet and security-related problems. It describes firewall components, the reasoning behind firewall usage, several types of network access policies, and resources for more information. The document assists federal and industry users in planning and purchasing a firewall.

NIST SPEC PUB 800-7
SECURITY IN OPEN SYSTEMS

By R. Bagwill, J. Barkley, L. Carnahan, S. Chang, R. Kuhn, P. Markovitz, A. Nakassis, K. Olsen, M. Ransom, and J. Wack John Barkley, Editor
July 1994
This report provides information for service designers and programmers involved in the development of telecommunications application software; it focuses on building security into software based on open system platforms. The document is also useful for product planners, administrators, users, and management personnel who are interested in understanding the capabilities and limitations of open systems.

NISTIR 5232
REPORT OF THE NSF/NIST WORKSHOP ON NSFNET/NREN SECURITY, JULY 6-7, 1992
By Arthur E. Oldehoeft
May 1993
This report describes a workshop hosted by NIST and sponsored by the National Science Foundation to address the need for improving the security of national computer networks.

NISTIR 4734
FOUNDATIONS OF A SECURITY POLICY FOR USE OF THE NATIONAL RESEARCH AND EDUCATIONAL NETWORK
By Arthur E. Oldehoeft
February 1992
This report explores the foundations of a national network security policy and proposes a draft policy for the National Research and Educational Network (NREN).

8. RISK MANAGEMENT
NIST SPEC PUB 500-174
GUIDE FOR SELECTING AUTOMATED RISK ANALYSIS TOOLS
By Irene E. Gilbert
October 1989
This document recommends a process for selecting automated risk analysis tools, describing important considerations for developing selection criteria for acquiring risk analysis software. The report describes three essential elements that should be present in an automated risk analysis tool: data collection, analysis, and output results. It is intended primarily for managers and those responsible for managing risks in computer and telecommunications systems.

NBSIR 86-3386
WORK PRIORITY SCHEME FOR EDP AUDIT AND COMPUTER SECURITY REVIEW
By Zella Ruthberg and Bonnie Fisher
August 1986
This publication describes a methodology for prioritizing the work performed by EDP auditors and computer security reviewers. Developed at an invitational workshop attended by government and private sector experts, the work plan enables users to evaluate computer systems for both EDP audit and security review functions and to develop a measurement of the risk of the systems. Based on this measure of risk, the auditor can then determine where to spend review time.

9. SPECIAL TOPICS
NISTIR 5570
AN ASSESSMENT OF THE DOD GOAL SECURITY ARCHITECTURE (DGSA) FOR NON-MILITARY USE
By Arthur E. Oldehoeft
November 1994
This study assesses the potential of the DGSA as a model and framework for the development of non-military computer and information security architectures.

NIST GCR 94-654
FEDERAL CERTIFICATION AUTHORITY LIABILITY AND POLICY
By Michael S. Baum
June 1994
This report identifies technical, legal, and policy issues affecting a certificate-based public key cryptographic infrastructure utilizing digital signatures supported by "trusted entities."

NISTIR 5283
SECURITY OF SQL-BASED IMPLEMENTATIONS OF PRODUCT DATA EXCHANGE USING STEP
By Lawrence E. Bassham and W. Timothy Polk
October 1993
This report examines the security implications of the versions of the SQL standard as used to implement the Standard for the Exchange of Product Model Data (STEP), an emerging international standard.

NIST SPEC PUB 800-8
SECURITY ISSUES IN THE DATABASE LANGUAGE SQL
By W. Timothy Polk and Lawrence E. Bassham
August 1993
The Database Language SQL is a standard interface for accessing and manipulating relational databases. This document examines the security functionality that might be required of relational database management systems (DBMS) and compares these functions with the requirements and options of the SQL specifications.

NBS SPEC PUB 500-158
ACCURACY, INTEGRITY, AND SECURITY IN COMPUTERIZED VOTE-TALLYING
By Roy G. Saltman
August 1988
This study surveys some events concerning computerized vote-tallying and reviews current problems. The report recommends that accepted practices of internal control be applied to vote-tallying, including the use of software for integrity and logical correctness; dedicated software use and dedicated operation; improved design and certification of vote-tallying systems that do not use ballots; and improved pre-election testing and partial manual recounting of ballots.

10. TELECOMMUNICATIONS

NIST SPEC PUB 800-13
TELECOMMUNICATIONS SECURITY GUIDELINES FOR TELECOMMUNICATIONS MANAGEMENT NETWORK
By John Kimmins, Charles Dinkel, and Dale Walters
October 1995
This document gives guidance on enhancing the security of the Public Switched Network (PSN) which provides critical commercial telecommunications services and National Security and Emergency Preparedness (NSEP). The guidance assists telecommunications vendors in developing systems and service providers in implementing systems with appropriate security for integration into the PSN. It is also useful to government agencies or commercial organizations in formulating a specific security policy.

NIST SPEC PUB 800-11
THE IMPACT OF THE FCC's OPEN NETWORK ARCHITECTURE ON NS/EP TELECOMMUNICATIONS SECURITY
By Karen Olsen and John Tebbutt
February 1995
This report provides an overview of the Federal Communications Commission's Open Network Architecture (ONA), describes National Security and Emergency Preparedness (NS/EP) telecommunications security concerns, and details NS/EP telecommunications security concerns that the FCC's ONA requirement introduces into the Public Switched Network (PSN).

NIST GCR 93-635
PRIVATE BRANCH EXCHANGE (PBX) SECURITY GUIDELINES
September 1993
This document presents the basic concepts of PBX security. It describes a telephone switch system, hardware and software assets, specific security threats, and the functions of the PBX administrator. An example of a security policy and some controls needed to secure the PBX environment are also given.

NIST SPEC PUB 500-189
SECURITY IN ISDN
By William E. Burr
September 1991
This document discusses the standards needed to implement user security in Integrated Services Digital Network (ISDN) technology. The publication provides a broad discussion of user security needs and suggests possible solutions.

NIST SPEC PUB 500-137
SECURITY FOR DIAL-UP LINES
By Eugene F. Troy
July 1986
This publication describes a set of solutions to the problem of intrusion into government and private computers via dial-up telephone lines, the so-called "hacker problem."

11. FEDERAL INFORMATION PROCESSING STANDARDS

Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology (NIST) after approval by the Secretary

of Commerce pursuant to Section 5131 of the Information Technology Reform Act of 1996, Public Law 104-106, and the Computer Security Act of 1987 (Public Law 100-235).

11.1 ACCESS CONTROL(FIPS)

FIPS PUB 48
GUIDELINES ON EVALUATION OF TECHNIQUES FOR AUTOMATED PERSONAL IDENTIFICATION
April 1977
This guideline discusses the performance of personal identification devices, how to evaluate them and considerations for their use within the context of computer systems security.

FIPS PUB 83
GUIDELINE ON USER AUTHENTICATION TECHNIQUES FOR COMPUTER NETWORK ACCESS CONTROL
September 1980
This document provides guidance in the selection and implementation of techniques for authenticating the users of remote terminals in order to safeguard against unauthorized access to computers and computer networks. Describes use of passwords, identification tokens, verification by means of personal attributes, identification of remote devices, role of encryption in network access control, and computerized authorization techniques.

FIPS PUB 112
STANDARD ON PASSWORD USAGE
May 1985
This standard defines ten factors to be considered in the design, implementation, and use of access control systems that are based on passwords. It specifies minimum security criteria for such systems and provides guidance for selecting additional security criteria for password systems which must meet higher security requirements.

FIPS PUB 190
GUIDELINE FOR THE USE OF ADVANCED AUTHENTICATION TECHNOLOGY ALTERNATIVES
September 1994

This guideline describes the primary alternative methods for verifying the identities of computer system users, and provides recommendations to federal agencies and departments for the acquisition and use of technology which supports these methods.

11.2 CRYPTOGRAPHY(FIPS)

FIPS PUB 46-2
DATA ENCRYPTION STANDARD
December 1993 (Reaffirmed until 1998, FIPS PUB 46-3 is in progress)
This standard reaffirms the Data Encryption Algorithm (DEA) until 1998 and allows for implementation of the DEA in software, firmware or hardware. The DEA is a mathematical algorithm for encrypting and decrypting binary-coded information.

FIPS PUB 74
GUIDELINES FOR IMPLEMENTING AND USING THE NBS DATA ENCRYPTION STANDARD
April 1981
This document provides guidance for the use of cryptographic techniques when such techniques are required to protect sensitive or valuable computer data. For use in conjunction with FIPS PUB 46-2 and FIPS PUB 81.

