The Chain-Link Fence Model: A Framework for Creating Security Procedures

Robert F. Houghton
Utah State University

Follow this and additional works at: https://digitalcommons.usu.edu/etd

Part of the Information Security Commons, and the Management Information Systems Commons

Recommended Citation
https://digitalcommons.usu.edu/etd/1967

This Dissertation is brought to you for free and open access by the Graduate Studies at DigitalCommons@USU. It has been accepted for inclusion in All Graduate Theses and Dissertations by an authorized administrator of DigitalCommons@USU. For more information, please contact digitalcommons@usu.edu.
THE CHAIN-LINK FENCE MODEL: A FRAMEWORK FOR CREATING SECURITY PROCEDURES

by

Robert F. Houghton

A dissertation submitted in partial fulfillment of the requirements for the degree of DOCTOR OF PHILOSOPHY in Education (Management Information Systems)

Approved:

____________________  ______________________
Dr. Zsolt Ugray  Dr. David Paper
Major Professor  Committee Member

_____________________  _____________________
Dr. Jeffrey J. Johnson  Dr. David Olsen
Committee Member  Committee Member

_____________________  _____________________
Dr. Thomas P. Rohrer  Dr. Mark McLellan
Committee Member  Vice President for Research
And Dean of the School of Graduate Studies

UTAH STATE UNIVERSITY
Logan, Utah

2013
ABSTRACT

The Chain-Link Fence Model: A Framework for Creating
Security Procedures

By

Robert F. Houghton,
Utah State University, 2013

Major Professor: Dr. Zsolt Ugray
Department: MIS

A long standing problem in information technology
security is how to help reduce the security footprint. Many
specific proposals exist to address specific problems in
information technology security. Most information
technology solutions need to be repeatable throughout the
course of an information systems lifecycle.

The Chain-Link Fence Model is a new model for creating
and implementing information technology procedures. This
model was validated by two different methods: the first
being interviews with experts in the field of information
technology and the second being four distinct case studies
demonstrating the creation and implementation of information technology procedures.

(169 pages)
PUBLIC ABSTRACT

Information technology security professionals are facing an ever growing threat to the networks that they defend. The process for creating procedures to help stem this threat is very difficult for security professionals. The Chain-Link Fence Model helps security professionals by guiding them through the process of creating and implementing new security procedures.

Robert F. Houghton
DEDICATION

This dissertation is dedicated to my loving family, without whose help I could not have accomplished this monumental task. To Ron and Lani Vanderbeek, I thank you for opening your house to me. To George and Denise Houghton, your loving encouragement and exciting demeanor kept me motivated. To Stephen, Brielle, Mary, and Gabe, your help with all of fine details kept the dissertation on track.

To Calvin, Paisley, Ginny, and Ronald, your love and kindness made my heart melt every time I had to come home late, or go to Idaho to work.

To Sarah, words alone cannot describe how much thanks and love I give you. As promised here is your space for ABD:
ACKNOWLEDGMENTS

The author wishes to thank Utah State University, the USU Information Technology Team, and specifically the Central IT Security team for contributing data and allowing access to sensitive parts of their security infrastructure.

Robert F. Houghton
## CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABSTRACT</td>
<td>iii</td>
</tr>
<tr>
<td>PUBLIC ABSTRACT</td>
<td>v</td>
</tr>
<tr>
<td>DEDICATION</td>
<td>vi</td>
</tr>
<tr>
<td>ACKNOWLEDGMENTS</td>
<td>vii</td>
</tr>
<tr>
<td>LIST OF TABLES</td>
<td>xi</td>
</tr>
<tr>
<td>LIST OF FIGURES</td>
<td>xii</td>
</tr>
<tr>
<td>INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>Background</td>
<td>1</td>
</tr>
<tr>
<td>Purpose Statement</td>
<td>11</td>
</tr>
<tr>
<td>Conceptual Framework</td>
<td>11</td>
</tr>
<tr>
<td>Original Contribution</td>
<td>13</td>
</tr>
<tr>
<td>Layout of the Dissertation</td>
<td>13</td>
</tr>
<tr>
<td>REVIEW OF THE LITERATURE</td>
<td>15</td>
</tr>
<tr>
<td>Review Procedures</td>
<td>15</td>
</tr>
<tr>
<td>Locating the Papers</td>
<td>16</td>
</tr>
<tr>
<td>The History and Current State of Information Technology Security</td>
<td>17</td>
</tr>
<tr>
<td>The Process of the Creation of Policy, Procedures, or Industry Standards and Their Effects on Information Technology Security</td>
<td>27</td>
</tr>
<tr>
<td>DESCRIPTION OF THE CHAIN-LINK FENCE MODEL</td>
<td>52</td>
</tr>
<tr>
<td>Establishment</td>
<td>52</td>
</tr>
<tr>
<td>The Chain-Link Fence Model</td>
<td>56</td>
</tr>
</tbody>
</table>
RESEARCH METHODS AND PROCEDURES..........................56

Timeline of Events in the Research.........................57
  Study Design.......................................58
  Details of the Study................................60
  The Process of Interviewing the Subjects..............61
  Criteria for Selection of Subjects’ Interviews......61

THE DEVELOPMENT OF THE CHAIN-LINK FENCE MODEL..........64

  History............................................64
  Creation of the Procedures..........................65
  The Need for a Framework................................69
  Formulation of the Components..........................71
  Buy-In...............................................71
  Ease-Of-Use.........................................71
  Implementation......................................72
  Effectiveness.......................................73

VALIDATION OF THE COMPLETENESS OF CLFM-PART 1: DEEP
INTERVIEWS AND EFFECTIVENESS MEASURE............................76

  Introduction.......................................76
  The Interview Process................................76
  Reception of the Security Procedures....................78
  Buy-In...............................................79
  Implementation......................................83
  Ease-Of-Use.........................................85
  Effectiveness.......................................88
  Summary of Qualitative Validation.......................89
  Numerical Support for Effectiveness....................90
  Data, Nessus Report..................................91
  Analysis of Data.....................................92
  Measuring Conclusions................................94

VALIDATION of CLFM-PART 2: USING THE CHAIN-LINK FENCE MODEL
TO CREATE SECURITY PROCEDURES AT UTAH STATE UNIVERSITY...95

  Procedure Development Using CLFM.......................95
  The Interview Process................................96
  Case Study 1........................................97
Case Study 2.....................................103
Case Study 3.....................................107
Case Study 4.....................................113

Review of Effectiveness of CLFM in Procedure Creation...........................................120
Conclusions of the Case Studies.........................122

FINAL CONCLUSIONS AND DISCUSSIONS.........................124
Summary of CLFM and Its Validation......................124
Conclusions........................................125
Weaknesses.......................................128
Future Research................................129

REFERENCES........................................132

APPENDICES........................................141
A. Timeline of Events............................142
B. Security Setup................................143
C. Interview Questions..........................148
D. Subject Biographies.........................150
LIST OF TABLES

Table 1. Task Force Survey Results.................. Page 68
LIST OF FIGURES

Figure 1. The Chain-Link Fence Model............... Page 54
Figure 2. Developmental Step 1 of The CLFM........ Page 75
Figure 3. Developmental Step 2 of The CLFM........ Page 76
Figure 4. Vulnerable Computers on the Nessus Report Page 95
In the early days of management information systems, network security was not thought of as a necessity because little threat existed. The only computers were mainframe computers, so users only had remote terminal access to run programs. As computers got smaller, dumb terminals were replaced by microcomputers, which eventually evolved into personal computers on every single desk. All those computers were eventually joined together to form the first intra-office computer networks. By the mid-1980s, the DARPA net had evolved from a closed, wide-area computer network consisting of universities and military organizations into the internet (ARPANET, 2012), which is a series of networked computers that are based on open communication protocols to which anyone can join. Applications which run on the internet include email, file transfer protocol, and the World Wide Web. In 1990, CERN invented the World Wide Web (http://en.wikipedia.org/wiki/WorldWideWeb, para. 3).
World Wide Web is an application which uses, at its core, open standards including hypertext transfer protocol to display text and graphics. The World Wide Web brought forth open communication between organizations and people in general. Customers could place orders directly into a company’s computer systems, suppliers and vendors could use shared intranets to keep track of inventory, and library catalogs could be accessed by academics anywhere in the world. This openness and free flow of information would come at a cost, however, as the very system which was the new “information superhighway” also became an “unpoliced back alley” (A. Beckett, 2009) for malicious programmers and hobbyist hackers.

The first major computer security threat was in 1971 (Creeper, 2012). It was the first self-replicating program, later known as a “virus,” called The Creeper. It displayed the text, “I am The Creeper. Catch me if you can.” Because computers were not as networked together, viruses were transferred disk-to-disk by what is now known as a sneakernet: a user would unknowingly take a virus-infected disk and insert it into a computer, which would then become infected. Any disk put in an infected computer would become infected, and an infected disk would infect any computer
with which it came in contact. In 1988, the Morris Worm (Morris Worm, 2012) was the first virus to use the internet to self-replicate and infect multiple computers. It infected 6,000 computers, which at the time, was ten percent of all of the computers connected to the internet. The government estimated the damages to be between $10 million and $100 million. In 1999 the Happy99, Melissa Worm, ExploreZip, and Sub7 viruses permeated the World Wide Web and email (Backhouse, Hsu, & Silva, 2006). The viruses had become so widespread and damaging that it became painfully obvious to the Information Technology (IT) community that network security procedures and systems were needed.

