



UNIVERSITY OF OREGON
APPLIED INFORMATION MANAGEMENT

Presented to the Interdisciplinary
Studies Program:
Applied Information Management
and the Graduate School of the
University of Oregon
in partial fulfillment of the
requirement for the degree of
Master of Science

Fundamental Practices for Security of Information Assets In the Small to Medium Sized Organization

CAPSTONE REPORT

**Roger Sample
Technology And Information Management
Portland VA Medical Center**

University of Oregon
Applied Information
Management
Program

March 2004

722 SW Second Avenue
Suite 230
Portland, OR 97204
(800) 824-2714

Approved by

Dr. Linda F. Ettinger
Academic Director, AIM Program

Abstract**For****Fundamental Practices for Security of Information Assets
In the Small to Medium Sized Organization**

Securing information assets is not a one-time activity, but involves continuous risk assessment. This study identifies practices for managers in small to medium sized organizations who need to establish minimum security levels. Selected literature published from 1998 to 2003 was analyzed to identify common practices. Findings are presented in a set of eighteen practices, aligned with Allen's five basic steps of Harden/Secure, Prepare, Detect, Respond, Improve (2000), and categorized as strategic or operational in nature.

Table Of Contents

Chapter I – Purpose of the Study	
Brief Purpose	1
Full Purpose	2
Definitions	6
Significance	7
Limitations	10
Problem Area	11
Chapter II – Review of Reverences	14
Chapter III – Method	22
Data Collection	22
Data Analysis	23
Data Presentation	25
Chapter IV – Analysis of Data	27
Chapter V – Conclusions	29
Fundamental Practices	31
Explanation of Fundamental Practices	32
References	36
Appendix A	41
Appendix B	42
Appendix C	43
Appendix D	45
Appendix E	46

Chapter I. Purpose of the Study

Brief Purpose

The purpose of this study is to provide a set of ‘fundamental practices’ for protecting the networked information assets of small to medium sized organizations. Fundamental practices are defined as those practices that are identified on a recurring basis in the literature as necessary or very important for the security of networked information assets. Networked information assets are defined by ITTS at Stanford University (Stanford 2003) as academic and intellectual capital, proprietary business management and financial data, personally identifiable health information, and personally identifiable customer or consumer data. These recommended practices address the three basic information security concepts of confidentiality, integrity, and availability as identified by the Software Engineering Institute (CERT® 2002).

The notion of “small to medium sized organization” is defined as any organization that does not have full-time information security officers or specialized security personnel. In such cases, the responsibility for protecting information most often falls to either the general management staff or IT staff who do not have specific security training. (ISA 2002) In some cases, management will resort to using outside consultants to handle security issues and there is a need for management to better understand the basics of what is really needed as opposed to just accepting what consultants want to sell (Allen 2002).

A literature review (Creswell 2003), focusing on information security, is conducted to identify the fundamental practices, through which, the three basic

information security concepts listed above (confidentiality, integrity, and availability) are being currently used to protect networked information assets. Because three major milestones in the evolution of the entire concept of “Networked Information” have occurred since 1988 (Zakon 2000), this study focuses on literature published since 1988. Rather than focusing on specific technologies for specific threats, content analysis (Krippendorf 1980, Leedy and Ormrod 2000, Palmquist 2001) of selected literature focuses on practices that can be effective as preventative measures against the compromise of networked information assets.

The results of the content analysis are presented in the form of a series of five tables of fundamental practices that are grouped in five top-level categories of Hardening/Securing, Preparing, Detecting, Responding, and Improving (Allen 2001) to address the three core concepts of confidentiality, integrity, and availability. These five categories represent a top-level depiction of how to secure and protect information assets. The Prepare, Detect, Respond, and Improve steps assume that the Harden/Secure steps have already been implemented and provide further guidance regarding what to do when something suspicious, unexpected or unusual occurs. It is intended that this will provide managers with a quick and concise way to evaluate the current condition and needed additions to their security policies, procedures, and practices (CERT® 2002).

Full Purpose

Nearly every week there are reports in the media of new computer crimes, malicious code based attacks, system break-ins or other disruptions to the security of information located on networked computer systems. At the same time, more information

is located on networked systems because it is more valuable to the companies that control the information if more employees and customers have authorized access to it. The result is that more information is vulnerable. Also there are increasing numbers of laws protecting information for which companies are liable. Examples include the Gramm-Leach-Bliley Act (1999), the HIPAA act (Health Information Portability and Accountability Act (1996) and California Senate bill SB1386 (2002).

Because it is so important, in many larger businesses, entire departments that are separate from and have different goals than the normal system administration staff often manage security. The purpose of this study is to provide a set of 'fundamental practices' for protecting the networked information assets of small to medium sized organizations. Many small to medium sized organizations do not have full-time information security officers or specialized security personnel to deal with such threats (INSTAT/MDR 2003). In such cases, the responsibility for protecting information most often falls to either the general management staff or IT staff that does not have specific security training (ISA 2002). In some cases, management will resort to using outside consultants to handle security issues and there is a need for management to better understand the basics of what is really needed as opposed to just accepting what consultants want to sell (Allen 2002). In smaller firms, the same staff often performs both the systems administration tasks and the information security tasks. The basic dichotomy here, identified by Johansson (2004), is that normally, system administration's goal is to make information and services available to everyone as needed, while security's goal is to restrict access to information and services unless the access is authorized. There is also a trend in recent legislation to push the fiduciary responsibility for information security further up the management

ladder to the executive management staff who may have neither system administration nor security experience (Rasmussen 2003).

In order to collect pertinent literature, searches for the initial key terms of ‘Information Security’, ‘Network Security’, ‘Computer Network Security Risks’, and ‘Network Survivability’ were done using the University of Oregon library web site, LexisNexis Academic, FirstSearch and Google. Sources include web sites, articles, white papers, and books. Thirty-two of the collected resources were selected for use in this study.

Content analysis as described by Leedy and Ormrod (2001) was used to examine the contents of the literature. More specifically, Conceptual Analysis (CSU 2003) as defined in the CSU writing guide was used to identify those articles whose ‘theme’ (CSU 2003) aligned with the initial search terms of ‘Information Security’, ‘Network Security’, ‘Computer Network Security Risks’, and ‘Network Survivability’. Additional themes were also identified as ‘Information Confidentiality’, ‘Information Integrity’, ‘Information Availability’, ‘Information Security Policies’, ‘Information Security Procedures’, and ‘Information Security Practices’. Repetitions of similar practices were then identified to develop the set of fundamental practices. The results are presented in a clear and concise manner with a minimum of technological jargon, enabling the organization without highly technical personnel to understand the foundational needs to protect the information in their system. The data is presented in a series of tables in which the fundamental practices are identified as either strategic or operational and are grouped according to Allen’s (2001) five steps of Hardening/Securing, Preparing, Detecting, Responding, and Improving. These steps represent a top-level depiction of how to secure

and protect information assets. The Prepare, Detect, Respond, and Improve steps assume that the Harden/Secure initial steps of software and hardware configuration have already been implemented and provide further guidance about what to do when something suspicious, unexpected or unusual occurs. *Hardening/Securing* refers to the initial configuration of software and hardware in a system and the relationship or architecture of how the different elements of the system are interconnected. In a sense, hardening attempts to solve known problems by applying known solutions (Allen 2001). *Preparing* hinges on the philosophy that there exists a collection of vulnerabilities yet to be identified and is the process of knowing how a system operates in a production setting to aid in the identification of new vulnerabilities or problems (Allen 2001). *Detecting* is the process of monitoring the transactions of particular assets and investigating unexpected or suspicious behavior (Allen 2001). *Responding* refers to the processes for identifying the damage caused by an intrusion or disruption, and containing that effect as much as possible. It also includes preventing future intruder access and returning information assets to a known operational state (Allen 2001). *Improving* actions typically occur following a detection or response activity and include changes to initial configurations, tools, and processes. In a sense, Improvement is the revisiting of the Hardening/Securing to reflect newly acquired knowledge about possible vulnerabilities (Allen 2001).