FIPS PUB 81
DES MODES OF OPERATION
December 1980
This standard defines four modes of operation for the Data Encryption Standard which may be used in a wide variety of applications. The modes specify how data will be encrypted (cryptographically protected) and decrypted (returned to original form). The modes included in this standard are the Electronic Codebook (ECB) mode, the Cipher Block Chaining (CBC) mode, the Cipher Feedback (CFB) mode, and the Output Feedback (OFB) mode.

FIPS PUB 113
STANDARD ON COMPUTER DATA AUTHENTICATION
May 1985
This standard specifies a Data Authentication Algorithm (DAA) which, when applied to computer data, automatically and accurately detects unauthorized modifications, both intentional and accidental. Based on the Data Encryption Standard (DES), this

standard is compatible with the requirements adopted by the Department of the Treasury and the banking community to protect electronic fund transfer transactions.

FIPS PUB 139
INTEROPERABILITY AND SECURITY REQUIREMENTS FOR USE OF THE DATA ENCRYPTION STANDARD IN THE PHYSICAL LAYER OF DATA COMMUNICATIONS
August 1983

This standard facilitates the interoperation of government data communication facilities, systems, and data that require cryptographic protection using the Data Encryption Standard (DES) algorithm. The standard specifies interoperability and security-related requirements using encryption at the Physical Layer of the ISO Open Systems Interconnection (OSI) Reference Model (International Standard 7498) in the telecommunications systems conveying ADP or narrative text information.

FIPS PUB 140-1
SECURITY REQUIREMENTS FOR CRYTOGRAPHIC MODULES
January 1994
This standard provides specifications for cryptographic modules which can be used within computer and telecommunications systems to protect unclassified information in a variety of different applications.

FIPS PUB 141
INTEROPERABILITY AND SECURITY REQUIREMENTS FOR USE OF THE DATA ENCRYPTION STANDARD WITH CCITT GROUP 3 FACSIMILE EQUIPMENT
April 1985
This standard specifies interoperability and security-related requirements for use of encryption with International Telegraph and Telephone Consultative Committee (CCITT), Group 3 type facsimile equipment conveying Automatic Data Processing (ADP) and/or narrative text information.

FIPS PUB 171
KEY MANAGEMENT USING ANSI X9.17
April 1992
This standard specifies a selection of options for the automated distribution of keying material by the federal government when using the protocols of ANSI X9.17. The standard defines procedures for the manual and automated management of keying

materials and contains a number of options. The selected options will allow the development of cost effective systems which will increase the likelihood of interoperability.

FIPS PUB 180-1
SECURE HASH STANDARD
April 1995
This standard specifies a Secure Hash Algorithm (SHA) which can be used to generate a condensed representation of a message called a message digest. The SHA is required for use with the Digital Signature Algorithm (DSA) as specified in the Digital Signature Standard (DSS) and whenever a secure hash algorithm is required for federal applications. The SHA is used by both the transmitter and intended receiver of a message in computing and verifying a digital signature.

FIPS PUB 181
AUTOMATED PASSWORD GENERATOR (APG)
October 1993
This publication specifies a standard to be used by federal organizations that require computer generated pronounceable passwords to authenticate the personal identity of an automated data processing (ADP) system user, and to authorize access to system resources. The standard describes an automated password generation algorithm that randomly creates simple pronounceable syllables as passwords. The password generator accepts input from a random number generator based on the Data Encryption Standard (DES) cryptographic algorithm defined in FIPS PUB 46-2.

FIPS PUB 185
ESCROWED ENCRYPTION STANDARD (EES)
February 1994
This standard specifies a technology developed by the federal government to provide strong encryption protection for unclassified information and to provide that the keys used in the encryption and decryption processes are escrowed.

FIPS PUB 186-1
DIGITAL SIGNATURE STANDARD (DSS)
December 1998
This standard specifies a suite of algorithms that can be used to generate a digital signature. Digital signatures are used to detect unauthorized modifications to data and

to authenticate the identity of the signatory. In addition, the recipient of signed data can use a digital signature in proving to a third party that the signature was in fact generated by the signatory. This is known as nonrepudiation since the signatory cannot, at a later time, repudiate the signature.

FIPS PUB 196
ENTITY AUTHENTICATION USING PUBLIC KEY CRYPTOGRAPHY
February 1997
This standard specifies two challenge-response protocols by which entities in a computer system may authenticate their identities to one another. These protocols may be used during session initiation, and at any other time that entity authentication is necessary. Depending on which protocol is implemented, either one or both entities involved may be authenticated. The defined protocols are derived from an international standard for entity authentication based on public key cryptography, which uses digital signatures and random number challenges.

11.3 GENERAL COMPUTER SECURITY(FIPS)

FIPS PUB 31
GUIDELINES FOR ADP PHYSICAL SECURITY AND RISK MANAGEMENT
June 1974
This document provides guidance to federal organizations in developing physical security and risk management programs for their ADP facilities. Covers security analysis, natural disasters, failure of supporting utilities, system reliability, procedural measures and controls, protection of off-site facilities, contingency plans security awareness, and security audit. Can be used as a checklist for planning and evaluating security of computer systems.

FIPS PUB 41
COMPUTER SECURITY GUIDELINES FOR IMPLEMENTING THE PRIVACY ACT OF 1974
May 1975
This publication provides guidance in the selection of technical and related procedural methods for protecting personal data in automated information systems. Discusses categories of risks and the related safeguards for physical security, information management practices, and system controls to improve system security.

FIPS PUB 73
GUIDELINES FOR SECURITY OF COMPUTER APPLICATIONS
June 1980
This guideline describes the different security objectives for a computer application, explains the control measures that can be used, and identifies the decisions that should be made at each stage in the life cycle of a sensitive computer application. For use in planning, developing and operating computer systems which require protection. Fundamental security controls such as data validation, user identity verification, authorization, journaling, variance detection, and encryption are discussed.

FIPS PUB 87
GUIDELINES FOR ADP CONTINGENCY PLANNING
March 1981
This guideline describes what should be considered when developing a contingency plan for an ADP facility. Provides a suggested structure and format which may be used as a starting point from which to design a plan to fit each specific operation.

FIPS PUB 102
GUIDELINE FOR COMPUTER SECURITY CERTIFICATION AND ACCREDITATION
September 1983
This guideline describes how to establish and carry out a certification and accreditation program for computer security. Certification consists of a technical evaluation of a sensitive system to see how well it meets its security requirements. Accreditation is the official management authorization for the operation of the system and is based on the certification process.

FIPS PUB 188
STANDARD SECURITY LABEL FOR INFORMATION TRANSFER
September 1994
This standard defines a security label syntax for information exchanged over data networks and provides label encodings for use at the Application and Network Layers of the Open Systems Interconnection (OSI) Reference Model. Security labels convey information used by protocol entities to determine how to handle data communicated between open systems. Information on a security label can be used to control access, specify protective measures, and determine additional handling restrictions required by a communications security policy.

FIPS PUB 191
GUIDELINE FOR THE ANALYSIS OF LOCAL AREA NETWORK SECURITY
November 1994
This guideline can be used as a tool to help improve the security of a local area network (LAN). A LAN security architecture is described that discusses threats and vulnerabilities that should be examined, as well as security services and mechanisms that should be explored.

COMPUTER SECURITY RESOURCE CLEARINGHOUSE
ITL maintains an electronic Computer Security Resource Clearinghouse (CSRC) to encourage the sharing of information on computer security. The CSRC contains computer security awareness and training information, publications, conferences, software tools, security alerts, and prevention measures. The CSRC system, available 24 hours a day, also points to other computer security servers.

Internet Access
To access the clearinghouse via an http client, use the following Uniform Resource Locator (URL): http://csrc.nist.gov. For information on the Cryptographic Module Validation Program: http://csrc.nist.gov/cryptval/

FedCIRC

The Federal Computer Incident Response Capability (FedCIRC) is a new initiative undertaken by NIST, the Department of Energy's Computer Incident Advisory Capability (CIAC), and the Carnegie Mellon, Software Engineering Institute's CERT/CC. These established computer security organizations have banded together to offer the federal civilian community assistance and guidance in handling computer security-related incidents.
Most agencies require incident response assistance now because of their rapid and expanding involvement in the use of the Internet and other networking technologies. OMB has recognized this long-term need by requiring agency incident response capabilities in OMB Circular A-130 (Appendix III). FedCIRC is designed to address those near-term and long-term needs.

For more information on FedCIRC, call (301) 975-4369, e-mail fedcirc-info@fedcirc.nist.gov, or visit the Web site at: http://csrc.nist.gov/fedcirc.

Source: The above information on computer security related and general computer government standards was obtained from the NIST website on 13 September, 2000 at www.nist.gov.