In 1989, the United Kingdom’s Department of Trade and Industry (DTI) started an IT security awareness campaign called "keep IT safe" (Backhouse et al, 2006 p. 418). By 1990 this campaign was recognized throughout Europe. The first European conference on IT security was held in 1992 (Backhouse et al, 2006). The nations of France, Germany, The United Kingdom, and The Netherlands formed the first European multi-national security taskforce, called the Organization for Economic Cooperation and Development (OECD), from which a subgroup was formed, called the
European Security Forum (Backhouse et al., 2006). “There were three of us at the [first] meeting [of the European Security Forum]: the security manager, his director, and myself. At the end of the meeting, we agreed to bring together our key contacts who had expressed interest in security standards in formal and informal meetings. This decision was a very significant step forward in this context” (Backhouse et al., 2006 p. 419).

In 1992 the DTI published a report called Security Breaches Survey (Backhouse et al., 2006), which concluded that UK businesses were losing £1.1 billion annually because of computer security breaches. In 1993 the Abraxas virus, the first major virus that was automatically generated by virus-generating software, was the spark that started the standardization process. Seven UK businesses were involved in drafting the code: BOC group, British Telecommunication, Marks and Spencer, Midland Bank, Nationwide Building Society, Shell International Petroleum, Shell UK, and Unilever (Backhouse et al., 2006). All representatives were high-level security managers. The first draft of what would become industry standard BS7799 was written in only 3 months. It was called “A Code of Practice for Information Security Management,” (Backhouse
et al., 2006) and it became an immediate bestseller for the British Standards Institute. "There was a significant amount of interest in both DISC and BS7799," a high-level security manager interviewed at the time reported. "My company was an IT consulting company, and after both publications were released, and in particular after BS7799, we received a lot of inquiries about BS7799 implementation" (Backhouse et al., 2006, p. 421). Over 10,000 copies were sold in September 1993. The transition from a draft into a ratified standard took place between 1993 and 1995. In 1999 BS7799 was proposed as an International Standards Organization (ISO) standard. This was changed to ISO 17799:2000 on December 1, 2000 (Backhouse et al., 2006).

In 1991, computer security breaches cost U.S. companies 5.5 billion dollars. By 2006, that number was projected to have reached $25 billion (Gal-Or & Ghose, 2005). On October 16, 2001, U.S. President George W. Bush issued executive order 13231, titled "Critical Infrastructure Protection in the Information Age" (Bush, 2001). This executive order specifically called for the implementation of "a voluntary public-private partnership, involving corporate and non-governmental organizations." The partnership was tasked with protecting information
systems infrastructures from disruption or damage. Out of this initiative came the Computer Emergency Response Team (CERT). The group was focused on free sharing of computer security information, and that led disastrously to what Next Generation Software Services claimed was a “violation of trust because information was leaked to potential competitors” (Gal-Or & Ghose, 2005 p. 187). NGSS severed ties with CERT, providing a glaring example of the failure of open communication in resolving security issues. Because of this failure the U.S. market shifted from a governmental policing system to an internal business security system. As a result, many American companies began following the guidelines set forth in ISO17799:2000.

Every U.S. organization, including each university, is now responsible for its own information security and is liable for any breaches. According to data collected from the border firewall flow reports, thousands of Internet-based attacks every second bombard the Utah State University (USU) campus computing community. The implication is that a poorly managed computer with basic security deficiencies can be infected within seconds of connecting to the campus network. A single infected computer is a hazard to the rest of the campus. USU is such
a large, complex environment that demands standardized computer security policies and procedures. A visual
timeline of the proceeding events is located in the appendices (see Appendix A). In February 2008, Utah State
University adopted Computer Management Policy 551, which stated, “All computers connected to the USU Network must be
configured and managed to reduce or eliminate the risk of loss of control of the computer resource or the stored or transmitted information.” The policy mandated university IT to “develop Computer Management Procedures according to industry best practices in collaboration with IT advisory committees and user groups”
(http://it.usu.edu/policies/htm/computer-management-policy, para. 2).

The policy was a good starting point, but without accompanying procedures and recommendations, the Chief Information Officer (CIO) and the USU Central IT Security Team felt it was only a façade of security. In August 2009, a task force was organized for the purpose of creating security procedures which could be enacted to fulfill the requirements of Computer Management Policy 551. The task force comprised volunteers from the campus-wide network managers group. The task force faced a special challenge:
An endeavor like this could not simultaneously be broad enough to account for all computing environments and situations and focused enough to protect the computers most at risk. The task force also faced the challenge of acceptance and implementation of its procedures. If the recommendations were too specific, their application could be deemed too rigid, regularly irrelevant, and rapidly obsolete. A small, vocal group of campus IT stakeholders expressed concern at the university Network Managers meeting that the official procedures could be used to override in-the-field expertise. Others expressed concern that a restrictive policy would equate to restrictions on academic freedom. On the other hand, if the recommendations were too vague, their application could be deemed regularly ineffective, confusing, and even meaningless.

The creation of these procedures took place between August 2009 and March 2010. The task force (Okelberry & Houghton, 2010) comprised representatives of three major colleges, two members of the university central IT department, and one member from the business and finance department. This task force met weekly to determine the scope of systems to be included in the management, the size of the number of recommendations, and the process of
determining the specific recommendations. The task force thought that there were four specific types of computer systems that composed the bulk of the campus network. They were computers that used Microsoft Windows operating systems for high security transactions, specifically users that handled monetary transactions or student records; computers that used Apple Mac OS X for high security transactions; computers that used Microsoft Windows for routine use; and computers that used Apple Mac OS X for routine use.

The final draft was presented to the university management, IT professionals, and the general public at the March 2010 network managers meeting. The procedures were approved by majority, voice vote and went into effect March 15, 2010 (Okelberry & Houghton, 2010).

Throughout this process the task force went to great lengths to ensure that the final recommendations were accurate, dependable, and most importantly, secure. Users of university networks were demanding more and more features to support the myriad of new devices that they were using to communicate. The task force realized early on in the process that it needed to limit the scope in order to accomplish the goal of creating the computer security
procedures. However in going forward, there would be a need for further computer security policies and procedures as always-available communications, on-demand television, and completely connected devices became the standard use of computer networks.

As the issue of computer and network security was ever-changing, there needed to be a streamlined method for creating policies and procedures without having to start over from scratch each time. This methodology needed to be created, documented, and followed to help give uniformity and accuracy to future procedures.

The Chain-Link Fence Model, created by the author, is a resulting methodology for creating information security procedures. It consists of four components: Buy-In, Ease-of-Use, Implementation, and Effectiveness. The components operate in this order: First, one must create Buy-In needs before the procedure can be approved. Next, the procedure is introduced to the users. Ease-of-Use is a major determinant of whether or not the procedure will be followed. Computer managers generally handle the software configuration and training included in Implementation. Lastly, Effectiveness is measured by an audit system.
Purpose Statement

The purpose of this research is to create a framework from which future security policies and procedures can be created. Additionally, this research seeks to establish how to encourage universal adoption of and adherence to the framework, both by designing the framework to be acceptable to the strong majority of users and by shaping the organizational culture of an hierarchical organization into a culture of security. Furthermore, this develops and refines the Chain-Link Fence Model and assesses how it increases the quality of the creation, implementation, and effectiveness of security policies and procedures in a hierarchical organization.

Conceptual Framework

In the creation of these new security procedures recommendations, the author relied on the guidance of theories from the studies of communication and organizational culture.

The theory of Competing Values Model of Organization Culture was adapted to fit the task force's goals. This theory, proposed by Iivari and Huisman (2007), states that
an organization can be classified into one of four main cultures:

1. Group culture: change, internal focus. Human relationships and flexibility

2. Development culture: change, external focus. Future oriented, considering what might be

3. Rational culture: stability, external focus. Achievement oriented, focused on productivity

4. Hierarchical culture: stability, internal focus. Security, order, routing, following regulations

(Iivari & Huisman, 2007, p. 37)

When presented with these points during its meetings, the task force members agreed that Utah State University fit within the Hierarchical culture classification. In accordance with the organizational culture model, the task force concluded that they would need to achieve a level of Buy-In among information systems (IS) administrators from all units around the institution in order to accomplish its goal of creating a system of security for Utah State University. The theory helped shape the focus of the task
force and its goals by giving specific methods to present
the proposed security procedures.

Several themes emerged from the review of the task
force meeting notes. These themes were interwoven into a
model to help define information systems security as a
whole for hierarchical institutions. These themes became
components of the Chain-Link Fence Model of Information
Systems Security. This study analyzes and validates the
Chain-Link Fence Model of Information System Security
Policy and Procedure Creation.

**Original Contribution**

The contribution to the general IS knowledge base of
this research is the development, validation, and analysis
of the Chain-Link Fence Model of creating Information
System Security Procedures. After reviewing relevant
literature to date, no other comprehensive framework has
been established to observe this procedure in a large
organizational setting.

**Layout of the Dissertation**

The first section is a review of literature explaining
the history and current state of information technology
security as well as a look into the creation of policy, procedures, or industry standards. Next is the presentation of the Chain-Link Fence Model, the full description, and its development. The third section is the establishment of the methods and procedures followed by the researcher. This includes the timeline of events and the study design consisting of two parts: 1) deep interviews with three members of the university information technology department and 2) the case study interviews with four lab managers.

The following section outlines the development of the Chain-Link Fence Model. This includes the history of security at Utah State University, creation of security procedures, the need for replication, the formulation of components, and how it links to prior research.