Additionally, each practice is associated with one or more of the specific security concepts identified by the Software Engineering Institute (CERT® 2002) of confidentiality, integrity, and availability. It is intended that this will provide management, particularly of those businesses that that operate in a LAN environment with Internet connectivity, and which are small enough to not have full-time personnel

devoted to information security, with a quick and concise way to evaluate the current condition and needed additions to their security policies, procedures, and practices.

Stakeholders are management professionals in organizations that have internal local area networks (LANs) with connections to the World Wide Web and that are not large enough to have full time professional security personnel guarding their information assets (INSTAT/MDR 2003).

Definitions

Fundamental Practices	Practical actions, which are of central importance, serving as a generating force (Merriam-Webster 2004).
Gramm-Leach-Bliley Act	Passed in 1999 by the US Congress, this bill states that firms must ensure the security and confidentiality of customer records and information, protect against any anticipated threats or hazards to the security or integrity of such records, and protect against any unauthorized access to or use of such records (FTC 2004).
HIPAA	Health Information Portability and Accountability Act (1996) (HHS 2004).
Information Availability	Ensuring that authorized users have access to information and associated assets when required (BSI).
Information Confidentiality	The concept of protecting information from unauthorized access. In practice, only authorized users should be allowed access to specific data or resources (ITsecurity).
Information Integrity	Safeguarding the accuracy and completeness of information and processing methods (BSI). More properly called 'data integrity', it is the property that the data in question has not been changed. Maintaining demonstrable data integrity is one of the cardinal aims of data security. It is particularly important that integrity and confidentiality be combined, so that sensitive information can be neither altered without being read, nor read without being altered. Data whose integrity has failed is said to be corrupted (ITsecurity).
Networked Information Assets	Academic and intellectual capital, proprietary business management and financial data, personally identifiable health information, and personally identifiable customer or consumer data (Stanford 2003).
SB1386 (2002)	The California Security Breach Information Act, mandates a disclosure requirement if any customer's personal electronic data has been obtained without authorization. (FTC 2004). Provides strict requirements for notification of consumers

	following any breach of unencrypted personal data. This includes any combination of an individual's name and such data as credit cards, social security numbers, driver's license number, and other information (FTC 2004).
Security Policy	Organization-level rules governing acceptable use of computing resources, security practices, and operational procedures (BSI) the security policy is the collection of rules that define an organization's security objectives and how those objectives are to be achieved. It is sometimes said that the security policy should be divided into two parts: issue policy and functional policy. The issue policy is required to specify the organization's areas of concern, and its attitude towards them. The functional policy defines the mechanics of how those concerns are to be satisfied. This requires hardware and software specifications and usage policies, and also staff behavioral policies. The security policy must also be clearly and fully documented and enforced. For example, the policy's First Rule could be "Failure to comply with the Corporate Security Policy is a disciplinary offence". (ITsecurity) A policy is a documented high-level plan for organization-wide computer and information security. It provides a framework for making specific decisions, such as which defense mechanisms to use and how to configure services, and is the basis for developing secure programming guidelines and procedures for users and system administrators to follow. Because a security policy is a long-term document, the contents avoid technology-specific issues (Dekker).
Security Practices	Practical steps system administrators and security personnel can take to protect against security compromises (CERT).
Security Procedures	Procedures are sets of specific practices to follow that are based on the computer security policy. Procedures address such topics as retrieving programs from the network, connecting to the site's system from home or while traveling, using encryption, authentication for issuing accounts, configuration, and monitoring (Dekker).
Small to medium sized organizations	Businesses that are not large enough to have dedicated information security personnel.

Significance

The need for such a study can be explained with an example. One of the first significant computer break-ins, the Morris Worm, occurred in November 1988. In this case, a program inadvertently used a method that has come to be described as a Buffer Overflow. This method presented the code in a program with more data than it could handle, allowing the incoming data to destroy or replace code of the host system. (Rogers 2002) It seems that little has changed in the past sixteen years. In the months of April and May of 2002, 69 alerts and advisories issued by the Cert® Coordination Center at the Software Engineering Institute describe Buffer Overflows in common computer and network software. (SSI, 2002) In 2003 over 15 percent of the vulnerability bulletins issued by the Department of Energy's Computer Incident Advisory Capability were for various Buffer Overflows (USDE 2003).

According to Richard Mogull (InfoWorld 2002), research director for Gartner Research, the majority of successful attacks on computer systems exploit security weaknesses which are well known and for which remedies exist. This is problematic for smaller firms because of the generally lower levels of internal security expertise and an increased demand is placed on managers, who are ultimately responsible for that security. This illustrates the need for a manageable set of practices that can be implemented efficiently.

Computer networks and inter-networking have grown more pervasive each year and are now an integral part of the functioning of nearly every academic, business and government organization. Gartner estimates that through 2005, twenty percent of firms will experience a security incident, and that the repair costs for the incident will cost fifty

percent more than prevention costs would have been (InfoWorld 2002). A security incident is defined as an attack more serious than a virus. There is a significant potential for loss from intrusions to networked systems, either from disrupting operations or by covertly stealing information assets. This risk is quantified by Allen's (2000) report of more than \$250 million in losses documented by the FBI. Financial losses from network security breaches are costly. They regularly exceed \$100 million a year. The top causes are loss of proprietary information (\$42.5 million) and financial fraud (\$39.7 million). Additionally, Yankee Group estimates that the denial-of-service attacks on web sites last year could cost the companies more than \$1.2 billion. On the days of the attacks, losses exceeded \$100 million. Service disruptions ranged from two and three-quarter hours to five hours (CERT Feb. 23, 2003). Because a large portion of computer crime goes unreported, primarily due to concerns about publicity and subsequent loss of public trust, the FBI estimates that computer crime will actually cost companies over \$10 billion in 2003 (CERT Feb. 23, 2000). In addition to direct costs, governments have now begun to create legislation that spells out specific procedures for protecting data and penalties for organizations that fail to adequately protect the Personally Identifiable information of the public. This includes both financial, health, and general person-specific information. The White House Office of Science and Technology estimates an annual cost of \$100 million for US losses of proprietary information. The American Society for Information Science (ASIS) estimates that the losses may exceed \$250 billion. Additionally, an intrusion in which price lists, discount rates, or interest rates were changed could cause huge damage. Untold costs in loss of business can occur when customers lose faith in a company's

ability to protect information such as credit card numbers, names, addresses, and credit information (CERT Feb. 23, 2000).