APPENDIX D

WILD LIST as of May 2000

WildList Index

Home

VB 100% Award
Subscriptions
Conference
Virus Hoaxes
Project VGrep
Prevalence Tables
WildLists
AV Links
Contact Us

Joe Wells has, for a few years now, been collecting virus reports from anti-virus experts around the world. He combines these to produce the WildList, a list of those viruses currently in the wild.
In recent times, the list has started to be used by Virus Bulletin and other anti-virus product testers as the definitive guide to the the viruses found in the real world.

An anti-virus product is expected to score 100% detection against this group of viruses.
In addition to viewing the lists here, you may download individual WildLists (in ZIP or text format) from links at the top of each list's page.

May 2000
April 2000
February 2000
January 2000
December 1999

November 1999
October 1999
September 1999
August 1999
July 1999
June 1999
May 1999
April 1999
March 1999
February 1999
January 1999
December 1998
October 1998
August 1998
July 1998
June 1998
May 1998
April 1998
March 1998
February 1998
January 1998
December 1997
November 1997
October 1997
September 1997
August 1997
July 1997
May 1997
March 1997
February 1997
December 1996
October 1996
September 1996
July 1996
June 1996
May 1996
March 1996

February 1996
January 1996
November 1995
October 1995
September 1995
August 1995
July 1995
June 1995
May 1995
February 1995
January 1995
September 1994
August 1994
July 1994
March 1994
February 1994
December 1993
November 1993
September 1993
July 1993

WildList, May 2000
A version of this WildList is available for download, either in ZIP or text format.

==========

PC Viruses in the Wild - May, 2000

==========

This is a cooperative listing of viruses reported as being in the wild by 61 virus information professionals. The basis for these reports are

virus incidents where a sample was received, and positively identified by the participant. Rumors and unverified reports have been excluded.

Some programs included in this list may fall outside the traditional definition of a computer virus. However, such programs are spreading throughout diverse user populations, are a threat to users and are therefore included in this list.

This report is cumulative. That is, this is not just a report of which viruses were seen last month. Monthly data is received from most participants, but the new data is added to the old. Participants are expected to let us know when to remove their name from a virus.

The list should not be considered a list of "the most common viruses", however, since no specific provision is made for a commonness factor.

This data indicates only "which" viruses are in the wild, but viruses reported by many (or most) participants are obviously widespread.

The WildList is currently being used as the basis for in-the-wild virus testing and certification of anti-virus products by the ICSA, Virus Bulletin and Secure Computing. Additionally, a virus collection based upon the WildList is being used in an effort to standardize the naming of common viruses.

The WildList - (c)1993-2000 by Joe Wells - info@wildlist.org

Key Participant	Region	Organization	Product
Aa Asaf Achitoov	Israel	iRiS Software	AntiVirus Plus
Ac Alan Candy	New Zealand	Applied Insight	-
Ad Allan Dyer	Hong Kong	Yui Kee Co. Ltd.	F-Prot
Ae Amir Elbaz	Israel	Aladdin	eSafe Protect

Ak	Ahmad Y. Kashoor	Syria	CompuKashoor	Dr Solomon's
Am	Andreas Marx	Germany	Univ. of Magdeburg	-
As	Alex Shipp	UK	MessageLabs	StarScan
Bh	Bruce Hughes	USA	ICSA	-
Cb	Carl Bretteville	Norway	Norman ASA	NVC
Cr	Costin RAIU	Romania	GeCAD	RAV
Cs	Christian Schmid	Austria	DataPROT Linz	F-Prot
Dc	Dave Chess	USA	IBM	NAV
Dg	Dmitry Gryaznov	UK	McAfee (UK)	VirusScan
Dp	David Phillips	UK	Open University	-
Ei	Eddy Willems	EU	EICAR	-
Ek	Eugene Kaspersky	Russia	KAMI	AVP
Ew	Eddy Willems	Belgium/Lux.	Data Alert Int'l	VirusScan
Fh	Fraser Howard	UK	Virus Bulletin	-
Fl	Ferenc Leitold	Hungary	Hunix Ltd.	Virus Buster
Fp	Francois Paget	France	McAfee (France)	VirusScan
Gb	Gerald Batten	Canada	Independent	-
Gm	Gerard Mannig	France	Independent	-
Ic	Ieta Chi	Taiwan	Trend Micro	PC-cillin
Jd	Joost de Raeymaeker	Portugal	RSVP	-
Jh	Joe Hartmann	USA	Trend Micro	PC-cillin
Jk	Jimmy Kuo	USA	McAfee (Independent)	-
Jm	Jose Martinez	Peru	HackSoft S.R.Ltda	TH AV
Jr	Joon Radley	South Africa	VPS	VPS
Kb	Kenneth Bechtel	USA	Team Anti-Virus	-
Kd	K. T. Davies	India	Pioneer Micro	Vaxine
Ls	Luca Sambucci	Italy	Itaweb	-
Mh	Mikko Hypponen	Finland	Data Fellows	F-Prot Pro
Ml	Mickey Loh	Malaysia	R.E.Solutions	Armour AV
Ms	Marek Sell	Poland	Marek Sell, Ltd.	MkS_vir
Mt	Miroslav Trnka	Slovakia	ESET Ltd	NOD-ICE
Oz	Jakub Kaminski	Australia	Computer Associates	VET
Pb	Pavel Baudis	Czech Republic	ALWIL Software	Avast!
Pn	Patrick Nolan	USA	McAfee (US)	VirusScan
Pt	Peter Theobald	India	IT Secure Software	VirusScan
Ra	Ruben Arias	Argentina	RALP	Integ Master
Rf	Richard Foley	Ireland	Reflex Magnetics	TBAV

Rg	Ray Glath, Sr.	USA	Tavisco Ltd.	Vi-Spy
Rp	Ronnie Pineda	Philippines	Mannasoft Corp.	VirusScan
Rv	Robert Vibert	Canada	Independent	-
Rz	Righard Zwienenberg	Netherlands	Norman Data Defense	NVC
Sb	Sherra Buzzell	USA	Symantec	NAV
Sh	Sha-Li Hsieh	USA	Computer Associates	Inoculate IT
Sk	Seok-Chul Kwon	Korea	HAURI	ViRobot
Sm	Seiji Murakami	Japan	JCSR	-
So	Simon Borduas	Canada	HYPERTEC Security	F-Prot Pro
Sr	Subramanya Rao	India	Proland Software	Protector Plus
St	Stuart Taylor	UK	Sophos Plc.	Sweep
Ta	Tjark Auerbach	Germany	H+BEDV GmbH	AntiVir
Tc	Tzvetan Chaliavski	USA	Command Software	F-Prot Pro
Td	Toralv Dirro	Germany	U of Hamburg	VirusScan
Ti	Torben Immisch	Denmark	Swanholm Distrib.	NAV
Wl	WLO	-	WLO	-
Ws	Wolfgang Stiller	USA	Stiller Research	Integ Master
Xc	Xabier Cazalis	Spain	Panda Software	Panda
Za	Corporate #1	Western USA	-	-
Zb	Corporate #2	Eastern USA	-	-

==========

The WildList

==========

This main list includes viruses reported by multiple participants, which appear to be non-regional in nature. Technically, this first list is "the" WildList according to original specification, which required viruses to be verified in the wild by a minimum of two participants. A supplemental list follows that contains viruses reported by single participants.

+ Viruses marked with a plus sign (+) are new to the main list this month.