This study next reports the specifics of the deep interviews. In part one of the study, three subjects discussed their experience with components of the Chain-Link Fence Model and how it helped develop the new USU security procedures. Part two presents the validation of the model as a whole. Four start-to-finish case studies validate the entire model. Finally the study concludes with the summary of findings, a discussion of any weakness of the study, and a call for further research.
REVIEW OF THE LITERATURE

Many studies have been conducted on a wide range of topics to help information security professionals obtain their goals of mitigating security threats in their own organizations. In order to help future security professionals, it is important to see the current state of research into information technology security. This literature review looks into research in the field of information technology security.

The objectives for this literature review are:

1. to explore the evolution of information technology security;
2. to discuss the research into the creation of policy, procedures, or industry standards, the results of that research, and their effect on information technology security; and
3. to discuss conclusions drawn by previous research.

Review Procedures

In order to sort the broad array of topics found in the search, the papers were coded using a system developed to help identify the type and conclusion of the study. Based upon the coding system, the papers were included in
or discarded from this review. The papers included in this review all have characteristics that relate to the creation of security policy and procedure.

**Locating the Papers**

Papers were located using a search of JSTORE, Business Source Premier, and Google Scholar. Ninety-eight papers were identified that are relevant for this research via this search. The author’s discussion with his major professor led to another recent paper. From this paper two other references were obtained.

The keywords for the Internet searches are as follows: Management information security, security policy, security policy creation, security procedures, security procedures creation, information technology security, technology security management, Internet security policy, Internet security procedures, network security, management network security, network security policy creation. The papers included in this review needed to meet the following criteria:

1. they needed to be referenced by a scholarly source or
2. they needed to be referenced by two other papers
that met the first criteria.

This process identified 95 papers for reference in this review.

The History and Current State of Information Technology Security

Mustonen-Ollila and Lyytinen (2003) studied IS process innovation from 1940 through 1997. Their paper gave a brief history of information technology. It addressed the issues that faced information technology professionals including the beginnings of information security. Due to the nature of the research, a case study methodology was used. They identified four generations: Gen 1 (1940-1960) dealt mostly with hardware constraints, Gen 2 (1960-1980) dealt with software constraints, Gen 3 (1980-1990) dealt with user relationships and Gen 4 (1990-present) dealt with organizational constraints. “The most important items in these factors observed to influence adoptions were: user need recognition, technological infrastructure, past technological experience, own trials, autonomous work, ease of use, learning by doing and standards” (Mustonen-Ollila and Lyytinen, 2003, p. 293).

Overall, IS process innovations are expected to
improve the quality and productivity of IS development where the products – ISs – are defined as systems of hardware and software capable of digital information storage, processing and communication that can serve some organizational functions or purposes. (Mustonen-Ollila and Lyytinen, 2003, p. 276)

One of the largest constraints in developing security process was discussed by Kotulic and Clark (2004). They conducted a survey to determine whether their proposed security model would have any success. “Information security research is one of the most intrusive types of organization research, and there is undoubtedly a general mistrust of any ‘outsider’ attempting to gain data about the actions of the security practitioner community” (Kotulic and Clark, 2004, p. 604). The response rate to the questionnaire was 5.1%, which was statistically not enough to conduct an analysis. They surmised that the scope was too large and the population too diverse.

Historically, threats and vulnerabilities have not been considered until after a security breach had occurred. The goal of risk management is to maximize possible gain while minimizing possible loss. The risk management process must be a cost-effective, nontechnology driven, value creation process that contributes to the overall effectiveness of the organization. (Kotulic and Clark, 2004, p. 598)

They also concluded that because of the secrecy nature of
IT, security companies were reluctant to share data.

Firms are unwilling to divulge such information without strong assurances that the information provided will in no way harm them, yet could provide insight in how to improve their organization. Time is far better spent focusing on a few, select firms with whom the researcher has developed an excellent rapport and trust. (Kotulic and Clark, 2004, p. 605)

They recommended further studies to advance the study of IT security.

While actual security breaches are rarely reported, spyware (software written for the purpose of gaining information about their target) attacks have been widely reported and analyzed by researchers. Warkentin, Luo, and Templeton (2005) were among the first to discuss the rising threat of spyware to government and the resulting incentive for lawmakers to create anti-spyware laws.

Many spyware components use the veiled approach of placing the intention to monitor notification within End User License Agreements (EULAs) immediately before the installation of other programs. But because users commonly accept the EULAs without being aware they are installing software that will monitor their activities, there may be consent without awareness, certainly not true informed consent. (Warkentin, Luo, and Templeton, 2005, p. 80)

They comment that legislators do not fully understand the problem. "Confusion over spyware has caused many companies
to refrain from adequately implementing spyware solutions. Spyware is not understood as well as other security threats (such as P2P, viruses, worms, and hacking)” (Warkentin, Luo, and Templeton, 2005, p. 84). In conclusion, they ask, “Why are the distinctions between positive and negative consequences important? If legislators enact laws without clear specification, unintended outcomes could ensue” (Warkentin, Luo, and Templeton, 2005, p. 83).

Most current businesses do not realize the potential for network security breaches. Herath and Rao (2009) stated, “We, however, found that the certainty of security breaches does not have a significant impact on the security concern” (Herath and Rao, 2009, p. 117). Along those lines, LaRose, Rifon, and Enbody (2008) stated that “four-fifths of all home computers lack one or more core protections against virus, hacker, and spyware threats” (LaRose, Rifon, and Enbody, 2008, p. 71).

Sriramachandramurthy, Balasubramanian, and Hopis (2009) used a survey to determine how users protect themselves from spyware and adware.

Spyware refers to applications that include adware which may be installed without an end-user's consent, with the goal of tracking and collecting personal information without consent ... [We] define adware as computer-
resident software applications that serve pop-up windows with advertisements that are not related to, or authorized by, the Web sites an individual chooses to visit. (Sriramachandramurthy, Balasubramanian, and Hopis, 2009, p. 42)

They found that there are two main components to security: technical (firewalls, security software suites) and risk-avoidance (not going to questionable websites, not using p2p software.) They hypothesized that users with a greater technical knowledge, greater security awareness, higher experience, and greater confidence in their own skills were more likely to use defensive measures to protect themselves and their computers. They found their hypotheses to be statistically valid.

Vroom and von Solms (2004) detailed how IT auditing was currently working, namely auditing the validation of data. The authors stated that from IT auditing grew a subset called IS security auditing, which audits the policies and procedures of the organization and not just the technology. “As organizations have expanded globally, auditing the financial transactions only is no longer enough” (Vroom and von Solms, 2004, p. 192). The authors further stated that human factors were not being addressed.

For example, if an unauthorized employee attempts to access information, the audit logs will record this. Unfortunately, it may go undetected until
the auditor reviews the documentation. The results of the employee’s behavior and actions have been detected and audited, but not the behavior itself ... According to the 2001 Information Security Industry Survey, of all the security breaches perpetrated by the employees of the organization, 48% of them were accidental. This demonstrates that not all security breaches are maliciously intended, but may be the result of negligence or ignorance of the security policies of the organization. Of the remaining security breaches, 17% was intentionally committed, and of the other 35%, it was [sic] unsure whether it was malicious or not.” (Vroom and von Solms, 2004, p. 193)

The authors suggested that by changing the culture of the organization, security could be enhanced. “A utopian information security culture would be where the employees of the organization follow the guidelines of the organization voluntarily as part of their second nature” (Vroom and von Solms, 2004, p. 195).

Gal-Or & Ghose (2005) stated, “IT executives revealed that they were more concerned with the ripple effects of online security breaches on consumer confidence and trust in e-business than the actual financial losses of physical infrastructure” (Gal-Or & Ghose, 2005, p. 197).

Dinev and Qing (2007) reported that:

computer viruses, spyware, cyber attacks, and computer system security breaches are daily occurrences. In the ten year period from 1993-2003, the number of security incidents reported
to CERT increased from 1,334/year to 137,529/year. In order to effectively manage and control the ever-evolving and growing security threats, it is obviously not enough just to rely on deployment of security technologies such as anti-virus and intrusion detection software and hardware. (Dinev and Qing, 2007, p. 387)

At the beginning of the recession of 2009, Hoffman (2009) interviewed security analysts about whether or not the recession would cause any changes to information security. All the analysts interviewed recommended to purchase security software. Brian Fuher, a program manager of SoftwareOne stated, "'[The reason to install antimalware] is the same reason we're probably buying insurance on our cars. The cost of damage is so great ... It's low-risk, high-reward. It's low-cost and such a great devastation if you get successfully attacked'" (Hoffman, 2009, p. 2). Sean Stenovitch, a partner with M&S Technologies, is quoted, "'In a down economy, desperation is going to create even more of a security risk.'" He concluded, "'[What] it really boils down to [is that] customers have to have security. They have to have protection'" (Hoffman, 2009, p. 1).

Tittle (2005) introduced the concept of a Managed Security Services Provider (MSSP). These MSSPs are useful for small to medium size organizations that cannot employ an internal IT security team. An MSSP is an outsourced
security company that conducts both security evaluations (audits) as well as active monitoring for other organizations. "An MSSP is a third party that works with clients to assess and define security needs, evaluates any security policies, practices and procedures in place, and then implements and maintains a security infrastructure on its clients' behalf" (Tittle, 2005, p. 20).

Manning (2010) refers to using Software as a Service (SaaS) to help mitigate and outsource IS security. The article details how SaaS systems can integrate and fulfill government regulations. "Preservation of principal and value is another headline risk management concern for treasurers" (Manning (2010), p. 2). "Technology has provided a solution via bureau-based 'soft-ware as a service' (SaaS) options that allow companies to outsource their SWIFT messaging processing to a third-party for a service charge plus transaction costs, avoiding the need to manage the necessary infrastructure in-house" (Manning, 2010, p. 1).