Limitations

Because the first significant and documented threat to the integrity of networked information assets occurred in November 1988 when the Morris Worm (Rogers, 2002) burrowed into over 10% of the approximately 80,000 computers on the ARPANET, this study will only utilize resources published since 1988. The ARPANET, which was shut down in 1991 and was the forerunner of the current Internet, consisted primarily of university and government computers, and the applications supported on this network were simple: electronic mail (E-mail), electronic news groups, and remote connection to other computers. Protection of networked information assets only became an important topic after the Internet, as we know it today, began with Tim Berners-Lee's creation of the World Wide Web in 1991 (Zakon 2000). As the web was designed to allow universal and ubiquitous access to virtually everyone, it also opened the door to many unscrupulous activities. Also in 1988, the Computer Emergency Response Team (CERT) at Carnegie Mellon University was created by DARPA (Defense Advance Research Projects Agency) (Dekker 1997) to deal with threats to information security. It was the first, and most respected, of several organizations that have been created to track threats and study solutions to threats to networked assets. As a result many of the references cited in this study issue from the CERT center.

The swiftness and constantly evolving nature of new technologies, new attacks, and responses, etc. precludes being able to publish any final, definitive plan, which, if

implemented would absolutely secure an organization's information assets. There will always be new technical developments. This paper sifts from the myriad of technically oriented literature the basic fundamental practices for the small to medium sized organization to follow in setting a plan to secure its information assets.

For the purposes of this paper, all identifiable practices were initially recorded and those that appeared in less than five sources were excluded from the resulting set of fundamental practices.

This paper also assumes the existence of business goals and objectives from which security requirements derive. These may require periodically conducting an information security risk analysis and assessment to help set priorities and formulate protection strategies. Western Banking magazine (April\May 2003) comments, "It is NOT just a technology problem, solved merely by installing a firewall on your bank's computer network. Information security requires executive commitment and a comprehensive plan of action."

This paper also assumes the existence of organization-level and site-level security policies that can be traced to the above business objective, goals, and security requirements. If they do not exist, developing them is an essential task, preceding actual security practice (Allen 2001). However, this is an issue beyond the scope of this paper.

Problem Area

A review of the literature reveals theoretical perspectives and previous research findings related to the problem at hand (Leedy 2001). That problem is identified as the lack of a basic, yet fully encompassing, plan for small to medium sized businesses to follow to protect their information assets.

Protecting critical information assets can challenge the capabilities of almost any organization. Add to that the complexity associated with continuing technological changes and the task becomes especially daunting, particularly for small to medium sized organizations, in which the responsibility for security often falls to managers who lack a high level of technical expertise (Rasmussen 2003).

Some of the issues faced by managers in small to medium sized organizations can be:

- How to protect internal systems from unauthorized users while at the same time enhancing access to them, and in particular meeting demands for "open access" to information. This can require the flexibility of higher levels of discretionary access controls on sensitive information while still providing quick and reliable access to those who need it (Verity 2003).
- How to account for confidentiality and integrity of information passing out of the system and possibly back in again, for example through the Internet. New technology has resulted in an increasing proportion of documents existing primarily in electronic form (ISCC 1994).
- How to foster confidence in information systems. Particular attention must be paid to the preservation of critical processes for the sake of business continuity. Users count on their systems working properly when they want them and assume that they are being operated securely (Allen 2001).
- How to meet demands to use the latest technology, often before it has been fully tested. Rapidly changing technology, increased system usage and growing

demands from users for new and expanded connectivity have increased the variety and magnitude of risks (ISCC 1994).

- How to make policy and management decisions that reduce risk. Organizations should ensure that the magnitude and scope of threats are accounted for in planning information security strategies (ISCC 1994).
- How to minimize damage and accelerate the response time for attacks that do occur. This often includes deploying monitoring and detection systems as well as ensuring the ability to restore systems and assets to an operational state (CERT 2001).
- How to control your exposure to computer security compromises, whether accidental or malicious. These events can happen despite the best efforts of administrators (CERT 2001).

The recent media attention to business-stopping viruses, worms, and denial of service attacks, has heightened the awareness of senior management in most small to medium sized businesses to the issue of information security as a vital part of their business strategy (Johansson 2003). However, most executives probably do not have an adequate understanding of what it takes for them to protect their information assets (MetaGroup 2000). This paper seeks to provide a resource enabling those businesses to understand what the basic protections need to be and how to implement them.

Previous works in this field have consistently been quite technically oriented, and rather voluminous and hard to distill into the basic issues. Some examples include the 350 pages Standard of Good Practice for Information Security by the Information Security Forum (ISF 2003), and the 300 pages CERT Guide to System and Network

Security Practices (CERT 2003). Neither is particularly user friendly, especially for the less-technically inclined.

Chapter II. Review of References

The review of references describes the primary sources that were utilized by this study. These sources are also included in the References section. These sources are organized in the general sections of Method, Context, and Data Sources.

Method

Creswell, J (2003) Research Design, Qualitative, Quantitative and Mixed Methods Approaches Thousand Oaks, Ca. Sage Publications

This reference served as a foundation for the design of this study. It was used to identify and define the literature review process. Following the descriptions provided by Creswell, literature was selected to frame the Problem and as the data sources for the findings of a qualitative study. This source was selected because it is used as a primary text in the UO AIM masters program.

Krippendorff, K (1980) Content Analysis: An Introduction to its Methodology (5th ed.) Newbury Park, Calif.: SAGE Publications.

Krippendorff's book serves as a primary reference on the topic of Content Analysis. It was selected because the general principles of Content Analysis that are presented can be applied for the purposes of analyzing the literature in this study. The Section on Semantics of Data was used in establishing the coding categories for this study (pp. 75-78).

Leedy, P., Ormrod, J. (2001) Practical Research (7th ed.) Upper Saddle River, New Jersey: Merrill Prentice Hall

This book describes the general principles that can be applied to a research paper. Methods for locating source material, formatting the study, and presenting data are discussed. For the purposes of this study it provided general guidelines for analyzing the literature and presenting the analysis. Leedy was used to define the process of data analysis and as a guide to tabulating the frequency for practices that occurred in source literature.

Palmquist, M. (2001). Content Analysis. CSU Writing Guides, Accessed January 21, 2004, from Colorado State University, Writing Center Web Site:

<http://writing.colostate.edu/references/research/content/com2b1.cfm>

A Colorado State University web-based resource, this very usable and concise source, is based on the work of Palmquist and others. This source was used as a guide to establish the broad definitions of literature used for this study and for the concept of themes within that literature. It also provided guidelines to establish the level of analysis and to identify the terms to be coded for. This source was selected because of the general stature of Palmquist in this field and because it is associated with a credentialed institution.