Name of Virus	List [Alias(es)]	Reported Date	by:

==========
AntiCMOS.A.....[Lenart.....] 1/95 AkAmEwFhFpIcJdJhJrMhMlOzRz
SbShSkSmStWs
AntiCMOS.B.....[LiXi.....] 10/95 AmSbTd
AntiEXE.A.....[D3.....] 9/94 AaAkAmEwFhFpJmMhOzSmStTdWs
Boot-437.A.....[Bath.....] 3/94 JmPbWs
Burglar.1150.A.....[GranGrave.1150.] 2/96 AkPbWs
Byway.A.....[Dir2.Byway.....] 9/95 JdJmSb
Cascade.1701.A.....[1701.....] 9/93 RzSm
Die_Hard.4000.A.....[DH2, Wix.....] 1/95 AkCrIcJrPnRzShTdWs
Dir-II.A.....[Creeping Death.] 3/00 AkWs
Eco.B.....[Eco.B, Sevilla.] 3/98 FpJmXc
Empire.Monkey.A.....[Monkey.....] 7/94 FpIcOzSb
Empire.Monkey.B.....[Monkey 2.....] 7/94 EwFhFpIcJdSbSmStTdWsXc
EXE_Bug.A.....[CMOS Killer....] 9/93 EwJdWs
Form.A.....[Form 18.....] 7/94 EwFlFpJhJmJrMhMlPbRzSbSmTd
TiWsXc
Form.D.....[Form May.....] 7/94 FpRzSbSt
HLLP.Toadie.7800.A.....[Termite.7800...] 9/99 BhPnSbShSt
HLLP.Toadie.7800.B.....[Termite.7800.B.] 9/99 JdPn
J&M.A.....[Jimi,Hasita....] 6/95 MtPbSm
Jerusalem.1808.Standard.[Israeli.....] 7/93 FpWs
JS/Kak.worm.....[.....] 2/00 AmAsCrEiEwFpJhJrKbMtOzPbPn
ShTc
JS/Unicle.A.....[JS/RUNftp.....] 3/00 AaAs
Jumper.B.....[.....] 4/99 AkFp
Junkie.mp.1027.A.....[DrWhite.1027...] 7/94 AkEwFpMhOzSbStTiWsXc
Michelangelo.A.....[.....] 7/93 FlSbWs
Natas.mp.4774.....[Satan.....] 10/95 IcJdJmJrSbTdXc
NYB.A.....[B1.....] 7/94 AaAkEwFhJrMhSbSmTdTcWsXc
O97M/HalfCross.A.....[.....] 11/99 AsIcSrZb
O97M/Jerk.B.....[O97M/AllNet....] 5/99 AsEwPnSoZb
O97M/Tristate.C.....[O97/Crown.B....] 4/99 AaAcAdAkAsBhCrEiEwFhFpJhJr
KbKdLsMhMsOzPbPnPtShSkSmSt
TcXcZb
One_Half.mp.3544.A.....[Dis, Free Love.] 10/95 AaAkCrEwFlFpIcMtPbSkTdWsXc

Parity_Boot.B.....[Generic 1.....] 9/93 AkAmEwFpJdMhShSmStXc
Pieck.mp.4444.A.....[Kaczor.4444....] 6/96 CrJrMtPbXc
Ripper.....[Jack Ripper....] 3/94 AkEwFhFlFpMhMtPbSmStTdWs
Sampo.....[Turbo, Wllop...] 1/95 EwJrSmStWs
Spanska.4250.A.....[.....] 11/97 CrFhFpJmRzSbTi
Stealth_Boot.C.....[AMSE, NopB2....] 9/94 AkEwFhJd
Stoned.Angelina.....[.....] 5/95 AaJdJrMlPbShSmTd
Stoned.June_4th.A.....[Bloody!.....] 7/93 IcSm
Stoned.No_INT.A.....[Stoned.....] 9/94 AkEwWs
Stoned.Spirit.....[.....] 6/96 FpJrMsMtXc
Stoned.Standard.B.....[New Zealand....] 3/93 CrWsXc
TMC_Level-69.....[TMC.5454.....] 2/98 MtPb
VBS/BubbleBoy.A.....[VBS/BubbleBoy_1] 12/99 JhSbSh
VBS/Freelink.....[.....] 10/99 AsBhEiEwFhGbJdJhJkJmKbMtPn
SbShSmStTcTiZb
+VBS/LoveLetter.A.....[.....] 5/00 AaAdAmAsCrDpEkEwFpJdJkJmJr
KdPbRaRzShSkTcTi
VBS/Netlog.A.....[VBS/Network....] 3/00 AaJmMtSbShTc
+VBS/Tune.B.....[.....] 5/00 AsJhJm
W32/Babylonia.....[11036.....] 12/99 AaAeFpJrOzPnSbSr
W32/Beast.A.....[(W32, W97M)....] 5/99 AaAsJdKdPnShTcZb
W32/ExploreZip.....[Worm.ExploreZip] 6/99 AaAcAdAsEwFhFpGbIcJhJmKbKd
LsMlMtOzPbPnPtRfRpSbShSkSm
SrStTdTiXcZb
W32/ExploreZip.pak.....[.....] 12/99 AmAsEiEwFpJdJhKbMtOzPbPnRz
SbShSkStZb
W32/Fix2001.worm.....[.....] 2/00 AsEiEwFhFpGbJdJhJmKbKdPnRa
ShXcZb
W32/Funlove.4099.....[.....] 12/99 JhOzPn
W32/Kriz.4029.....[.....] 1/00 SkXc
W32/Mypics.worm.....[.....] 12/99 JhPnSbSh
W32/NewApt.A.....[.....] 1/00 AsJhShSk
W32/NewApt.C.....[.....] 2/00 AsSbTc
W32/NewApt.D.....[.....] 2/00 AaJhKbSh
W32/Oporto.....[Totilix.3075...] 12/99 JdPn
W32/PrettyPark.....[.....] 6/99 AaAdAsCrDpEiEwFhFpGbJdJhJm
JrKbKdMhMsMtPbPnRaShSkSmSt

TcTiXcZb
W32/Ska.A.....[HAPPY99.....] 3/99 AcAdAkAmAsBhCrDpEiEkEwFhFp
GbGmIcJdJhJkJmJrKbKdLsMhMl
MsMtOzPbPnRaRpShSkSmSrStTc
TiXcZb
W32/Winext.worm.....[TryIt.....] 2/00 AsFpJhShZb
W95/CIH.1003.....[Spacefiller....] 8/98 AaAcAdAkAmAsCrEiEwFhFlFpGb
IcJdJhJmJrKbKdLsMhMlMsMtOz
PbPnRpShSkSmSrStTiWlXcZb
W95/CIH.1019.A.....[.1019, CIH.C...] 7/98 AaEkEwFhMhSbXc
W95/Fono.....[W95/El_Inca.mp.] 12/98 FhMtPbPnXc
W95/Kenston.1895.....[.....] 5/99 AaMhPb
W95/Lovesong.998.....[.....] 3/00 SkSm
W95/Marburg.8590.....[W95/Marburg.A..] 7/98 AsEwIcMsOzRpSbSm
W97M/Astia.L.....[.....] 3/00 AsPn
W97M/Bablas.A.....[.....] 1/00 AsPn
W97M/Brenda.A.....[.....] 1/99 AsFhRzZb
W97M/Chack.B.....[.....] 3/00 AsDp
W97M/Chack.H.....[.....] 7/99 AkJmSm
W97M/Class.B.....[.....] 2/99 AaAsCrFpKbMhPnSh
W97M/Class.BV.....[W97M/Insert....] 11/99 AsShTc
W97M/Class.D.....[.....] 12/98 AcAsBhCrDpEiEwFhFpGmIcJdJh
KdMhMlMsOzPnRaRzShStTcTiXc
Zb
W97M/Class.ED.....[.....] 2/00 AsPn
W97M/Class.Q.....[.....] 12/98 AcAkAmAsCrJhMhMsOzPnRzShSt
Xc
W97M/Claud.A.....[.....] 4/00 JmSh
W97M/ColdApe.A.....[.....] 12/98 AaAcAsFhFpGbPnShSmSoTcZb
W97M/ColdApe.B.....[.....] 3/99 AdFhFpJdKbMhMsOzPnZb
W97M/Cont.A.....[.....] 11/99 AsSt
+W97M/DB.A.....[.....] 5/00 AsFp
W97M/Ded.A.....[.....] 10/99 AsKbSoSt
W97M/Ded.B.....[.....] 1/00 AsOzSh
W97M/Ded.C.....[.....] 3/00 AsRz
+W97M/Eight941.D.....[.....] 5/00 AsEwPn
W97M/Eight941.E.....[.....] 3/00 AsJhSb