The Institute of Management and Administration (IOMA) (2002) details fully automated security systems. The author predicts that by 2015 robot security guards will start to become economical compared to their human equivalents. This
futuristic technology is already one of the primary tools used by the military for combat surveillance. "While the U.S. military has for years used robot patrols to monitor warehouses and other indoor environments, they are investing significant resources to improve the technology so they can conduct outdoor patrols of airport grounds, military compounds, and fuel storage facilities" (IOMA, 2002, p. 6).

Herath and Herath (2009) stated that in 2007, 74% of organizations reporting attacks confirmed that the source of the attack was a virus or other malicious code. "Given the importance of computer and information security, investment in information security is now recognized as a critical issue by both practitioners and academics alike (Herath and Herath, 2009, p. 338)." "Information security projects have high-risk characteristics due to the changing threats to IT systems and the uncertainty associated with potential breaches" (Herath and Herath, 2009, p. 343). They concluded the following:

If the first security investment is undertaken, the manager can undertake the second information security investment ... at any time between years 1 and 3. If both the first and second information security investments are undertaken, the manager can invest in a third platform information security investment ... anytime between years 3
and 5. (Herath and Herath, 2009, p. 359)

The Security Director's Report of IOMA in August of 2009 summarized new data about technology-based security systems. The report found that, despite prevailing beliefs about these systems, technology alone does not prevent IS crime.

In fact, property owners are so confident that these new, high-end systems will deter crime, few of them make an effort to validate the effectiveness of the systems they've implemented—perhaps, because no one wants to find out they just spent a lot of money for nothing. (IOMA, 2009, p. 1)

"The fact that researchers could find no proof of the systems’ [sic] ability to cut crime should give security executives a moment’s pause" (IOMA, 2009, p. 13). They concluded, "We found no persuasive evidence that the introduction of CCTV [closed circuit television] and ancillary electronic monitoring equipment to [the subject complex] in Manhattan reduced the incidence of crime in [it]” (IOMA, 2009, p. 15).

Though not prosecutable in criminal court, use of spyware is harmful, and attempts have been made to prosecute it in civil court. Oser (2004) discussed court proceedings against Claria Corp and WhenU.com. The article stated how the defendants produced spyware and provided ad
services across the internet. As of 2004, they were on the
verge of having an initial public offering (IPO).

Claria Corp. and WhenU.com, the two largest companies that produce the free, downloadable software called "ad ware," are increasing their profits year after year. Claria, the Redwood City, Calif., leader, which filed to go public in April, had $90.5 million in revenue in 2003 and is expected to enjoy a 30% expansion in revenue in 2004. Claria's main competitor, WhenU, is profitable and on its way to $50 million in gross revenue in 2004, according to CEO Avi Naider. (Oser, 2004, para. 3)

"Top advertisers across the pop-up space, as compiled by Nielsen/NetRatingsAdRelevance, range from bottom feeders such as LowerMyBills to blue-chip brands such as American Express" (Oser, 2004, para. 5).

The Process of the Creation of Policy, Procedures, or Industry Standards and their Effects on Information Technology Security

Organizations combat the aforementioned threats by creating security policies and procedures. The first procedures focused on the technology. As the threats changed, the policies and procedures shifted from technology-based to human-based solutions. Adams and Sasse (1999) first studied password schemes. The authors used a
web based questionnaire to study password systems. The questionnaire focused mainly on password related user behaviors (password construction, frequency of use, password recall, and work practices). They found that most users did not think that their job was high enough to warrant any effect on a breach of their account. They also found that users did not understand the authentication process, and that most confused the username with the password, thus trying to make their username as complex as their password and forcing further confusion. “Constantly changing passwords” were blamed by another employee for producing “...very simple choices that are easy to guess, or break, within seconds of using ‘Cracker’ Hence there is no security” (Adams and Sasse, 1999, p. 42). A cracker is a type of software program used to break passwords, either through brute force or by analytical attack. “Since security mechanisms are designed, implemented, applied, and breached by people, human factors should be considered in their design. It seems that currently, hackers pay more attention to the human link in the security chain than security designers do, for example, by using social engineering techniques to obtain passwords” (Adams and Sasse, 1999, p. 41)"
Sasse, Brostoff, and Weirich (2001) did not want to lay the blame solely on users. They argued that users should not be blamed for being the “weakest link” in the information security process. They stated that environment and lack of training were larger issues that need to be addressed. “Security has largely ignored usability issues; many users of security systems face unattainable or conflicting demands, and receive no support or training” (Sasse, Brostoff, and Weirich, 2001, p. 123).

BT security staff believed that the rising number of password resets was due to a small number of careless ‘repeat offenders’ — by their own definition, employees who ask for a reset 6 or more times a month. Study 2 found that 91.7% of resets were caused by ‘normal users’, i.e. more than 90% of users cannot cope with the password mechanism in the way they were expected to, which is a rather damning result in terms of usability of password mechanisms. (Sasse, Brostoff, and Weirich, 2001, p. 125)

“Consequently, security must be designed as an integral part of the system that supports a particular work activity in order to be effective and efficient” (Sasse, Brostoff, and Weirich, 2001, p. 128).

Spears and Barki (2010) stated:

It is widely believed that organizational efforts to manage IS security are typically focused on vulnerabilities in technological assets such as hardware, software, and networking, at the expense of managing other sources of
vulnerabilities, such as people, policies, processes, and culture. (Spears and Barki, 2010, p. 503)

"Users are likely to be more attentive when IS security is something to which they can relate" (Spears and Barki, 2010, p. 518).

Users can also allow themselves to become the gateway to security breaches. Bose and Leung (2007) found that five percent of people responded to phishing emails. A phish is when a hacker uses directed and customized message to entice a user to give private information. They stated: "Being a part of the global community, both corporations and individuals have certain social responsibilities to fight phishing" (Spears and Barki, 2010, p. 566).

Gillespie (2009) reported that, while CIOs realize that security is one of the high agenda items on their lists, they do not fund security studies, reports, or audits. "They must attract key stakeholders to Buy-In to security from the off, in order that any corporate security policies generated are received from the whole company" (Gillespie, 2009, para. 9). "Security, information management, and information risk management should stop being seen as a costly add-on and in some cases a 'perk'." "Instead, they need to be seen as fundamental core business
Cremonini and Nizovtsev (2006) focused on analyzing the behavior of the attacker to gain an understanding of how to concentrate on network security. "Viewing attackers as rational agents is consistent with several theoretical and empirical studies" (Cremonini and Nizovtsev, 2006, p. 1). "Any given security measure affects the frequency of intrusions through two mechanisms ... one is the increased ability of a target to withstand attacks of a given intensity. The other effect ... occurs through a change in attackers' perception of the target in question" (Cremonini and Nizovtsev, 2006, p. 2). "The main purpose of investing in security is to defend against malicious attackers" (Cremonini and Nizovtsev, 2006, p. 4). "Our analysis suggests that the magnitude of the behavioral effect can greatly exceed that of the direct one" (Cremonini and Nizovtsev, 2006, pp. 21-22).

Rees, Bandyopadhay, and Spafford (2003) proposed a framework for creating short-term security policies. They focused upon the fact that information technology changes rapidly and that security polices, when created, will outlive their useful life-cycle. Their model focuses upon constant feedback. After every ideation of the development
they consult their stakeholders for feedback. “Because policy development is an iterative process, the model includes feedback loops at every step” (Rees, Bandyopadhay, and Spafford, 2003, p. 102). They found that if one builds short-term policies “the security infrastructure” is more likely to be built on time and to meet requirements (Rees, Bandyopadhay, and Spafford, 2003, p. 102). This results in a Buy-In from their stakeholders as well as the ability to revisit the policy. “A security policy that is not constantly evaluated and updated is of no value” (Rees, Bandyopadhay, and Spafford, 2003, p. 105).

GoodHue and Straub (1991) studied user behavior concerning security models. The authors identified four issues:

1. as risk increases, users negative perceptions of security measures decrease;

2. as more resources are used to increase security awareness perceptions of satisfaction with security increases;

3. users who are more computer savvy will have lower levels of satisfaction with current security; and

4. risk and company action is affected by user awareness.
“Although I/S [sic] managers have at least marginal concerns about security, non I/S [sic] managers seem to be less concerned” (GoodHue and Straub, 1991, p. 118). They argued that “insufficient computer and data security is a major problem in many organizations, [sic] and that low levels of concern contribute to the danger” (GoodHue and Straub, 1991, p. 124).

Weirch and Sasse (2002) interviewed users to find how they responded to security threats and password policies at their institutions. The authors found that most of the users did not have enough insight into security threats to use good judgment in challenging password policies. “Users cannot be forced to behave in a proper fashion, but an effort to persuade them to do so has to be made” (Weirch and Sasse, 2002, p. 143). “In addition, many users are not sufficiently educated about security issues. Thus, many users construct their own, often wildly inaccurate models of security threats and the importance and effective deployment of security measures” (Weirch and Sasse, 2002, p. 137).

Anderson and Agarwal (2010) took a unique view into the direct realm of the home user. They focused on home users because: “In late 2005, a watershed event occurred in
the worldwide penetration of information and communication technology: the number of computer users with Internet access crossed the one billion mark” (Anderson and Agarwal, 2010, p. 614). They conducted a study of local internet service providers (ISP) users, and when they did not receive enough replies for a proper representation, added undergraduate students at a large university as a sample. They concluded that “the factors influencing home computer users’ attitude toward security-related behavior include concern about security threats, self-efficacy, and perceived citizen effectiveness that, in turn, influence security behavior. Security behavior is also influenced by psychological ownership and subjective and descriptive norms” (Anderson and Agarwal, 2010, p. 630).