Context

Allen J (2000) Improving the Security of Networked Systems, Software Technology Support Center [On-Line] Accessed January 24, 2004

<http://www.stsc.hill.af.mil/crosstalk/2000/10/allen.html>

Allen addresses the problem of lack of time, experience and knowledge by those charged with the security of information assets in many organizations. This source was used to help frame the Problem and Significance sections of this paper, particularly the challenges facing small to medium sized organizations. Allen also references several emerging sets of practices that subsequently were examined in the data collection phase of this paper. This source was selected because of the credibility of the supporting institution and the fact that it is commonly referenced in other studies as a primary data source.

Allen, J. (2001 May 22-24) CERT® System and Network Security Practices, Software Engineering Institute at Carnegie Mellon University, New York, NY. [On-Line] Accessed January 2, 2004 http://www.cert.org/archive/pdf/NCISSE_practices.pdf

This paper was presented at the National Colloquium for Information Security Education at George Mason University and published in its proceedings. Allen discussed the state of current security practices, the need for improvements, and proposed the organization of security practices into the five top-level steps of Harden/Securing, Prepare, Detect, Respond, and Improve. These five steps were selected as an organizing principle for this paper. An initial set of specific practices is also identified. This source

was used to support the Purpose and to develop the organization of the data in this paper. Selection criteria for this source included the authority of the sponsoring entity and the fact that Allen is referenced in many other sources.

Cross, S. (2000, Feb. 23) Cyber Threats and the US Economy Testimony before the Joint Economic Committee of the US Congress [On-Line] Accessed May 10, 2002
http://www.cert.org/congressional_testimony/Cross_testimony_Feb2000.html

This source details the rapidly increasing numbers of documented security breaches. In addition to identifying many of these threats and their financial and other impacts on businesses, Cross identifies many of the underlying reasons for the acceleration of risks to many organizations. The authority of this author, the credibility of its sponsoring entity and its currency were all factors in the selection of this source. It was used to develop the Problem and Significance sections of this paper. In addition, it was helpful in forming a concise and usable guide for general management and IT staff of organizations who lack highly technical security training.

Data Sources

Alberts, C (October 2001) OCTAVE® Catalog of Practices, Version 2.0

This technical report from Carnegie-Mellon summarizes the Operationally Critical, Threat, Asset, and Vulnerability Evaluation (OCTAVE®) Method and presents a catalog of practices to enable organizations to identify risks to information assets and mitigation plans for those risks. For the purposes of this paper, those practices were identified as fundamental practices. Allen also is credited with further organizing the

identified practices by either strategic or operational in nature. This distinction is adopted as a method to achieve as much clarity and usability as possible in describing the practices included in the result of this study. The selection criteria for this source were the credibility of its authoring organization and its frequent reference in other works.

CERT® Security Improvement Modules (2003) Addison-Wesley, [On-Line] Accessed January 25, 2004 <http://www.cert.org/security-improvement/>

This exhaustive (300+ page) set of modules compiled by the CERT® Coordination Center at Carnegie-Mellon University is intended to provide an extensive source of system and network security practices. Each module contains sets of practices for a planned, practical approach to information security. These modules are presented by grouping them according to Allen's five top-level steps of Harden/Securing, Preparing, Detecting, Responding, and Improving. This corresponded to the presentation approach of this paper, however many of the practices were broken down to a level of detail that was beyond the scope of this paper. They were therefore coded at a higher level of generalization in order to maintain a consistency with other data sources. The criteria for selecting this source were the credibility of its authoring organization, as well as the fact that it is frequently referenced in other works. The CERT center located at the Software Engineering Institute (SEI) at Carnegie-Mellon is a federally funded research and development center and a center of Internet security expertise. Created by the Defense Advanced Research Projects Agency, SEI is charged with establishing a capability to quickly and effectively coordinate communication among experts during security

emergencies in order to prevent future incidents, and also with building awareness of security issues across the Internet community.

Information Security Forum (ISF) (March 2003) The Standard of Good Practice for Information Security, Version 4.0 [On-Line] Accessed January 6, 2004
http://www.isfsecuritystandard.com/index_ie.htm

This work is produced by ISF, an international association of over 250 leading organizations that fund and cooperate on the development of practical research in information security. ISF reports are normally for the exclusive use of its members, but the Standards of good Practices is made available to any organization with the objective of improving the general level of information security risks and assisting others to implement proven, effective practices. The practices in this source were coded for the Data Analysis section of this paper. This source was selected because of the credibility of its sponsoring entity and because of its currency.

Internet Security Alliance (ISA) (July 2002) Common Sense Guide for Senior Managers [On-Line] Accessed January 2, 2004 <http://www.isalliance.org/news/BestPractices.pdf>

The ISA aims to identify and standardize best practices in information security and information survivability. It is a collaborative effort of the Software Engineering Institute, the CERT Co-ordination center and the Electronics Industries Alliance, a federation of trade associations, private and public corporations. This source identifies an initial set of ten basic practices, targeted at executive management personnel who likely will lack a high level of technical skills. Each practice is presented with numerous sub-

practices, which for the purposes of this paper, were identified as individual practices. This source was selected because of the authority and objectivity of the sponsoring organizations.

National Security Agency (NSA) (2002) Ft. Meade, MD [Sixty Minute Guide to Network Security](#) [On-Line] Accessed December 28, 2003
SNAC.Guides@NSA.gov

Prepared by the Systems and Network Attack Center of this Department of Defense agency, this source contends that most security vulnerabilities are easily identified and rarely fixed, leading to the rapid increase in exploitations or incidents. This guide is intended to be a 'best practices' document and was written with the less experienced systems administrator or information systems manager in mind, thus making it applicable to typical small to medium business management personnel. It seeks to help these managers understand and deal with the risks they face in securing information assets. Much of the research on which this is based comes from Department of Defense or other government infrastructures, and is applicable to this paper because of its broad approach and less technical presentation. This source was used in the development of the Purpose and Significance sections of this paper as well as providing source data for the Analysis. This source was selected because of the authority of its sponsoring organization and because its technical level was in alignment with the objectives of this paper.

Whitman and Mattock (2003) Management of Information Security Chapter 6, Security Management Models and Practices, Canada, Thompson Course Technology, First edition

[On-Line] Accessed January 2, 2004

http://science.kennesaw.edu/~mwhitman/classes/ISA3300/MoIS_CH06.pdf

This textbook is used by many upper level college courses in Information Security. A major position taken by the authors is that organizations must make sure they have a reasonable level of security in all areas before improving individual areas to meet higher and more technical standards. With this in mind, several sets of best practices were presented which were coded to be included in the Data Analysis section of this paper. Whitman's assessment that information security is a managerial problem, not a technical one was also used to support the basic premise and Purpose of this paper. This source was selected because of the inclusion of its material in several other references and because it added pertinent additional data for analysis.

Chapter III. Method

The general method of study is literature review, as described by Creswell (2003). This method looks at the work others have done and seeks to build upon those previous works with a needed, new interpretation. A preliminary examination of the literature revealed that there is a significant amount of literature addressing information security available, but much of it is very technical, necessitating that its intended audience be quite sophisticated. By focusing on small to medium sized businesses, which comprise 80 percent of the US economy (SBA 2002), and looking for basic steps that can be used by managers who don't have a high degree of technical sophistication, a new and needed interpretation, specific to that group was developed.