W97M/Ethan.A.....[.....] 2/99 AaAcAmAsBhCrDpEiEwFhFpGbIc
JdJhJmJrKbLsMhMsMtOzPbPnRa
SbShSmSoSrStTcTiXcZb
W97M/Ethan.AT.....[.....] 10/99 AsJdPnStTcZb
W97M/Ethan.AW.....[.....] 11/99 AsJdPnShStZb
W97M/Ethan.B.....[.....] 8/99 AcAeAsCrJhMsOzSh
W97M/Ethan.BE.....[.....] 3/00 AsJm
W97M/Ethan.BI.....[.....] 3/00 AsJm
W97M/Ethan.Q.....[.....] 9/99 AsJhPnStZb
W97M/Footer.A.....[.....] 12/99 AsJhPn
W97M/Groov.A.....[.....] 7/98 AsFhJhJrKbKdPnSmTi
W97M/Groov.B.....[.....] 10/99 AsPn
W97M/Groov.C.....[.....] 11/99 AsPt
W97M/Heathen.12288.A....[.....] 10/99 IcXc
W97M/Hubad.A.....[.....] 12/99 FpJd
W97M/Jerk.A.....[.....] 2/00 AsPnTc
W97M/Locale.A.....[.....] 9/99 AaAsJdPnShStTcZb
W97M/Locale.B.....[.....] 10/99 AsPnSt
W97M/Marker.A.....[.....] 3/00 JhMs
W97M/Marker.AE.....[.....] 9/99 AsShSt
W97M/Marker.AQ.....[.....] 10/99 AsPnShSt
W97M/Marker.AR.....[.....] 10/99 ShSt
W97M/Marker.BA.....[.....] 3/00 AsSh
W97M/Marker.BJ.....[.....] 3/00 AsSt
+W97M/Marker.BN.....[.....] 5/00 AsPn
W97M/Marker.BO.....[.....] 2/00 AdAs
W97M/Marker.C.....[W97M/Spooky.C..] 4/99 AaAcAeAmAsCrDpEiEwFhFpIcJd
JhJmJrKbMhMsMtOzPnPtRaShSo
SrStTcXcZaZb
W97M/Marker.D.....[.....] 5/99 AkAsBhDpGbJhKdOzShSmTiXcZb
W97M/Marker.O.....[.....] 8/99 AsJmPnPtShSrStZb
W97M/Marker.P.....[.....] 11/99 ShStZb
W97M/Marker.Q.....[.....] 9/99 AsJdShStZb
W97M/Marker.X.....[.....] 9/99 AsPnStZb
W97M/Melissa.A-mm.....[Maillissa.....] 4/99 AaAsCrDpEiEwFhFlFpGbIcJdJh
JkJrKbKdLsMhMlMtOzPnPtRzSb
ShSkSmStTcTiXcZaZb

W97M/Melissa.AA-mm.....[.....] 12/99 OzPnSb
W97M/Melissa.AB-mm.....[.....] 12/99 JmSb
+W97M/Melissa.AL-mm.....[.....] 5/00 AsSh
W97M/Melissa.I-mm.....[.....] 7/99 AaAcAsOzPnShSt
W97M/Melissa.M-mm.....[.....] 12/99 DpPn
W97M/Melissa.O-mm.....[.....] 2/00 AsPn
W97M/Melissa.U-mm.....[.....] 11/99 FpPnShSo
W97M/Myna.B.....[.....] 1/00 AsDpSmZb
W97M/Myna.C.....[.....] 3/00 AaAsPn
W97M/Nono.A.....[Nono.....] 2/99 AsJhKbOzShSmStZb
W97M/Nottice.A.....[.....] 4/99 AaAsJhJmKbZb
W97M/Nottice.AA.....[.....] 3/00 AsSt
W97M/Nottice.D.....[.....] 5/99 AsMtXc
+W97M/NSI.B.....[.....] 5/00 AsSh
W97M/Odious.A.....[.....] 2/00 AsPn
W97M/Opey.A.....[.....] 3/00 AsRp
W97M/Opey.C.....[.....] 11/99 AsRpSm
W97M/Ozwer.F.....[.....] 9/99 IcSt
W97M/Panther.A.....[.....] 11/99 PnShSoSt
W97M/Pri.A.....[.....] 6/99 AkAsBhJkOzPnRgShSt
W97M/Pri.B.....[.....] 3/99 AcAsDpGbMhOzShSm
W97M/Pri.Q-mm.....[W97M/Prilissa.A] 11/99 AaAsEwFlFpJhPnSbSmSt
W97M/Proteced.A.....[.....] 5/99 OzSm
+W97M/Proverb.A.....[.....] 5/00 AsSh
W97M/RV.A.....[.....] 3/00 AsSt
+W97M/Smac.D.....[.....] 5/00 AsEw
W97M/Story.A.....[W97M_Jack_Box..] 8/99 AsCrDpIcJmKbMtPnShSmStTiZb
W97M/Thus.A.....[W97M/Thursday.A] 9/99 AaAmAsCrDpEiFpGbIcJdJmPbPn
RzShSmStTcXcZb
W97M/Turn.A.....[.....] 12/99 AsJmPnSh
W97M/TWNO.AC.....[.....] 3/00 AsFp
W97M/Verlor.A.....[.....] 1/00 AsDpEwStZb
W97M/Visor.A.....[.....] 3/00 AkAsCr
W97M/VMPCK1.BY.....[.....] 8/99 AsDpEwJdJmStZb
W97M/Walker.D.....[.....] 6/99 AsFhZb
W97M/Walker.E.....[.....] 6/99 AsDpShStTiZb
W97M/Wrench.C.....[.....] 2/00 PnRz

WelcomB.....[Bupt.....] 6/95 FlJrSb
WM/Appder.A.....[ntthnta.....] 5/97 EwOz
WM/CAP.A.....[.....] 5/97 AaAkAmAsCrDpEwFhFlFpIcJdJh
JmJrKbLsMhMsMtOzPbPnRpShSm
SrStTdTcXcZb
WM/Colors.A.....[Colours.....] 10/96 AsJdSm
WM/Concept.A.....[Prank Macro....] 12/96 AsBhDpEwFlIcJdJmJrKbKdMlOz
SmStTdWsZb
WM/CopyCap.A.....[.....] 7/98 AsEwKbOzStZb
WM/Demon.A.....[.....] 2/99 JmKb
WM/Johnny.A.....[Go Johnny.....] 5/96 AkIcJd
WM/MDMA.A.....[StickyKeys.....] 12/96 AsFpSbTdXcZb
WM/Niknat.A.....[.....] 12/98 JmSm
WM/Nottice.A.....[.....] 2/99 JmSm
WM/Npad.A.....[Jakarta.....] 10/96 AkAsEwFpGbJdOzRpSmTdXcZb
WM/ShowOff.A.....[.....] 9/97 EwKdZb
WM/Wazzu.A.....[Wazzu.....] 12/96 BhEwFlFpJdJhJmJrOzSmTdWsZb
WM/Wazzu.C.....[.....] 12/96 BhKbXc
WM/Wazzu.DO.....[.....] 4/98 EwFpXc
X97M/Clonar.A.....[X97M/Diablo.B..] 11/99 OzPnSh
X97M/Divi.A.....[.....] 12/99 AsCrMtPnShSt
+X97M/Divi.G.....[.....] 5/00 AmRz
X97M/Extras.A.....[.....] 12/98 AaSk
X97M/Extras.B.....[.....] 10/98 SbSm
X97M/Laroux.A.....[.....] 7/97 AaAmAsEwFlGbIcJhJrKbMlPbPn
PtSkStTdZb
+X97M/Laroux.AN.....[.....] 5/00 AsSt
X97M/Laroux.CF.....[.....] 7/99 KbKdPnPtSh
X97M/Laroux.CN.....[.....] 9/99 KdRpZb
X97M/Laroux.DO.....[.....] 6/99 JrKbKdSh
X97M/Laroux.DX.....[.....] 12/98 AkAsEwIcJdKbKdPnPtRpShStTi
Zb
X97M/Laroux.E.....[.....] 12/98 AsCrKbPnRpShZb
X97M/Laroux.EI.....[.....] 9/99 MtShZb
X97M/Laroux.FC.....[.....] 6/99 AsJmShSt
X97M/Laroux.HJ.....[Bayantel.....] 5/99 RpSt
X97M/Laroux.HO.....[.....] 5/99 KbPn

X97M/Laroux.JP.....[.....] 10/99 ShSt
X97M/Laroux.JX.....[.....] 10/99 PnSt
X97M/Manalo.E.....[.....] 12/99 FhPn
X97M/PTH.D.....[.....] 11/99 KbKdSt
X97M/VCX.A.....[.....] 4/99 KdPnSk
XF/Paix.A.....[.....] 12/98 FpMhPnSmSt
XF/Sic.A.....[.....] 4/99 KbMhPnShXc
XM/Compat.A.....[.....] 12/98 AaEwIcZb
XM/Extras.A.....[.....] 7/98 EwIcKbMlRzShSmZb
XM/Laroux.A.....[.....] 2/97 AaAmAsCrEwFpIcJdJmJrKbMlPb
SmTdZb
XM/Laroux.CF.....[.....] 6/99 KbOz
XM/Laroux.DX.....[.....] 10/99 KbShZb
XM/Laroux.E.....[.....] 10/97 KbPnZb
XM/Laroux.HO.....[.....] 12/99 KbKd
XM/Laroux.IC.....[.....] 7/99 PnPt
XM/Laroux.JO.....[.....] 1/00 StTc
Yankee_Doodle.2881.A....[Yankee.2C.A....] 9/93 AkEkEwSm

==========

Total for the WildList: 204

==========

Supplemental List

==========

As was noted at the start of the main list, this list is not technically part of "The WildList", as originally defined. By design, the WildList is a list of viruses verified as being in the wild by a minimum of two WildList participants. The viruses listed below do not currently meet that criteria.