Workman, Bommer, and Straub (2008) conducted a study to gauge how much people thought about security threats and how well they coped with them. The authors found that when people had a higher perception of security threats, they took more precautions, and when they had a higher level of coping, they again took more threats seriously. “Coping depends on whether people feel that their ability to take security actions have been reasonable (self-efficacy), providing that they perceived that the threat is
preventable in the first place (locus of control)” (Workman, Bommer, and Straub, 2008, p. 2802). However, they found that “fear appeals can be counter-productive. When there are excessive false-positive alarms, people will tend to discount fear appeals” (Workman, Bommer, and Straub, 2008, p. 2812).

Herath and Rao (2009) proposed a framework for security deterrence. They modeled this framework upon criminology general deterrence theory, theory of planned behavior, and procession motivation theory. The authors conducted a survey of 312 respondents representing 78 organizations. The framework focused upon changing attitudes about security perceptions throughout the organization because “although organizations actively use security technologies and practices, information security cannot be achieved through technological tools alone” (Herath and Rao, 2009, p. 106). They found that “Most organizations spend time and resources to provide, establish, and monitor computer security policies; however, if the end-users of organizational IS are not keen or willing to follow the policies, then these efforts are in vain” (Herath and Rao, 2009, p. 118). “We, however, found that the certainty of security breaches does not have a
significant impact on the security concern ... More
importantly, it is necessary for IT management to
communicate the reality of security threats to
organizational end-users” (Herath and Rao, 2009, p. 117).

Grossklags, Christin, and Chuang (2008) used game
theory from economics to explain hacker behavior and
possible solutions. Game theory is the study of how people
make strategic decisions.

Economics as a tool for security analysis has
gained in importance since the economy of
attackers has become ... motivated by greed over
the last years. This [is] in contrast to that
exhibited by the hacker communities of the 1980s
and 1990s, who valued reputation, intellectual
achievement, and even entertainment above
financial incentives. (Grossklags, Christin, and
Chuang, 2008, p. 3)

The authors identified two key components of a security
strategy: “self-protection (e.g., patching system
vulnerabilities) and self-insurance (e.g., having good
backups)” (Grossklags, Christin, and Chuang, 2008, p. 4).
The authors continued, “we model security as a hybrid
between public and private goods” (Grossklags, Christin,
and Chuang, 2008, p. 6). The computation of the protection
level will often take the form of a public goods
contribution function. Because network protection is a
public good, it may allow, for certain types of
contribution functions, individuals to free-ride on others’ efforts. “Agents have two security actions at their disposal. They can contribute to a network-side protection pool or invest in a private good to limit losses” (Grossklags, Christin, and Chuang, 2008, p. 33). At the same time, some individuals may also suffer from inadequate protection efforts by other members if those have a decisive impact on the overall protection level.

One of the most forceful industrial standards is that of the health care industry. Bresz (2004) discussed security frameworks in the context of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The article explains how to implement new security training programs that are compliant with HIPAA. The four main points of HIPAA in regard to IS security are security reminders, protection from malicious software, log-in monitoring, and password management.

If you do not plan to start a “reasonable and appropriate” security awareness and training program fairly soon, then your people will continue to be your weakest link in information security, and your organization may be at risk of not being in compliance with the HIPAA Security Rule as of April 21, 2005. (Bresz, 2004, p. 57)

"While a technology can be used to guard against malicious software and can aid in the detection and reporting aspects,
it is ultimately a personal responsibility to be aware of software anomalies and to report them” (Bresz, 2004, p. 58).

“Sound security needs to be something your organization’s personnel ‘live and breathe’ everyday. It must become an integral part of the company culture, with management sending the right message” (Bresz, 2004, p. 60).

Another major industry pursuing information technology security standards is the payment card industry (PCI). According to Kim (2011), standards such as HIPAA and PCI are the primary motivation for organizations to adopt security innovations. PCI compliance has been in the forefront for security experts due to the fact that most businesses-to-customer transactions utilize either a debit or credit card. Vijayan (2008) interviewed Hannaford, a New England grocer, about their upgrading to a PCI-compliant network. He questioned whether or not it is enough just to have new systems, or if there are other factors.

Despite the lack of more stringent requirements, encrypting card numbers on point-of-sale devices is "the most significant action" that retailers can take to stop attacks such as the one that hit Hannaford, said Gartner Inc. analyst Avivah Litan. But that doesn't necessarily mean that the new security measures will make Hannaford — or other companies that follow its lead — immune to future attacks. (Vijayan, 2008, p. 14)

He concluded: “The unanswered question, though, is whether
that will put up a wall strong enough to keep future attackers out" (Vijayan, 2008, p. 14).

Beckett (2005) discussed the concept of information security in the field of music. This was a new concept that producers faced. The producers found that they needed to secure their events for the masses that use the wireless spectrum to conduct the business of concerts.

"Wireless networks are increasingly deployed at [concerts], as they are ideal for locations that lack existing infrastructure. But these too demand the highest levels of security," said Simons, a producer with Mean Fiddler. Because of the increasing threat, they disable all floppy and CD drives both for festival and permanent office use. All devices handed out to staff are anti-virused and pre-configured. "There's no chance of anyone being able to load any untoward software," Simons said. All devices are "ringed" and loaded with standard software. (Beckett, 2005, para. 15)

Scholz (2009) discussed how even security professionals make the basic mistakes. The author focused on scope as one of the main problems that professionals face. "Information system boundaries can be confusing and are seldom identified fully" (Scholz, 2009, p. 35). He concluded, "No matter how you are structured, you must have management buy in or you have nothing!" (Scholz, 2009, p. 33).

Burke (2006) detailed shoppers' concerns when
purchasing goods from a website. The author reviewed information gathered by Hewlett Packard (HP) about load times and Consumer Reports about privacy policies. He discussed third-party logos, such as Verified by Visa or Protected by McAfee, and how those logos increased consumer confidence in the websites on which they appeared.

"Encouraging consumers to trust your Website involves committing time and resources to communicate the safety of your site, the professionalism of your operation, and the credibility of your brand" (Burke, 2006, p. 42).

Yeh and Chang (2007) proposed a four-factor framework for creating measurable IS security. They surveyed 1000 Taiwanese IT professionals across 4 major industries: general manufacturing, high-tech, banking, and retail. The results showed that across the board, IS networks had the greatest threat severity in all categories. "Often the benefits of security are not considered important until a security breach has occurred" (Yeh and Chang, 2007, p. 489). "This study also considered the scope of countermeasure adoption; it did not appear to be commensurate with the severity of the perceived IS threats" (Yeh and Chang, 2007, p. 482). They found that "security adoption tends to be a need-pull innovation rather than technology-push. As a
result, organizations probably only adopt new countermeasures when their security methods appear insecure” (Yeh and Chang, 2007, p. 490). Their conclusion stated, “[Service based industries] should emphasize their security policy development and allocate security accountability” (Yeh and Chang, 2007, p. 491).

Von Solms and von Solms’ paper (2004) discussed the “10 sins of information security.” These sins were created from the authors’ perspective as security officers for the central bank of South Africa. The sins were simply presented and not researched. They were:

1. not realizing that information security is a corporate governance responsibility (the buck stops right at the top);
2. not realizing that information security is a business issue and not a technical one;
3. not realizing the fact that information security governance is a multi-dimensional discipline (information security governance is a complex issue, and there is no silver bullet or single “off the shelf” solution);
4. not realizing that an information security plan must be based on identified risks;
5. not realizing (and leveraging) the important role of international best practices for information security management;
6. not realizing that a corporate information security policy is absolutely essential;
7. not realizing that information security compliance, enforcement, and monitoring are absolutely essential;
8. not realizing that a proper information security governance structure (organization) is absolutely essential;
9. not realizing the core importance of information security awareness amongst users; and
10. not empowering information security managers with the infrastructure, tools, and supporting mechanisms to properly perform their responsibilities.

Da Veiga and Eloff (2007) proposed a framework for information security governance. They focused their framework on developing a security culture. “To inculcate an acceptable level of information security culture, the organization must govern information security effectively by implementing all the required information security
components.” (Da Veiga and Eloff, 2007, p. 361)

As time went by, the “technical people” in organizations started to realize that management played a significant role in information security and that top management needed to become involved in it too (Von Solms, 2000). This led to a second phase, where information security was incorporated into organizational structures. (Da Veiga and Eloff, 2007, p. 362)

They also stated, “Security policies, procedures, standards, and guidelines are key to the implementation of information security in order to provide management with direction and support (ISO 17799, 2005) and they should clearly state what is expected of employees” (Da Veiga and Eloff, 2007, p. 369).

Stanton, Stam, Mastrangelo, and Jolton (2004) analyzed end-user behavior. They surveyed 1,167 people in the U.S. about their use of passwords and how they responded to password policies. “Appropriate and constructive behavior by end users, system administrators, and others can enhance the effectiveness of information security while inappropriate and destructive behaviors can substantially inhibit its effectiveness” (Stanton, Stam, Mastrangelo, and Jolton, 2004, p. 2). “First, our survey suggested that end users have a rather dismal record of enacting the basic hygiene behaviors that security experts suggest are
important in maintaining the safety of user accounts (e.g., frequent changes to one’s password)” (Stanton, Stam, Mastrangelo, and Jolton, 2004, p. 8). “Through careful analysis of end user security-related behaviors, organizations can help to ensure that workers have the motivation and knowledge to follow the policies that the organization sets to promote its security agenda” (Stanton, Stam, Mastrangelo, and Jolton, 2004, p. 9).