Data Collection

Searches for the initial key terms of 'Information Security', 'Network Security', 'Computer Network Security Risks', and 'Network Survivability' were done using the University of Oregon library web site, LexisNexis Academic, FirstSearch and Google. Sources include web sites, articles, white papers, and books. The initial search for 'Network Security' yielded 3,070,000 sources, and 'Information Security' a similarly unwieldy 2,350,000. 'Computer Network Security' yielded only 32,000, 'Network Survivability' resulted in 5600 potentials, and 'Information Survivability' returned 5400. In an effort to reduce the size of the field, the term 'Computer Network Security Risks' was used, returning only 12 results, none of which were particularly useful. As a result, additional themes were also identified as 'Information Confidentiality', Information

Integrity’, ‘Information Availability’, ‘Information Security Policies’, Information Security Procedures’ and ‘Information Security Practices’. The search strategy was then modified to initially search for the terms ‘Network Security’ and ‘Information Security’, and then to apply a second or third search criteria of searching the initial results using the additional terms of ‘Information Confidentiality’, Information Integrity’, ‘Information Availability’, ‘Information Security Policies’, Information Security Procedures’ and ‘Information Security Practices’. A restriction was also used, requiring that sources only be in English. This strategy resulted in several collections of possible sources numbering only in the several hundreds. Thirty-Two of the collected resources were selected for use in this study. Repetitions of similar practices were then identified to develop the sets of fundamental practices.

Information sources were evaluated using the four criteria identified by the University of Oregon Libraries (UO 2003) for evaluating information on the World Wide Web. Those criteria are authority, objectivity, accuracy, and currency. Authority addresses questions on who is the author, what were their credentials, if they have been peer-reviewed, and what institution are they affiliated with. Objectivity attempts to identify the purpose and goals of the literature and whether the author was affected by any biases or is attempting to persuade or sell. Accuracy is evaluated by looking at completeness, grammatical correctness, general visual quality, and existence of valid cross-references. Currency is concerned with when the page was created, is it maintained reasonably currently, and whether the links to references work.

Data Analysis

Because content analysis is suitable to determine the presence of certain words or concepts within texts (Leedy and Ormrod 2001), this method was selected as the data analysis strategy. More specifically, a sub-section of content analysis, conceptual analysis (Palmquist 2000) was used to establish the existence and frequency of themes related to fundamental practices for protection of information assets.

To perform the analysis of the literature collected for this study, data is first collected according to the existence of the three themes, Information Security Policies, Information Security Procedures, and Information Security Practices. There was a lack of total agreement in the literature as to the definitions of these terms, therefore, this researcher felt that any of these areas could contain pertinent information to this study.

Next, this literature was coded, following a strategy presented by Palmquist (2000), for the existence of traits that could be associated with the five top-level steps that depict how to secure and protect information assets, presented by Allen (2001). These steps are framed as five coding categories: Hardening/Securing, Preparing, Detecting, Responding, and Improving (Allen 2001), and with the concepts of confidentiality, integrity, and availability (CERT 2002). In Palmquist's terms, these became the pre-defined or interactive set of concepts. The coding process was one of selective reduction at a fairly broad level for specific words, sets of words or phrases (Palmquist 2001) that could be identified as relating to one of those terms. According to Palmquist, this enabled a level of coding flexibility. Texts were first coded only for the existence and not frequency of material relating to the pre-defined concepts. Next a dynamic list of key words, sets of words and phrases was established in order to identify unique practices.

Additional terms were added as they were discovered in the literature. Because the list is lengthy, it is presented in Appendix A.

Occurrences of selected coding terms were then recorded in a matrix and practices that were identified as existing in five or more sources were deemed significant and were grouped according to Allen's top-level categories of Hardening/Securing, Preparing, Detecting, Responding, and Improving (Allen 2001). An example of the coding matrix is included in Appendix B.

Data Presentation

The result of data analysis is presented as a series of eighteen practices, grouped according to Allen's (2001) five steps of Hardening/Securing, Preparing, Detecting, Responding, and Improving. Each step is explained in the Full Purpose section of this paper.

Each of the fundamental practices identified through the content analysis is further categorized as being either strategic or operational in nature. According to Allen, strategic practices focus on organizational issues and provide good general management practices. Operational practices focus on technology-related issues relating to how people use, interact with and protect technology. Since strategic practices are based more on good management practices, they should be fairly stable over time. Operational practices are more subject to changes caused by new technological developments and updated practices to deal with those developments (CERT 2002). Additionally, each fundamental practice is aligned with one or more of the specific security concepts (identified by the Software Engineering Institute (CERT® 2002) of confidentiality, integrity, and

availability. An example of the intended format the set of fundamental practices is included here, as Table 1: Hardening/Securing: Initial Configuration.

Hardening/Securing

<i>Category</i>	<i>Fundamental Practices</i>	<i>Associated Security Concepts</i>
Strategic		
Operational		

Table 1: Hardening/Securing: Initial Configuration (from Allen, 2001)

Chapter IV. Analysis of Data

Data analysis was conducted on thirty-two source documents that were selected using the criteria of authority, objectivity, accuracy, and currency (UO Library 2003).

The first phase of analysis was the coding of the selected articles for the existence of identifiable practices for securing networked information assets. The resulting list of forty-nine words, terms, or phrases is listed in Appendix A. Each of those phrases, etc. is used to represent an information security practice found in the source literature. Once the coding was finished and the list of practices established, the occurrence of all practices in each document was recorded in the matrix format illustrated in Appendix B. The occurrences of individual practices in each source were then combined in the summary found in Appendix C.

A further analysis was then conducted to identify practices from this summary that were similar, overlapping, or simply two different ways to describe the same thing. These practices were then combined into categories where appropriate and specific practices occurring in two or less sources were deemed insignificant and were dropped. This resulted in the final set of twenty-two practices found in Appendix D.

Next, those practices that occurred in less than five sources were dropped and the remaining eighteen were grouped according to Allen's five basic steps of Harden/Secure, Prepare, Detect, Respond, and Improve (2000). This set can be found in Appendix E. One final assessment was then done to determine whether each one should be identified as strategic or operational and which of the three attributes of information security each one

addresses; Availability, Integrity or Confidentiality. The result is detailed in the following Conclusions section.

Chapter V. Conclusions

It is the conclusion of this researcher that inadequate security of networked information assets is a significant issue for virtually all organizations, especially for management of those that do not have specialized information security personnel. The rapid growth and complexity of the information technology industry, the trend to push the fiduciary responsibility for the integrity, confidentiality, and availability of information assets to the highest management levels and fact that the demand for qualified individuals far exceeds the supply (Allen 2000) have created a need for a concise and pragmatic tool that can be used by management in those small to medium sized organizations to evaluate their condition and to attain a basic level of protection.