This additional list includes viruses reported by a single participant and are often either moving onto the main list, or dropping off of it.

Please note especially that this list also tends to be more of a regional reporting mechanism. For example, a virus is often reported as very common by one regional participant, but is found nowhere else in the world.

Viruses marked with a minus sign (-) dropped from the main list this month. Viruses marked with a plus sign (+) are new to the supplemental list this month.

Name of Virus	[Alias(es)]	List Date	Reported by:
Badass.Worm	[.....]	11/99	Sh
Barrotes.1310.A	[Barrotos.....]	1/99	Fp
Bleah.C	[.....]	3/98	Fp
Bye	[ByeBye.....]	1/99	Ls
-Cascade.1704.A	[1704.....]	7/93	Ew
Chimp.A	[.....]	11/99	Ew
Clonewar.cmp.923	[.....]	12/99	Sh
Crazy_Boot	[.....]	5/95	Sb
Cruel.A	[.....]	2/98	Rz
DelCMOS.B	[Int7F-E9, Feint]	1/99	Jm
DelWin.mp.1759.A	[Goblin.1759....]	6/95	Ti
DNA.1206	[.....]	8/99	St
Dodgy	[.....]	10/97	Cr
Flip.mp.2153.A	[Omicron.....]	7/93	Fp
Frodo.4096.A	[4096.....]	7/93	Ew
Ghost_II.792	[.....]	9/99	Sh
Helloween.1376.A	[1376.....]	7/93	Ws
Helloween.1839.A	[.....]	9/99	Kd
HLLP.5850.D	[Weed.....]	7/99	Fh
HLLP.7776	[.....]	11/99	Sh

HLLP.Toadie.9100.....[.....] 12/99 Pn
HLLW.DMSetup.....[.....] 12/99 Sh
Invader.2164.....[TPE 1.4.....] 9/99 Sh
J&M.B.....[.....] 2/99 Mt
Jerusalem.1364.A.....[Mummy.1364.....] 9/99 Sh
Joshi.A.....[.....] 3/00 Sk
Kampana.mp.A.....[AntiTel.....] 7/93 Jd
Kiev.1942.....[KVS.1942.....] 2/99 Ak
Leandro.....[TimeWarp.....] 9/99 Kd
Little_Red.1465.A.....[.....] 10/99 Sh
Lokky.336.....[LadyJ.....] 2/00 Sh
-Major.1644.A.....[Major BBS.....] 6/96 Pb
Maltese_Amoeba.2365.....[Grain of Sand..] 7/93 Ws
Neuroquila.mp.4544.A....[Havoc, Wedding.] 1/99 Ws
Nightfall.4518.....[N8Fal.....] 2/96 Pb
NRLG.700.A.....[.....] 1/00 Jh
O97M/HalfCross.C.....[.....] 12/99 Rz
O97M/Hopper.R.....[.....] 1/00 As
+O97M/Hopper.X.....[.....] 5/00 Rz
O97M/Tristate.A.....[.....] 5/99 Sr
O97M/Tristate.AA.....[.....] 6/99 Oz
O97M/Tristate.AB.....[.....] 7/99 Cr
O97M/Tristate.B.....[.....] 11/99 Fh
O97M/Tristate.BJ.....[.....] 12/99 Ae
O97M/Tristate.BR.....[.....] 11/99 Sh
O97M/Tristate.BU.....[.....] 1/00 Rz
O97M/Tristate.D.....[.....] 4/99 Pn
O97M/Tristate.F.....[.....] 4/99 Jd
O97M/Tristate.Y.....[.....] 6/99 Oz
-One_Half.mp.3577.....[.....] 2/99 Mt
Persefone.....[Pers.....] 9/99 Ra
Quandary.....[Parity_Boot.Enc] 3/96 Ak
Quox.A.....[Stealth 2.....] 9/99 Kd
W97M/Class.EJ.....[W97M/Trigram.A.] 7/99 St
RP.A.....[Rhubarb, PR.b..] 2/97 Cr
Stoned.Crypt.....[Bleah.E.....] 3/00 Ms
Stoned.W-Boot.....[Wonka.....] 12/93 Ws

-Tai-Pan.438.A.....[Whisper.....] 1/95 Ek
-Tequila.mp.2468.A.....[.....] 7/93 Ws
TMC_Level-42.....[.....] 2/99 Mt
TPE.Girafe.3005.....[.....] 3/00 Sh
-TPVO.mp.3783.A.....[TVPO, 3873.....] 10/96 Ic
-Tremor.4000.A.....[.....] 7/93 Ws
Unashamed.B.....[.....] 10/95 Jr
Urkel.....[Nwait.....] 1/99 Ws
-V-Sign.....[Cansu, Sigalit.] 3/00 Ak
VBS/Bhong.worm.....[.....] 2/00 Pn
VBS/BubbleBoy.B.....[VBS/BubbleBoy_2] 12/99 Jh
VBS/Fool.B.....[.....] 2/00 Pn
VBS/Fool.D.....[.....] 3/00 Jh
VBS/Happy.....[.....] 10/99 Sh
+VBS/Irok.A.....[.....] 5/00 Pb
VBS/Tune.A.....[.....] 1/00 Jh
VrapExe.3730.....[XRF.3730, 3730.] 3/98 Fp
W32/AntiQFX.....[AntiQFX.114688.] 3/00 Sh
W32/Badby.....[.....] 9/99 Pn
W32/Beast.B.....[(W97M, W32)....] 10/99 Sh
W32/Bolzano.3223.....[Bolzano.L.....] 1/00 Pb
W32/Crypto.....[.....] 1/00 Jh
W32/HLLP.Backdoor-Yai...[.....] 1/00 Aa
W32/HLLP.DeTroie.A.....[W32/Cheval.TCV.] 11/98 Fp
W32/Kezdett.644.....[.....] 3/00 Sh
W32/Kriz.3863.A.....[.....] 9/99 Pn
W32/Kriz.4050.....[.....] 12/99 Pn
W32/Kriz.4092.....[.....] 12/99 Pn
W32/Maya.....[W32/Maya.4153..] 5/99 Gb
W32/Melting.....[Melting.17920..] 4/00 Sh
W32/White.A.....[.....] 3/00 Jh
W95/Anxiety.1358.....[Poppy.....] 11/97 Fp
W95/Anxiety.1823.....[W95/Anxiety.B..] 4/98 Fp
W95/CIH.1024.....[.....] 3/99 Jm
W95/HPS.5124.....[WIN95/HPS.....] 11/98 Fp
W95/K32.3030.....[W95/Hazlo.....] 5/99 Sb
W95/Lizard.2381.....[.....] 11/99 Sh

W95/Lord.....[.....] 6/99 Xc
W95/MiniR3.431.....[W32/Gift.worm.b] 12/99 Sh
W95/Padania.....[.....] 2/00 As
+W95/Plage.....[HLLW.Plage.....] 5/00 As
W95/Spaces.1245.....[.....] 5/99 Mh
W95/Tip.2475.....[W95/Tip.A.....] 12/99 Cr
W97M/Antimarc.A.....[.....] 11/99 As
-W97M/Appder.A.....[.....] 7/97 Jm
W97M/Appder.Q.....[.....] 1/00 As
W97M/Appder.W.....[.....] 9/99 Ak
W97M/Arbeit.A.....[.....] 9/99 Pn
W97M/Argh.B.....[.....] 5/99 Mh
W97M/Armagidon.A.....[.....] 1/00 Aa
W97M/Assilem.A.....[.....] 1/00 As
W97M/Astia.A.....[.....] 1/00 Sm
W97M/Astia.B.....[.....] 6/99 Pn
W97M/Astia.C.....[.....] 1/00 As
+W97M/Astia.U.....[.....] 5/00 As
W97M/Astia.Y.....[W97M/BMH.....] 12/99 Ae
W97M/Bablas.K.....[.....] 3/00 As
W97M/Backhand.A.....[.....] 1/00 Jh
W97M/Bribagi.A.....[.....] 2/00 Sm
W97M/Caligula.A.....[.....] 4/99 Fp
W97M/Chack.AL.....[W97M/Jiuster.A.] 12/99 Jm
W97M/Chack.AP.....[.....] 3/00 As
W97M/Chack.BD.....[.....] 1/00 Rz
+W97M/Chack.BR.....[.....] 5/00 Rz
+W97M/Chack.K.....[.....] 5/00 As
W97M/Chantal.B.....[.....] 1/00 Aa
W97M/Class.A.....[.....] 12/99 Jh
W97M/Class.AY.....[.....] 10/99 Sh
W97M/Class.BZ.....[.....] 8/99 St
W97M/Class.CN.....[.....] 4/99 Ic
W97M/Class.CO.....[.....] 10/99 Sh
W97M/Class.CP.....[W97M/BlackviruZ] 7/99 Jm
W97M/Class.DZ.....[W97M/Claet.A...] 12/99 Rz
W97M/Class.EE.....[W97M/Mixture.A.] 12/99 Rz