Furnell, Dowland, Illingworth, and Reynolds (2000) surveyed users about authentication behavior. They discussed a lack of user understanding of authentication and stated that authentication was easily compromised. They discussed a replacement of authentication systems: “If the password approach is to be replaced or supplemented, then alternative means of authentication are clearly required. However, when considering such alternatives, a number of factors can be cited that may complicate their adoption:

• Effectiveness (i.e. the ability to detect impostors, whilst allowing legitimate access).
• Cost (i.e. financial overheads of deployment).
• User acceptance (i.e. the friendliness and transparency of the measure).” (Furnell, Dowland, Illingworth, and Reynolds, 2000, p. 529)
They concluded that “overall, a significant factor in the acceptance of alternatives to the password will be that of education. If people can be shown that newer authentication techniques are safe, reliable and secure, then their acceptance is likely to be improved” (Furnell, Dowland, Illingworth, and Reynolds, 2000, p. 538).

Charndra and Calderor (2005) proposed using biometrics as an enhanced security measure to positively identify users in high security areas. They predicted that biometrics will become more standardized as time goes on. The authors proposed six categories that stand in the way of full implementation: Technical, Legal, People (Trust and confidence), Business (Cost and control), Operation (Lab vs. real world), and Systems (integration with existing security measures). “The very connectivity that enhances global business increases vulnerability and exposure associated with attacks on computer systems” (Charndra and Calderor, 2005, p. 102). “Protection of information resources must involve a process that unambiguously identifies and authenticates users” (Charndra and Calderor, 2005, p. 102).

Cryptography is one method of ensuring that network communication stays private. Stix (2005) said, “The
challenge modern cryptographers face is for sender and receiver to share a key while ensuring that no one has filched a copy" (Stix, 2005, p. 1). Based on his study, network managers face a difficult task in ensuring that the appropriate key is sent to the correct people without publishing it across the Internet. "The current uses for quantum cryptography are in networks of limited geographic reach" (Stix, 2005, p. 3).

Backhouse, Hsu, and Silva (2006) showed how power is part of the standardization process. They studied the work of Stewart Clegg, who related power to a circuit. "The episodic circuit emphasized actions and changes in the organizational context. It manifests when an A makes a B do something the latter would otherwise not do" (Backhouse, Hsu, and Silva, 2006, p. 415). Just as electricity flows through an electrical grid, power also flows between social relations, working practices, and techniques of discipline.

Changes in power come from external forces like regulations, mimetic forces, or changes in industry. These changes in power cause people to go through obligatory passage points (OPPs). OPPs are exactly what A wants B to do (e.g., if B wants access to a document, A requires him to use a username and password). The authors used a case
study to conduct their research. They studied a British company transitioning from the standard BS7799 to ISO 17799. The term of the study was September 2003 to March 2004. The primary source of data was from interviews via telephone, via email, and in person, in that order. The interviews used validation criteria defined by Klein and Myers (1999). The authors’ findings suggested that the standard became an OPP when business B required A to adhere to the standard when dealing with business B. This again shows the external forces required when an OPP is in place.

The Organization for Economic Co-operation and Development's (OECD's) Guidelines for the Security of Information Systems and Networks suggested four tasks that management needed to perform: 1) state the policy, 2) direct action plans, 3) review results, and 4) take corrective action.

They further outlined nine principles that provide a comprehensive framework for information security: 1) awareness, 2) responsibility, 3) response, 4) ethics, 5) democracy, 6) risk assessment, 7) security design and implementation, 8) security management, and 9) reassessment.

1. Awareness: Participants should be aware of the need for security of information systems and networks
and of what they can do to enhance security

2. Responsibility: Everybody is responsible for security

3. Response: Everybody should act quickly and courteously to prevent, detect, and respond to security incidents

4. Ethics: Everybody should respect the legitimate interests of others

5. Democracy: The security of information systems should be compatible with the values of a democratic society

6. Risk assessment: Each aspect of operations is reviewed.

7. Security Design and Implementation: Follow the system development life cycle (SDLC) established by the company

8. Security management: Ensure that proper people are employed to follow both extremely scripted actions as well as outside-the-box thinking

9. Reassessment: Always follow up with auditing. (OECD, 2002, Section III, para. 2)

Cavusoglu and Raghunathan (2004) proposed that traditional decision theory-based approaches to security
create a dichotomy to the false-positive or false-negative rate of security systems (as one decreases, the other increases). They proposed using game theory as the basis of designing a security system due to the fact that outside threats use human intervention and not just an uncertain response.

Although the decision theory–based approach can provide a useful starting point for managing risk in settings where potential for fraud exists, we argue in this paper that this method is incomplete because of the problem’s strategic nature ... Hackers do not randomly select their targets. They rationally make their choices based on how much effort will be required to succeed in hacking, the probability of getting caught, and the possible penalty. (Cavusoglu and Raghunathan, 2004, p. 132)

Cavusoglu, Raghunathan, and Yue (2008) also used Game Theory to predict investment in IT security. They found that using game theory had a higher payoff than using decision theory approaches except when hacker activity levels were precisely estimated.

The reason for the limitation of traditional models, when applied to analyze IT security problems, can be stated as one simple proposition: They do not allow a firm’s security investment to influence the behavior of hackers. On the contrary, behavioral influences of security technology on hackers have long been recognized by researchers and practitioners in the security community. (Cavusoglu, Raghunathan, and Yue, 2008, p. 283)
Straub and Welke (1998) discussed risk, specifically loss based upon systems risk. This risk can be managed when managers are keenly aware of the full range of risk and the most effective controls to that risk. "The key to [managing risk is] successfully deterring, preventing, and detecting abuse as well as pursuing remedies and/or punishing offenders for abuse" (Straub and Welke, 1998, p. 445).

Davis (1989) proposed the Technology Acceptance Model (TAM). TAM dealt with how users responded to new technology. Davis found that users adapted new technology if it was easy (ease-of-use) and useful (help in their jobs).

Fang, Chan, Brzezinski, and Xu (2006) used the Technology Acceptance Model (TAM) to explain wireless technology acceptance. They categorized the tasks performed on wireless handheld devices into three categories: (1) general tasks that do not involve transactions and gaming, (2) gaming tasks, and (3) transactional tasks. They found that use of wireless handheld devices was increasing in all of these categories. Especially as these devices were used for electronic commerce, personal and financial information became more vulnerable. One of their conclusions was that "The future of electronic commerce depends on controlling information security threats, enhancing consumer security
perceptions, and building trust” (Fang, Chan, Brzezinski, and Xu, 2006, p. 129).

Rotchanakitumnuai and Speece (2009) used TAM in the context of internet securities trading. They examined the antecedents of perceived usefulness and explored the role of trust and attitude of securities investors toward usage. The behavioral intention of investors to use the internet securities trading service was influenced by perceived usefulness, attitude toward usage, and trust. “In addition, trust is important at all levels of the TAM” (Rotchanakitumnuai and Speece, 2009, p. 1069).
DESCRIPTION OF THE CHAIN-LINK FENCE MODEL

Establishment

The Chain-Link Fence Model of security procedure creation was derived from the need to establish a streamlined method of creating security procedures at Utah State University. Based on a review of current literature, some studies discussed a need for more security. Other papers proposed better security through various methods, such as increasing user trust of IT professionals, proposing specific technologies, and creating management Buy-In. None of the studies detailed how an organization should go about creating security procedures. The contribution of this study to the general IS knowledge base will be the development, validation, and analysis of the Chain-Link Fence Model for the creation of Information System Security Procedures. According to the preliminary research conducted, no other comprehensive framework was found to guide the development of the procedures in a large organizational setting.

The goals of the Chain-Link Fence Model are:

1. to provide a model from which anyone can create procedures that have the best possible chance of
accomplishing the security goals of the organization;

2. to identify how to create procedures that are in harmony with the goals of the organization;

3. to assist in creation of procedures that can be understood by all levels of the organization; and

4. to outline a method for efficiently creating procedures without the need to convene a group of representatives from the organization.

From these points the interdependent components of the Chain-Link Fence Model: Buy-In, Implementation, Ease-of-use, and Effectiveness, were derived (see Figure 1).

Each of these components addresses issues that were highlighted in notes from the task force meetings or found in previous research.
Buy-In is the process of selling the new policy or procedure to all users of the organization. Management needs to buy-in to the procedure so that it will be implemented. Users need to buy-in to the procedure because they will be the people who choose whether or not to follow it on a daily basis. Without this user Buy-In, they will find ways to circumvent the procedure without raising
suspicion. This affects both the Effectiveness and Ease-of-Use domains.

Implementation is the process by which computer managers configure software, use security tools, or teach their users how to follow the new procedure. The success of Implementation is directly related to Ease-of-Use. A procedure that has the support of the management and users will still fail if the proper steps are not taken to implement it.

Ease-of-Use mitigates costs associated with training and lack of compliance with new procedures. It also lessens the need for an in-depth knowledge of security tools. Users who are burdened by the new procedures may rebel against them. If the new procedure is easy to follow, users are more likely to use it. If Ease-of-Use is not included in procedure, both Buy-In and Implementation are ineffective.

Effectiveness is an assessment of how the security procedure reduces the threat it addresses. Effectiveness is the hardest component to predict because it can only be measured after the procedure is implemented. If the procedures do not change the threat impact, then there was no point gained in creating procedures in the first place, thereby wasting time, effort, and resources. These points
are the basis for the Chain-Link Fence Model

The Chain-Link Fence Model

Graphically, each component of the Chain-Link Fence Model links to create a fence of security for the organization. If one of the components is missing, the fence will have a gap through which security threats can enter the organization.