The results of this study are presented here as eighteen fundamental practices, grouped in Allen's (2001) five steps of Harden/Secure, Prepare, Detect, Respond, and Improve. The selected practices were identified because of recurring frequency in the literature surrounding this issue. These five categories represent a top-level depiction of how to secure and protect information assets. Harden/Secure refers to the initial configuration of software and hardware in a system and the relationship or architecture of how the different elements of the system are interconnected and implemented. The Prepare, Detect, Respond, and Improve steps assume that the Harden/Secure steps have already been implemented and provide further guidance to maintain the level of security, as well as guidelines in the event that something suspicious, unexpected or unusual occurs. The practices are further associated with the categories of availability, integrity and confidentiality that each one addresses and whether they are strategic or operational in nature.

These practices can be used by the management of smaller organizations as a guideline to establishing a basic level of security around information assets and for identifying those areas in which the organization might be best served by outsourcing or contracting for specialized expertise.

In using these practices, management will first need to identify the business goals and objectives from which security requirements derive, and possibly conducted a Risk Management Assessment. The OCTAVE (Albert 2001) self-assessment, which is available from CERT but is beyond the scope of this paper, is one possible tool to understand the value of the assets that need to be protected, the consequences of a loss of confidentiality, vulnerabilities or existing threats, the likelihood that a threat might occur, and the availability or appropriateness of options and resources. The attainment of total security is a daunting challenge; however adopting these recommended practices should enable an organization to mitigate its most critical risks. Following the listing of the fundamental practices, a more detailed explanation of each practice is provided, aligned with resources.

Fundamental Security Practices for Small to Medium Organizations

Harden/Secure		Associated Concepts
Strategic	1. Architecture and Design	Availability, Confidentiality, Integrity
	2. Asset Configuration	Availability, Confidentiality, Integrity
	3. Access Control-Password management-VPN	Availability, Confidentiality, Integrity
	4. User security awareness training and education	Confidentiality, Integrity
	5. Use only trusted sources of code	Confidentiality, Integrity
Operational	6. Anti-virus applications	Availability, Confidentiality, Integrity
	7. Authentication	Availability, Confidentiality, Integrity
	8. Authorization	Availability, Confidentiality, Integrity
	9. Encryption/Cryptography	Confidentiality, Integrity
	10. Firewall	Confidentiality, Integrity
	11. Physical Security	Confidentiality, Integrity
	12. Port Security-VLANs	Integrity
	13. Securing Public Hosts	Confidentiality, Integrity
Prepare		
Operational	14. Logging, Logs, Audits	Confidentiality, Integrity
Detect		
Operational	15. Monitoring Tools- IDS	Confidentiality, Integrity
Respond		
Operational	16. Backup and Recovery, Documentation, Removable Storage	Confidentiality, Integrity
Improve		
Strategic	17. Contingency Planning	Availability, Confidentiality, Integrity
Operational	18. Product and Application updates, patches and hot fixes	

Explanation of Fundamental Practices

1) Architecture and Design

Use a layered approach (ISA 2002) that must be documented and should include provisions for adequate capacity, availability through redundancy, and load balancing (Wagner 2001).

2) Asset Configuration

Establish and maintain a standard minimum essential configuration for each type of computer and service (Wayne State 2003).

3) Access Control-Password Management-VPN

Passwords must have low maximum length of validity, a large minimum number of characters, a long reuse restriction, significant complexity and a lockout policy for failed attempts (Goodman 2003). VPN (Virtual Private Network) is the creation of an encrypted access process called a dynamic tunnel (Dexter 2002) for those users outside the network who need to access network assets, such as remote workers, or contractors.

4) User Security Awareness Training and Education

Should include responsibilities, accountability, and consequences, as well as approved personal use access parameters (Herbert 2003).

5) Use Only Trusted Sources of Code

Attachments from unknown sources should never be opened; all software must be legally obtained and properly registered (PISC 2002).

6) Anti-virus Applications

Software designed to scan for, and disable viruses, worms and malicious code that reach the network environment. Symantec and McAfee are the best known and provide daily Internet updates, but there are other brands available.

7) Authentication

The process of validating that someone or something is who or what they say they are.

8) Authorization

The granting of access, rights or privileges to files, folders, or servers. Implement the concept of “least privilege”(NSA 2002).

9) Encryption/Cryptography

The process of changing plain text information, such as credit card numbers, account numbers, or passwords into an encoded, incomprehensible form before it is transmitted outside your network or possibly when storing especially valuable data inside your network. The data cannot be opened unless the recipient has the proper key to decipher it. Using tools such as MD5 checksums, a strong cryptographic technique, to ensure software integrity (Dekker 1997).

10) Firewall

Hardware or software that examines all traffic to or from a network and passes or blocks it based on predetermined criteria, for example a firewall might block certain types of attachments from e-mail. Also enables Network Address Translation to keep internal addresses private.

11) Physical Security

Access to server rooms, wiring closet, cable distribution facilities, and network terminals should be appropriately regulated. May involve only locks and keys, or more sophisticated monitoring, and even biometric verification (Wagner 2001).

12) Port Security-VLANs

Disabling unused ports, restricting access on a per-port basis to specific MAC addresses, and the segregation of portions of the network into distinct segments with restricted connectivity to increase the protection for any given section (Wagner 2001).

13) Securing Public Hosts

Shutting down unneeded services, disabling unused ports and interfaces, specific protection for all active interfaces and extra durable passwords (NSA 2002).

14) Logging, Logs, Audits

Logging is the recording of events of some type for retrieval and analysis at a later time. Auditing is the process of tracking certain types of events, such as access success or failure for certain assets, (Goodman 2003) one common method is to use Windows Active Directory.

15) Monitoring Tools- IDS

IDS (Intrusion Detection Systems) are software that can run either inside or outside the firewall and identify suspicious network traffic by looking

for exceptions to normal patterns of behavior for the network, hosts or users.

16) Backup and Recovery, Documentation, Removable Storage

Documentation includes network diagrams, system information, incident reports, policies, contact lists, as well as data and files that are backed up daily or more often. The practice of removing back up storage to an off site location can be crucial.

17) Contingency Planning

Having an incident response plan that includes the course of action to a security incident, sometimes called a disaster recovery plan.

18) Product and Application Updates, Patches and Hot Fixes

Identifying and downloading updates and solutions to newly discovered vulnerabilities for all software programs. Many, but not all, of these can be automated, so a regular schedule of checking for updates needs to be established. In addition, a good source of current security alerts is the CERT center.