W97M/Class.EH.....[.....] 1/00 Rz
W97M/Class.EI.....[.....] 1/00 Rz
W97M/ColdApe.H.....[.....] 6/99 Oz
W97M/ColdApe.I.....[.....] 6/99 Oz
W97M/ColdApe.O.....[.....] 10/99 St
+W97M/Dariem.A.....[.....] 5/00 Jm
+W97M/Eight941.F.....[.....] 5/00 Rz
W97M/Ephan.A.....[.....] 8/99 St
W97M/Ephan.B.....[.....] 1/00 Rz
W97M/Ethan.AB.....[.....] 9/99 St
W97M/Ethan.AC.....[.....] 11/99 Tc
W97M/Ethan.AK.....[.....] 2/00 As
W97M/Ethan.AL.....[.....] 9/99 St
W97M/Ethan.BA.....[.....] 2/00 St
W97M/Ethan.BB.....[.....] 11/99 So
W97M/Ethan.BC.....[.....] 3/00 As
W97M/Ethan.BN.....[.....] 1/00 Rz
W97M/Ethan.BR.....[.....] 2/00 As
W97M/Ethan.BW.....[.....] 2/00 As
+W97M/Ethan.CC.....[.....] 5/00 As
W97M/Ethan.D.....[.....] 3/00 Ak
W97M/Ethan.G.....[.....] 6/99 Oz
W97M/Ethan.J.....[.....] 7/99 Cr
W97M/Ethan.L.....[.....] 6/99 Oz
W97M/Ethan.P.....[.....] 2/00 As
W97M/Ethan.U.....[.....] 10/99 As
W97M/Ethan.V.....[.....] 3/00 As
W97M/Evolution.B.....[.....] 2/00 Pn
W97M/FF.A.....[W97M/Lys.H.....] 11/99 As
W97M/Footer.E.....[.....] 6/99 St
W97M/Footer.G.....[.....] 8/99 St
W97M/Footer.H.....[.....] 3/00 As
W97M/Footer.N.....[.....] 1/00 Rz
W97M/Galero.A.....[.....] 3/00 As
W97M/Gamlet.A.....[.....] 9/99 St
W97M/Groov.D.....[.....] 7/99 St
W97M/Groov.I.....[.....] 6/99 Oz

W97M/Groov.T.....[.....] 4/00 Sh
W97M/Hope.A.....[.....] 2/00 As
W97M/Hope.P.....[.....] 3/00 As
W97M/Idea.A.....[.....] 9/99 Jm
W97M/IIS.D.....[.....] 8/99 Ic
W97M/IIS.L.....[.....] 2/00 As
W97M/Iseng.A.....[.....] 1/00 As
W97M/JB.....[W97M/JB.A.....] 10/99 Pn
+W97M/Jerk.C.....[.....] 5/00 Rz
+W97M/Jim.C@mm.....[.....] 5/00 As
W97M/Locale.C.....[.....] 11/99 St
W97M/Lucia.A-mm.....[.....] 1/00 Kb
W97M/Lulung.F.....[.....] 1/00 As
W97M/Marker.AF.....[.....] 2/00 St
+W97M/Marker.AG.....[.....] 5/00 As
W97M/Marker.AL.....[.....] 9/99 Rz
W97M/Marker.AN.....[.....] 11/99 St
W97M/Marker.AV.....[.....] 11/99 St
W97M/Marker.AW.....[.....] 11/99 St
W97M/Marker.AX.....[.....] 11/99 St
W97M/Marker.AZ.....[.....] 2/00 As
W97M/Marker.BG.....[.....] 1/00 St
W97M/Marker.BP.....[.....] 1/00 Rz
W97M/Marker.BQ.....[.....] 1/00 Rz
W97M/Marker.BT.....[.....] 3/00 As
W97M/Marker.BU.....[.....] 2/00 St
+W97M/Marker.BX.....[.....] 5/00 As
W97M/Marker.BY.....[.....] 3/00 As
W97M/Marker.CC.....[.....] 2/00 Rz
W97M/Marker.CD.....[.....] 2/00 Rz
W97M/Marker.CI.....[.....] 3/00 As
+W97M/Marker.CQ.....[.....] 5/00 As
W97M/Marker.CX.....[.....] 4/00 Sh
W97M/Marker.J.....[.....] 3/00 As
W97M/Marker.N.....[.....] 2/00 As
W97M/Marker.W.....[.....] 11/99 Tc
W97M/MDMA.D.....[.....] 1/99 Jm

W97M/MDMA.K.....[.....] 3/00 As
W97M/Melissa.AD-mm.....[.....] 2/00 Pn
W97M/Melissa.AK-mm.....[.....] 2/00 As
W97M/Melissa.AU-mm.....[.....] 4/00 Jm
W97M/Melissa.B-mm.....[.....] 6/99 Oz
W97M/Melissa.V-mm.....[.....] 10/99 Pn
W97M/Model.A.....[.....] 2/00 As
W97M/Myna.D.....[.....] 2/00 Jh
+W97M/Myna.J.....[.....] 5/00 Rz
W97M/Nid.A.....[.....] 3/00 As
W97M/Nottice.H.....[.....] 3/00 As
W97M/Nottice.I.....[.....] 11/99 Sh
W97M/Odious.B.....[.....] 12/99 Kb
W97M/Opey.D.....[.....] 4/99 Rp
W97M/Opey.E.....[.....] 3/00 As
W97M/Opey.G.....[.....] 11/99 As
W97M/Opey.H.....[.....] 10/99 St
W97M/Opey.M.....[.....] 3/00 As
W97M/Opey.N.....[.....] 2/00 Pn
W97M/Osm.A.....[.....] 9/99 Ac
W97M/Ozwer.B.....[.....] 9/99 St
W97M/Panther.D.....[.....] 2/00 St
+W97M/Panther.H.....[.....] 5/00 Rz
W97M/PassBox.B.....[.....] 2/00 Pn
W97M/PassBox.E.....[.....] 12/99 Ae
W97M/Passbox.I.....[.....] 1/00 As
W97M/Ping.B-mm.....[.....] 3/00 As
W97M/Pri.E.....[.....] 7/99 St
W97M/Pri.I.....[.....] 3/00 As
W97M/Pri.M.....[.....] 3/00 As
W97M/Proteced.G.....[.....] 12/99 Oz
+W97M/Proverb.C.....[.....] 5/00 Rz
W97M/Seke.A.....[.....] 4/00 Jm
+W97M/Seliuq.B.....[.....] 5/00 Jm
W97M/Seqnum.A.....[.....] 2/00 Pn
W97M/Shepmah.A.....[.....] 3/00 As
W97M/Shiver.C.....[.....] 3/99 Sm

W97M/Solafish.A.....[.....] 1/00 As
W97M/Story.B.....[.....] 9/99 Rz
W97M/Story.E.....[.....] 3/00 As
W97M/Stun.A.....[.....] 2/00 As
W97M/Surround.A.....[.....] 1/00 St
+W97M/Talon.R.....[.....] 5/00 Rz
W97M/Taro.A.....[.....] 3/00 Sm
W97M/Temple.A.....[.....] 1/00 As
W97M/Thus.B.....[.....] 3/00 As
W97M/Thus.C.....[.....] 3/00 As
W97M/Thus.D.....[.....] 3/00 As
W97M/Thus.E.....[.....] 3/00 As
+W97M/Thus.G.....[.....] 5/00 As
W97M/Thus.H.....[.....] 3/00 As
W97M/Thus.I.....[.....] 3/00 As
W97M/Thus.J.....[.....] 3/00 Sb
+W97M/Thus.Q.....[.....] 5/00 As
W97M/Tie.T.....[.....] 5/99 Aa
W97M/Titch.A.....[.....] 1/00 As
+W97M/Titch.D.....[.....] 5/00 As
W97M/Uka.D.....[.....] 9/99 Jm
W97M/Vale.A-mm.....[.....] 2/00 Pn
W97M/Venus.A-mm.....[.....] 12/99 Rz
W97M/VMPCK1.BG.....[.....] 12/99 Ae
W97M/VMPCK1.DD.....[.....] 2/00 As
W97M/Vp.A.....[.....] 7/99 Jm
W97M/Wazzu.A.....[.....] 5/97 Cs
+W97M/Wrench.E.....[.....] 5/00 As
Wafer.1953.....[.....] 3/00 Sb
Win/Najemnik.9000.....[Pawel.9000.....] 3/00 Ms
Win/Tentacle.1944.....[.....] 5/96 Rz
WM/Cap.AT.....[.....] 7/99 St
WM/Concept.BB.....[.....] 9/99 Sh
-WM/Divina.A.....[Infeczione.....] 12/96 Ew
WM/DZT.A.....[.....] 2/99 Ak
WM/Helper.B.....[.....] 7/97 Xc
WM/Imposter.E.....[.....] 4/99 Kb