The components of the Chain-Link Fence Model usually operate in sequence: Buy-in must be created to entice stakeholders to invest time, effort, and resources in developing procedures. Next, the procedure is introduced to all the necessary users, thus implementing the procedures. Computer managers generally handle the software configuration and training included in Implementation. After Implementation, Ease-of-Use is a major factor in whether or not the procedure will be followed by the users. Lastly, Effectiveness is measured by an audit system.
RESEARCH METHODS AND PROCEDURES

Timeline of Events in the Research

The task force for creating computer security management at Utah State University was created in August 2009 (see Appendix A). One of the first processes that the task force set out to accomplish was to define the scope for new computer management procedures. It was decided that the scope should be narrow to help focus the task force to complete the procedures without having to become experts in every future technology issue. Because of the narrow scope, the author realized that newer and broader security procedures would need to be created to help manage security threats as technology changed. This realization implied that the entire process would be repeated as security threats changed. By creating a process for creating security procedures, future resources may be saved.

One of the tasks the task force assigned to its members was to find out how peer institutions responded to security threats and if they had any procedures that could be implemented at USU. Most institutions’ security procedures were too narrow to use or were nonexistent. This led to a study of industry standards and academic research
into both procedures as well as the processes for creation of security procedures. This research helped form the components and structure of the Chain-Link Fence Model.

The Chain-Link Fence Model was created as a framework to help standardize the process of creating security procedures. As co-chair of the task force, the author used the Chain-Link Fence Model to create the computer management procedures. The Network Managers Group, a group composed of computer professionals from the colleges, departments, and labs at USU, approved the computer management procedures in February of 2010.

The interviews as outlined in the study design were conducted in two groups. Subjects A, B, and C were interviewed in April 2010 with follow up interviews in February 2011. Data collection from the Nessus results started in September 2009 and continued until the end of May 2010. Subjects D, E, F, and G were asked to use the Chain-Link Fence Model framework to create security policies in July of 2011, and final interviews were in late September and early October 2011.

**Study Design**

The first portion of the research was model
development. The model was developed based upon theory, observation, and expert insight. After the creation of the model, seven subjects were interviewed, and these interviews were divided into two main parts. The primary methodology of the interview portion was the case study model. In Part One, the Validation of the components of the Chain-Link Fence Model, the first case study gathered data through interviews, observation notes, and statistical reports to validate the components of the Chain-Link Fence Model by analyzing the adoption of new security procedures at Utah State University. In Part Two, the Validation of the Chain-Link Fence Model, four computer lab managers tested the Chain-Link Fence Model by using it to create new procedures for their labs. The resulting data was gathered through further interviews. For both main parts, the subjects were given the opportunity to review the transcription of the interview and to clarify any comments. The case study technique provided in-depth study of a single event, in the case of Part One, the adoption of new security procedures at Utah State University. A case study also allowed for the testing of the model proposed as outlined in Part Two with the four additional subjects.
Details of the Study

This paper is divided into two parts. Part One refines and establishes the validity of the Chain-Link Fence Model; Part Two tests its actual implementation.

Part One: the validation process for each component of the Chain-Link Fence Model:

This is an assessment of the Chain-Link Fence Model using interviews with upper IT management personnel regarding the success of the new security procedures at USU. Their responses validated each of the four components of the Chain-Link Fence Model.

Additionally, a statistical analysis of computer security data from before and after the implementation of the new security procedures was conducted. Because the new procedures contained the components of the Chain-Link Fence Model, the statistical data was used to determine correlation between the Chain-Link Fence Model and IT security threats.

Part Two: The study of the model from start to finish:

Four computer lab managers at USU were presented with the Chain-Link Fence Model along with an explanation of its components. They were then asked to use the model to create
security procedures for their labs. After they implemented the procedures, follow-up interviews gauged their perceived results.

**The Process of Interviewing the Subjects**

In order to refine and validate the Chain-Link Fence Model, information technology professionals were interviewed. The interviews were held over the course of two years and were divided into two groups. The first, presented as Part One, consisted of three information technology professionals from the university information technology department. The other four subjects, as presented in Part Two, were lab managers from different colleges or departments from across the university. These seven subjects came from all levels of the organization from the CIO to small lab managers. The subjects had all been in the information technology field for more than seven years, were currently managers of either departments or computer labs, and had been with the organization for more than five years.

**Criteria for Selection of Case Study Subjects**

The primary criteria for selection of subjects was
that they did not participate in the task force. This was necessary to help validate the Buy-In category, as members of the task force would have a bias toward accepting the computer management procedures.

Second, the subjects needed to be managers of departments or computer labs. This insured that they had perspective on the Implementation component. They would need to either teach their subordinates how to implement the new procedures or do it themselves. This consistency of implementation was extremely important in the computer lab environment because each lab would have dozens, potentially hundreds, of users on a given system.

Third, subjects needed to have experience in computer management. This gave them insight into Ease-of-Use. By having years of experience, they knew what users needed and how users interacted with the computer system. They were able to evaluate the difficulties of different procedures, including their own.

Fourth, the subjects needed to be actively involved in computer management. In order to see if a procedure was effective, they needed to have access to log files, audit reports, and Nessus penetration results. They then needed to interpret the reports to see if security procedures were
having any effect on their labs.

All seven subjects were specifically selected for each of the above categories and agreed to participate in the study without any expectation of gain. Each also agreed to participate in multiple interviews over a 2-year span. Each subject was recommended by another member of the university’s Network Managers group for their handling of computer management. Together, the subjects managed or were part of the group that managed over 90% of the computer labs across the campus. Each subject was given a letter designation (A through G) to ensure anonymity.
As co-chair the task force beginning August 2009, the author determined that there must be a framework for achieving the goal of developing IT security procedures on the USU campus. After researching many different institutions for their security procedures and finding that most did not have any formal written procedures available, the research literature guided the development of this model.

The available literature showed no single standard for creating security policy or procedures. There were helpful guidelines provided by the National Institute of Standards and Technology (NIST) that contained references to computer security, the International Information Systems Security Certification Consortium, Inc., (ISC)² maintained a global standard for information technology security professionals, and Microsoft offered a class on how to properly configure Windows in various environments.

These resources, however, did not contain any method of a higher level framework to create security procedures. They had either very specific guidelines for a subset of
requirements (e.g., Microsoft’s configuration for small business and (ISC)² model for penetration testing), or in contrast, they were overly broad (like NIST’s statement of security management and assurance). In part, NIST stated, “Ultimately, responsibility for the success of an organization lies with its senior management. They establish the organization's computer security program and its overall program goals” (NIST, 2012). The author then started searching the academic research topics for guidelines, frameworks, procedures, and other keywords to help develop a framework so that the efforts of the task force could be replicated quicker and easier.

The Creation of the Procedures

The university employed many individuals who had information technology responsibilities. All had varying degrees of knowledge of information technology. The task force realized early on that this potential knowledge base needed to be used to help guide the formation of the computer management procedures. The task force decided to create a survey to help identify and prioritize the procedures.
The task force created a survey in September 2009 to determine how different departments handled computer setup, maintenance, and replacement. It was hosted on surveymonkey.com and given by invitation to all IT professionals at the university. This survey was conducted through November 15, 2009 and had 44 respondents. The survey contained a list of security tasks. Each respondent was required to categorize each task by required, suggested, or optional. The raw data was then coded by a scoring system of five points for required, three points for suggested, and one point for optional. Each task was then averaged for the total mean score of that procedure. Tasks that scored above four points were initially placed in Tier 1 (Required). Tasks that scored between three points and four points were initially placed in Tier 2 (Suggested), and, tasks that scored below three points were initially placed in Tier 3 (Optional) (see Table 1).

These tasks constituted the computer management procedures for Windows, standard security. Results for other systems can be seen in Appendix B.
### Table 1