References

- Alberts, C. (October 2001) OCTAVE Catalog of Practices, Version 2.0 [On-Line]
<http://www.cert.org/archive/pdf/01tr020.pdf>
- Allen, J. (2000) Improving the Security of Networked Systems, Software Technology Support Center [On-Line] Accessed January 24, 2004
<http://www.stsc.hill.af.mil/crosstalk/2000/10/allen.html>
- Allen, J. (2001 May 22-24) CERT® System and Network Security Practices, Software Engineering Institute at Carnegie Mellon University, New York, NY. [On-Line] Accessed January 2, 2004 http://www.cert.org/archive/pdf/NCISSE_practices.pdf
- Allen, J. (2002) Ask the Right Questions, White Paper for Software Engineering Institute at Carnegie Mellon University, New York, NY. [On-Line] Accessed January 22, 2004 <http://www.cert.org/>
- Allen, Alberts, Behrens, Laswell, Wilson. (2000 Oct.) Improving the Security of Networked Systems White Paper [On-Line] Accessed May 15, 2002
<http://www.stsc.hill.afmil/crosstalk/2000/oct/allen.asp>
- CERT® (February 23, 2000) Cyber Threats and the US Economy, Testimony before the Joint Economic Committee, US Congress [On-Line] Accessed January 24, 2004
http://www.cert.org/congressional_testimony/Cross_testimony_Feb2000.html
- CERT® (2002) Computer Emergency Response Team at Carnegie Mellon University, Improving the Security of Networked Systems [On-Line] Accessed January 10, 2004 <http://www.cert.org/security-improvement/practices/practices.html>
- CERT® Coordination Center (CERT/CC 2003) is a center of Internet security expertise, located at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University [On-line] Accessed December 2003
<http://www.cert.org/>
- Creswell, J. (2003) Research Design, Qualitative, Quantitative and Mixed Methods Approaches Thousand Oaks, Ca. Sage Publications
- CSI (2000) CSI/FBI Computer Crime and Security Survey, Computer Issues and Trends, Vol. VI, No 1 [On-Line] Accessed May 15, 2003
<http://www.stsc.hill.af.mil/crosstalk/2000/10/allen.html>

- Cross, S. (2000, Feb. 23) Cyber Threats and the US Economy Testimony before the Joint Economic Committee of the US Congress [On-Line] Accessed May 10, 2002 http://www.cert.org/congressional_testimony/Cross_testimony_-_Feb2000.html.
- Dekker, M. (1997). Security of The Internet. The Froehlich/Kent Encyclopedia of Telecommunications, vol. 15. New York, pp. 231-255. [On-Line] Accessed May 10, 2002 http://www.cert.org/encyc_article/toecencyc.html
- Dexter, J. (2002) The Cyber Security Management System, SANS Institute [On-Line] Accessed January 25, 2004 <http://www.sans.org/rr/papers/48/591.pdf>
- Florida State University (2003) Firewall Best Practices, University portal for security resources, [On-Line] accessed January 15, 2004 <http://www.security.fsu.edu>
- Federal Trade Commission (FTC) (2003) Security Check: Reducing Risks to your Computer Systems, Federal Trade Commission- Facts for Businesses [On-Line] Accessed December 27, 2003 <http://www.ftc.gov/bcp/online/pubs/buspubs/security.htm>
- Federal Trade Commission (FTC) (2004) Federal Trade Commission web site on privacy initiatives [On-Line] Accessed January 26, 2004 <http://www.ftc.gov/privacy/glbact/>
- Goodman, J. (2003) How to Secure Your Small to Medium Size Microsoft Based Network, SANS Institute, [On-Line] Accessed January 25, 2004 http://www.giac.org/practical/GSEC/Jerry_Goodman_GSEC.pdf
- Herbert, J. (2003) Introducing Security to the Small Business Enterprise, SANS Institute, [On-Line] Accessed January 24, 2004 http://www.giac.org/practical/GSEC/Jeff_Herbert_GSEC.pdf
- Hernan, S. (2000, Oct.) Security Often Sacrificed for Convenience CERT@Continuation Center [On-Line]. Accessed May 15, 2002 <http://www.stsc.hill.afmil/crosstalk/2000/oct/heman.asp>
- Health and Human Services, US Department of (HHS) (2004) HIPAA web site [On-Line] Accessed January 26, 2004 <http://www.hhs.gov/ocr/hipaa/>
- Information Systems Coordination Committee (ISCC) (1994) Information Security: Recommended Practices [On-Line] Accessed February 5, 2004 <http://accsubs.unsystem.org/iscc-documents/documents/distribution/maintext/security-managers.html>
- Information Security Forum (ISF) (March 2003) The Standard of Good Practice

- for Information Security, Version 4.0 [On-Line] Accessed January 6, 2004
http://www.isfsecuritystandard.com/index_ie.htm
- InfoWorld (May 2, 2002) (On-Line) accessed January 2, 2004
<http://www.cnn.com/2002/TECH/internet/05/03/security.indifference.idg/>
- INSTANT/MDR (2003) Two Groups Predict Managed Security Services Growth [On-Line] Accessed January 27, 2004
http://searchsecurity.techtarget.com/newsItem/0,289139,sid14_gci850020,00.html
- Internet Security Alliance (ISA) (2002, July) Common Sense Guide for Senior Managers [On-Line] Accessed January 5, 2004
<http://www.isalliance.org/news/BestPractices.pdf>
- Internet Security Alliance (ISA) (2002, July) Top Ten recommended Security Practices [On-Line] Accessed January 4, 2004
<http://www.isalliance.org/news/BestPractices.pdf>
- Internet Security Systems (ISA) (2000) Creating, Implementing and Managing the Information Security Lifecycle [On-Line] Accessed December 28, 2003
<http://documents.iss.net/whitepapers/securityCycle.pdf>
- Internet Security Systems (2000, Aug. 2) Evaluating an Intrusion Detection Solution White Paper [On-Line] Accessed May 13, 2002
http://documents.iss.net/literature/RealSecure/ids_eval.pdf
- Internet Security Systems (2001, Oct.) A Vision for Complete Protection [On-Line] Accessed May 13, 2002
<http://documents.iss.net/whitepapers/visionforcompleteprotectionmktg.Pdf>
- Internet Security Systems (2002) Response Strategies For Hybrid Threats White Paper [On-line] Accessed May 13, 2002
<http://documents.iss.net/whitepapers/HybridThreat.pdf>
- Internet Security Systems (2003) Internet Risk Impact Summary [On-Line] Accessed January 24, 2004
<https://gtoc.iss.net/documents/summaryreport.pdf>
- Itsecurity.com The ITsecurity.com Dictionary+ of Information Security [On-Line] Accessed December 28, 2003
<http://www.itsecurity.com/dictionary/dictionary.htm>
- Johansson, J. (2003) Security Management-The Fundamental Tradeoff Microsoft TechNet, Security Program manager, Microsoft Corporation [On-Line]

Accessed January, 25, 2004

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/security/essays/tradeoff.asp>

Krippendorff, K. (1980) Content analysis: An introduction to its methodology (5th ed.) Newbury Park, Calif.: SAGE Publications

Leedy, P., Ormrod, J. (2001) Practical Research (7th Ed.) Upper Saddle River, New Jersey: Merrill Prentice Hall

Linger, R.C. (1998) Requirements Definition for Survivable Network Systems, Carnegie-Mellon University [On-Line] Accessed December 27, 2003
<http://csdl.computer.org/comp/proceedings/icre/1998/8356/00/83560014abs.htm>

MetaGroup (2003) [On-Line] Accessed January 25, 2004
http://smallbusiness.itworld.com/4385/040120trendmicro/page_1.html

National Security Agency (NSA), (2002) Ft. Meade, MD Sixty Minute Guide to Network Security [On-Line] Accessed December 28, 2003
SNAC.Guides@NSA.gov

Pacific Information Security Consulting (PISC) (2002) Best Practices Information Security Policy, [On-Line] Accessed January 14, 2004
<http://www.PacificIS.com>

Palmquist, M. (2001) Content Analysis, Accessed January 21, 2004, from Colorado State University, Writing Center Web Site:
<http://writing.colostate.edu/references/research/content/>

Pethia, R. (May 25,2000) Internet Security Issues, Testimony before the US Senate Judiciary Committee, Carnegie-Mellon University [On-Line] Accessed January 25, 2004
http://www.cert.org/congressional_testimony/Pethia_testimony25May00.html

Rasmussen, M. (2003) New Threats, Regulatory Woes to Cause '04 Security Headaches, Forester Research, Cambridge, Mass [On-Line] Accessed January, 25, 2004
http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci942121,00.html.