WM/Inexist.A:Fr.....[WM/Warning.....] 2/99 Fp
WM/Johnny.B.....[.....] 12/98 Jm
WM/Mental.A.....[.....] 12/99 Kb
WM/Muck.R.....[.....] 1/00 Kb
WM/Niceday.N.....[.....] 12/98 Kb
WM/Pesan.B.....[.....] 10/97 Jd
WM/ShowOff.C.....[.....] 9/99 Sh
WM/Stall.A.....[.....] 11/98 Fp
WM/Stall.C.....[.....] 12/99 Ae
WM/Switcher.A.....[.....] 12/97 Ew
WM/Swlabs.B.....[.....] 10/97 Jm
WM/Swlabs.G.....[.....] 12/97 Fp
WM/Temple.R.....[.....] 7/98 Rz
WM/TWNO.A:Tw.....[Taiwan_No. 1...] 12/96 Ic
WM/TWNO.AC.....[.....] 8/98 Fp
WM/Veneno.D:Es.....[WM/Cap.GV.....] 10/98 Rz
WM/Wazzu.DV.....[.....] 4/98 Fp
WM/Wazzu.EC.....[.....] 4/98 Fp
X97M/Beliers.A.....[.....] 12/99 Kb
X97M/Button.A.....[.....] 11/99 St
X97M/Divi.B.....[.....] 3/00 Sm
+X97M/Divi.D.....[.....] 5/00 As
+X97M/Divi.G.....[.....] 5/00 Am
X97M/Extras.M.....[.....] 1/00 As
X97M/Friend.B.....[.....] 7/99 St
X97M/Hongo.C.....[.....] 2/00 Pn
X97M/Laroux.AA.....[.....] 6/99 Oz
+X97M/Laroux.AE.....[.....] 5/00 As
+X97M/Laroux.BP.....[.....] 5/00 As
X97M/Laroux.CG.....[.....] 11/98 Xc
X97M/Laroux.D.....[.....] 12/98 Cr
X97M/Laroux.DI.....[.....] 7/98 Rz
X97M/Laroux.DK.....[.....] 6/99 Xc
X97M/Laroux.EL.....[X97M/Massage...] 7/99 Aa
X97M/Laroux.FE.....[.....] 10/99 St
X97M/Laroux.GJ.....[.....] 4/99 Kb
X97M/Laroux.GV.....[.....] 5/99 Kb

X97M/Laroux.GW.....[.....] 6/99 St
X97M/Laroux.HZ.....[.....] 7/99 St
X97M/Laroux.IC.....[.....] 12/99 Kd
X97M/Laroux.JH.....[.....] 8/99 St
X97M/Laroux.JM.....[.....] 9/99 St
X97M/Laroux.JY.....[.....] 2/00 St
X97M/Laroux.KS.....[X97M/Laroux.CS.] 9/99 Sh
X97M/Laroux.KU.....[Majoduck.....] 3/00 Mt
X97M/Laroux.LN.....[.....] 1/00 St
X97M/Laroux.LX.....[.....] 2/00 St
+X97M/Laroux.MU.....[.....] 5/00 Rz
+X97M/Laroux.MV.....[.....] 5/00 Rz
X97M/Manalo.D.....[.....] 10/99 Pn
X97M/PTH.F.....[.....] 2/00 As
X97M/Smack.A.....[.....] 7/99 St
X97M/Sugar.A.....[.....] 3/00 Sk
X97M/VCX.B.....[.....] 9/99 St
X97M/VCX.G.....[.....] 9/99 Rz
XM/Extras.B.....[.....] 9/98 Ew
XM/Laroux.AJ.....[.....] 11/99 Tc
XM/Laroux.AN.....[.....] 9/99 Kd
XM/Laroux.D.....[.....] 9/97 Jd
XM/Laroux.DO.....[.....] 10/99 Kb
XM/Laroux.EO.....[.....] 4/99 Jd
XM/Laroux.FC.....[.....] 12/98 Ew
XM/Laroux.JM.....[.....] 9/99 Pt
XM/Laroux.JP.....[.....] 10/99 Sh
XM/Laroux.KS.....[XM/Laroux.CS...] 9/99 Sh
XM/Manalo.E.....[.....] 11/99 St
XM/PTH.F.....[.....] 11/99 Sb
XM/VCX.A.....[.....] 1/99 Sm

==========

Total for both lists: 551

==========

Other

==========

The WildList is a list of viruses that have been reported as spreading In the Wild. Sometimes WLO receives reports of programs which, according to the various reporters, may not fit strictly into the viral category, but which have been brought to their attention by concerned users. The following programs fall into that category.

Name of Virus	List [Alias(es)]	Reported Date	by:
BackOrifice_2000	[.....]	11/99	EkPnSkStXc
DUNpws.W.Trojan	[Kuang.C, Winskc]	9/99	AkTc
ICQ2000.RAS.Trojan	[ICQ2K.....]	11/99	Sh
MAC/AutoStart.Worm	[.....]	11/99	GbEwSm
Stealth.Backdoor	[.....]	10/99	Ek
SubSeven.Backdoor	[Backdoor-G.....]	7/99	AcAsJhPnSkSoTc

==========

==========

WildList Sorted by Frequency

==========

This is not a prevalence table. It does not show how common each virus

is. Rather it is the WildList sorted by the number of participants that report each virus.

This section gives the names, types, and aliases of the most frequently reported viruses. These viruses have been reported by at least 15 WildList participants. They are sorted with the most frequently reported first.

Freq	Name	Type	Aliases
42	W32/Ska.A	File	HAPPY99
38	W95/CIH.1003	File	Spacefiller
36	W97M/Ethan.A	Macro	
35	W97M/Melissa.A-mm	Macro	Maillissa
32	W32/ExploreZip	File	Worm.ExploreZip
32	W97M/Marker.C	Macro	W97M/Spooky.C
32	WM/CAP.A	Macro	
30	W32/PrettyPark.A	File	
29	O97M/Tristate.C	Macro	O97/Crown.B
27	W97M/Class.D	Macro	
20	VBS/Freelink	File	
20	W97M/Thus.A	Macro	W97M/Thursday.A
19	AntiCMOS.A	Boot	Lenart
18	W32/ExploreZip.pak	File	
18	WM/Concept.A	Macro	Prank Macro
18	X97M/Laroux.A	Macro	
16	Form.A	Boot	Form 18
16	W32/Fix2001.worm	File	
16	XM/Laroux.A	Macro	
15	JS/Kak.worm	File	

Release notes for the May WildList:

==========

The WildList is collated by board members of WildList Organization International.

A complete archive of WildLists is available at the WildList Organization web site (http://www.wildlist.org/WildList/wildlist.html)

The WildList Organization International and WildList reporters make a diligent effort to ensure the accuracy of the data presented in the WildList. However, The WildList Organization makes no warranty against the accuracy of the information presented herein. The WildList Organization and WildList reporters cannot be held liable for any loss, or damages incurred from the use of WildList information.

Press, print media & other queries about WildList Organization International should be sent to Sarah Gordon, WildList Organization's primary media contact, at info@wildlist.org.

==========

WildList Vol.A05 - (c) 1993-2000 Joe Wells - info@wildlist.org

==========

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.7

mQCNAy+wAnYAAAEEAO2alE3YclXZAxkqrSVXkhAuuOsx6NnVfUdKMghYtrBabFuJ
+zKiIsahmjeakA2J101KZOHtKMhb5iqLG0oCbRyuBFLtuMhJrjk+L9VRCoxoDB/4

XwFevOGyxRHYfancrIydlMUooe7TZJqbGhhQEROWYm8v6RvkPFtsMpyD+Lb1AAUR
tCNKb2UgV2VsbHMgPGMxandlbGxzQHdhdHNvbi5pYm0uY29tPg==
=aKXf
-----END PGP PUBLIC KEY BLOCK-----

==========