Rogers, L. (2002) Buffer Overflows-What They Are and What I Can Do About Them Software Engineering Institute, Carnegie Mellon University, Pittsburgh PA [On-Line] Accessed January 2, 2004
http://www.cert.org/homeusers/buffer_overflow.html

- SANS Institute (2003) Internet Storm Center, Develops, maintains, and makes available at no cost, the largest collection of research documents about various aspects of information security, and it operates the Internet's early warning system. [On-Line] Accessed December 28, 2003 <http://www.sans.org/aboutsans.php>
- SB 1386 (2002) California Database Security Breach Notification Act [On-Line] Accessed January 25, 2004 http://www.securitymanagement.com/library/SB1386_ca0203.pdf
- Software Security Institute (2003) Search of advisories posted on the web site [On-Line] Accessed January 4, 2004 http://www.cert.org/nav/index_red.html
- Stanford University (2003) ITTS [On-Line] <http://securecomputing.stanford.edu>
- University of Oregon (2003) Evaluating Information on the World Wide Web service of the university libraries [On-Line] Accessed December 28, 2003 <http://libweb.uoregon.edu/guides/searchweb/evaluating.html>
- USDE (2003) Computer Incident Advisory Capability, US Department of Energy web site [On-Line] accessed December 27, 2003 <http://ciac.llnl.gov/cgi-bin/index/bulletins?n>
- Verity (2003) Securing Your Intellectual Capital [On-Line] Accessed January 2, 2004
- Wagner, R. (2001) Securing Network Infrastructure and Switched Networks, SANS Institute [On-Line] Accessed January 15, 2004 <http://www.sans.org/rr/papers/48/451.pdf>
- Wayne State University (2003) Office of Internal Audit, Best Practices Information Security [On-Line] Assessed January 6, 2004 <http://internalaudit.wayne.edu/Internal/ITSecBP.htm>
- Whitman and Mattock (2003) Management of Information Security Chapter 6, Security Management Models and Practices Thompson Technology Publications, Canada [On-Line] Accessed January 2, 2004 http://science.kennesaw.edu/~mwhitman/classes/ISA3300/MoIS_CH06.pdf
- Zakon, G. (2000) An Internet Timeline [On-Line] Accessed January 22, 2004 <http://www.zakon.org/robert/internet/timeline/>

Appendix A

List of words, sets of words, and phrases for final coding of data

Access Control	IDS (Intrusion Detection System)
Access Control lists (ACL)	Logging, logs
ADS (Attack Detection Systems)	Monitoring tools
Application proxies	Packet Filter
Application software	Packet sniffer
Anti-virus	Password management
Application patches	Physical Security
Application hot fixes	Product updates/ patches/hot fixes
Application updates	Port security
Architecture and Design	Redundancy and diversity
Asset Configuration	Remove unused services
Audits	Removable storage
Authentication	Risk Management
Authorization	Routers
Backups	Security Awareness Training
Backups and recovery	Securing Public Hosts
Configuration	Simple Network Management Protocol (SNMP)
Contingency planning	Software integrity
Disable hidden file extensions	TCP/IP filtering
Disable mobile code	Topology
Disable scripting in e-mail	User training and education
DNS (Domain name server)	Use only trusted sources of code
Documentation	VLANs (Virtual Local Area Networks)
Encryption/Cryptography	VPN (Virtual Private Networks)
Firewall	

Appendix C

Raw data

Practice	Occurrences
Access Control	8
Access Control lists (ACL)	2
ADS (Attack Detection Systems)	1
Application proxies	1
Application software	1
Anti-virus	15
Application patches	5
Application hot fixes	5
Application updates	3
Architecture and Design	11
Asset Configuration	6
Audits	2
Authentication	15
Authorization	13
Backups	8
Backups and recovery	3
Configuration	2
Contingency planning	5
Disable hidden file extensions	3
Disable mobile code	2
Disable scripting in e-mail	3
DNS (Domain name server)	4
Documentation	4
Encryption/Cryptography	9
Firewall	22
IDS (Intrusion Detection System)	16
Logging, logs	13
Monitoring tools	13
Packet Filter	3
Packet sniffer	1
Password management	11
Physical Security	11
Product updates/ patches/hot fixes	15
Port security	5
Redundancy and diversity	3
Remove unused services	6
Removable storage	2
Risk Management	1

Routers	1
Security Awareness Training	2
Securing Public Hosts	5
Simple Network Management Protocol (SNMP)	4
Software integrity	2
TCP/IP filtering	6
Topology	6
User training and education	8
Use only trusted sources of code	7
VLANs (Virtual Local Area Networks)	2
VPN (Virtual Private Networks	10

Appendix D Consolidated data

(Reduced to Similar Practices)

Practice	Occurrences
Access Control-Access Control lists (ACL)-VPN (Virtual Private Networks)-Password management	31
Anti-virus	15
Architecture and Design-Redundancy and diversity-Topology	20
Asset Configuration-Configuration	8
Authentication	15
Authorization	13
Backups and recovery-Documentation-Removable storage	17
Contingency planning	5
Disable hidden file extensions	3
Disable scripting in e-mail	3
DNS (Domain name server)	4
Encryption/Cryptography	9
Firewall-Packet Filter-TCP/IP filtering	31
Logging, logs-Audits	15
Monitoring tools-IDS (Intrusion Detection System)	29
Physical Security	11
Product-Application updates/ patches/hot fixes	28
Port security-VLANs (Virtual Local Area Networks)	7
Securing Public Hosts-Remove unused services	11
Simple Network Management Protocol (SNMP)	4
User training and education-Security Awareness Training	10
Use only trusted sources of code	7

Appendix E

Fundamental Practices grouped by Allen's five steps

Harden/Secure

Practice	Occurrences
Access Control-Access Control lists (ACL)-VPN (Virtual Private Networks)-Password management	31
Anti-virus	15
Architecture and Design-Redundancy and diversity-Topology	20
Asset Configuration-Configuration	8
Authentication	15
Authorization	13
Encryption/Cryptography	9
Firewall-Packet Filter-TCP/IP filtering	31
Physical Security	11
Port security-VLANs (Virtual Local Area Networks)	7
Securing Public Hosts-Remove unused services	11
User training and education-Security Awareness Training	10
Use only trusted sources of code	7

Prepare

Logging, logs-Audits	15
----------------------	----

Detect

Monitoring tools-IDS (Intrusion Detection System)	29
---	----

Respond

Backups and recovery-Documentation-Removable storage	17
--	----

Improve

Contingency planning	5
Product-Application updates/ patches/hot fixes	28