*Task Force Survey Results*

<table>
<thead>
<tr>
<th>Tier 1 (REQUIRED)</th>
<th>Rating Average</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install/configure anti-virus software</td>
<td>4.95</td>
</tr>
<tr>
<td>Configure automatic Windows updates</td>
<td>4.80</td>
</tr>
<tr>
<td>Register IP address in OpenIPAM</td>
<td>4.55</td>
</tr>
<tr>
<td>Install/configure firewall software</td>
<td>4.37</td>
</tr>
<tr>
<td>Update drivers</td>
<td>4.27</td>
</tr>
<tr>
<td>Disable the local Windows Guest account</td>
<td>4.12</td>
</tr>
<tr>
<td>Disable auto-run</td>
<td>3.39</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Tier 2 (SUGGESTED)</th>
<th>Rating Average</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employ secure user password policies (complexity, length, expiration)</td>
<td>3.94</td>
</tr>
<tr>
<td>Convert file system to NTFS</td>
<td>3.91</td>
</tr>
<tr>
<td>Uninstall “bloatware”</td>
<td>3.79</td>
</tr>
<tr>
<td>Install/configure anti-malware software</td>
<td>3.79</td>
</tr>
<tr>
<td>Install/configure SCCM</td>
<td>3.29</td>
</tr>
<tr>
<td>Reformat hard drive and install Windows from scratch</td>
<td>3.11</td>
</tr>
<tr>
<td>Configure least necessary privileges for the computer owner’s account</td>
<td>3.05</td>
</tr>
<tr>
<td>Configure automatic third-party software updates, when available</td>
<td>3.05</td>
</tr>
<tr>
<td>Disable all unnecessary services (e.g., utilize Windows Baseline Security Analyzer)</td>
<td>2.94</td>
</tr>
<tr>
<td>Rename local Administrator account</td>
<td>2.52</td>
</tr>
<tr>
<td>Disable Administrator account</td>
<td>1.85</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Tier 3 (OPTIONAL)</th>
<th>Rating Average</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employ a backup solution (e.g., shadow copy, store-to-network, portable external drive)</td>
<td>2.94</td>
</tr>
<tr>
<td>Configure services to use non-default ports (e.g., Remote Desktop)</td>
<td>2.88</td>
</tr>
<tr>
<td>Employ security-related group policies via Active Directory (i.e., join Windows domain)</td>
<td>2.82</td>
</tr>
<tr>
<td>Install/disallow certain web browsers</td>
<td>2.82</td>
</tr>
<tr>
<td>Install security protections specific to installed web browser(s) (e.g., FireFox No Script plug-in)</td>
<td>2.69</td>
</tr>
<tr>
<td>Configure power management options</td>
<td>2.68</td>
</tr>
<tr>
<td>Employ security-related local group policies</td>
<td>2.60</td>
</tr>
<tr>
<td>Install/configure third-party software update notifiers (e.g., Secunia Personal Software Inspector)</td>
<td>2.52</td>
</tr>
<tr>
<td>Install Windows from an actively maintained image (e.g., Ghost)</td>
<td>2.50</td>
</tr>
<tr>
<td>Install Windows from scratch with slipstreamed service packs and/or patches</td>
<td>2.41</td>
</tr>
<tr>
<td>Rename the local Windows Guest account</td>
<td>2.41</td>
</tr>
<tr>
<td>Remove local administrator privileges from computer owner’s user account</td>
<td>2.40</td>
</tr>
<tr>
<td>Configure browser to automatically purge browsing history</td>
<td>2.20</td>
</tr>
<tr>
<td>Encrypt the hard drive</td>
<td>1.33</td>
</tr>
</tbody>
</table>
After compiling the results from the survey, the task force used them with subsequent internal discussion to create the finalized version of the computer management procedures. After conducting the survey, the university was given an outside security audit that found some of the procedures should be categorized higher to prevent a greater threat than others. The task force took into account these recommendations and created the final version of the computer management procedures.

The notes from the task force meetings show the following observations:

1. Each person on the task force was more concerned about his own departmental needs than the security needs of the organization as a whole. One member did not want any other members of the university IT community to have any type of access on his system. As a result, the person did not want to join any centralized administrative process, specifically the university’s global Windows domain.

2. The members of the task force did not all have an awareness of, or experience using, the security tools that the organization had at its disposal. One member did not know any of the benefits of
using organizational units (OU) within Windows Group Policy. Once this concept was explained, he realized that he could accomplish more security goals with less effort when he was working as part of the group.

3. Each person in the task force wanted the organization to have a more secure network and was willing to help produce that result. One member postponed his vacation for six months to be able to provide his input.

4. There was a need for the task force to establish the scope of the procedures, specifically what devices and software would be included or excluded.

The procedures that were created only covered Macintosh and Windows-based PCs. While the procedures were a guideline on how students should set up their computers, the procedures fell under the University employee policy, and there was no requirement that students use the procedures.

The Need for a Framework

Information Technology is an ever-evolving field, and the process of creating procedures needed to be repeated
time and time again to address new devices and technologies that arise. As USU grew, the largest growth area in the network was wireless connections. As the internet had increasingly become people’s main source of media, the number of devices that took advantage of this new method of distribution grown. New devices, including the Apple iPad, Motorola Droid, and Google Chromebooks, made it harder to define what an IT device was. Most people would agree that anything computer-related would come under the IT umbrella, like laptops, desktops, networking devices, etc. However, devices like game consoles, blue-ray players, and televisions had wireless internet connectivity built-in.

As more of these devices joined the network, new procedures were needed to define secure methods of using these devices. It took eight people six months of weekly meetings to create the current procedures in this study. Institutions cannot afford to dedicate numerous resources every time they need a new security procedure. If there was a model to follow for creating security procedures, then anyone who saw a security need could use it and quickly get procedures implemented. Using this experience on the task force as a guide, the author developed the Chain-Link Fence Model for the creation of security procedures.
Formulation of the Components

A major paper influencing the author’s development of the Chain-Link Fence Model was by Da Veiga and Eloff (2007). Their paper had a framework for IS governance, rather than security directly. Their framework suggested changes to the organization’s security culture. It discussed the need for management buy-in to change the culture.

Buy-in

Backhouse et al. (2006) addressed power. Without full buy-in from those in power, the process could not be completed. This and the Da Veiga and Eloff (2007) article showed how the process starts with buy-in. In their study of spyware Warkentin, Xin, and Templeton (2005) found that understanding the problem, or buy-in, would help in the use of anti-spyware software. Gillespie (2009) stated that buy-in was necessary for enhanced security.

Ease-of-Use

An influence of the Ease-of-Use component is a standard of IS research in the Technology Acceptance Model (TAM) by Davis (1989). His research into TAM suggested that ease-of-use helped users develop the necessary skills to
adopt new technology. In the current study, the author predicted that with new security procedures, there would be new-to-users technology that they would need to accept. Mustonen-Ollila and Lyytien’s study of IS history (2003) also showed that one of the most influential factors in progressing IS process was ease-of-use. In 2009, Scholz discussed basic mistakes that were caused by overly confusing the security process. This confusion suggested that ease-of-use must be part of the process in order to prevent human error.

**Implementation**

At this point, the model’s framework showed a logic gap. To go from organizational buy-in to ease-of-use, users needed the actual procedures to be written with full documentation. Bresz (2004) researched how hospital information technology dealt with Health Insurance Portability and Accountability Act (HIPAA). One of the key parts of HIPAA was full documentation before changes could be made to a system (i.e., a procedure for implementation).

Von Solms and von Solms’s (2004) article of the 10 sins of IS security suggested that training both the culture and users were very important to maintaining proper
security. Vroom and von Solms (2004) stated that up to 48 percent of breaches were accidental in nature. This showed that proper implementation of procedures could greatly reduce security issues. This led to the inclusion of implementation as a component of the Chain-Link Fence Model. Sasse et al. (2001) showed that users needed training to avoid being the weakest link in the security process.

**Effectiveness**

The buy-in component was necessary for development, and the ease-of-use component was necessary for users to change the overall culture of security. Rees et al. (2003) created short-term security policies. The usefulness of these policies was determined by feedback from stakeholders. This led to the inclusion of evaluation as part of the Chain-Link Fence Model framework. Vroom and von Solms (2004) showed how auditing was an effective tool for gauging how an organization complied with their security policies. Furnell et al. (2000) specifically discussed how effectiveness could also lead to adoption of security measures, showing how the starting point of a future model could be at the end of a process.

As the components were identified, the model of the
framework needed to be expounded upon. The first diagram for the model of the framework was a straight line (see Figure 2).

The straight line, however, implied that once the process was complete, the goal was achieved. As the Rees et al. (2003) article stated, there needed to be a constant feedback part to the model, in essence closing the loop.

![Figure 2. Developmental Step 1 of Chain-Link Fence Model.](image)

This led to a different model demonstrating an ever-completing cycle required by constant feedback (see Figure 3).
Further thought led to the realization that each component was not a stand-alone component. They needed interaction to build upon each other. Also, while the cycle did start with Buy-in, the linear model could only run forward in sequence.

This led to back the final completed framework and the name for the Chain-Link Fence Model.
VALIDATION OF THE COMPONENTS OF THE CHAIN–LINK FENCE MODEL

PART 1: DEEP INTERVIEW AND EFFECTIVENESS MEASURE

Introduction

The need to replicate the process of creating security procedures drove the need to create a repeatable model. In order to ascertain whether or not the proposed model worked, experts needed to validate the proposed model. This created a need to interview experts in information technology security.

The Interview Process

The questions for the interviews were composed based upon a review of the literature in the field. The questions were also written specifically to avoid using the names of the components of the Chain-Link Fence Model in order to draw out responses that would not have bias toward expounding the model. Finally, while the same questions were asked of all subjects, the questions were open-ended, and each subject was free to elaborate on topics important to him regarding computer security. These digressions also helped provide data that reflected on the overall model.

Each interview was scheduled before a significant
break, either lunch, mid-day, afternoon, or before end-of-business to allow for as limitless a time period as possible. Each interview was held at the subject’s primary work environment. In addition to placing the subjects in an area with which they were familiar and in which they were accustomed to thinking about security matters, this had the added benefit of placing them near their work resources so that they were able to answer questions on the spot, without having to research the question and report back later.

Each interview was recorded on analog tape, forcing a human interpretation of the transcriptions. After transcripts of the interviews were made, each subject was allowed to look at the transcript of his interview to judge whether the transcript was accurate. Because there were no digital copies of the recordings, it was much easier to prevent duplication and to help keep the interview subject anonymous.

Questions asked of the first subjects interviewed were asked of subsequent subjects as deemed relevant. Questions which were confusing in early interviews were clarified for later subjects. The full list of interview questions can be found in Appendix C.
Reception of the Security Procedures

Everyone at the organization knew that the status quo was not a good security plan. At the January 2010 meeting outlining the new procedures, the Network Managers Group discussed the ramifications of establishing organizational procedures. Notes from the meeting included the following exchange:

Attendee 1: Does this apply to everybody?

Bob: Everybody connected to the network.

Attendee 2: What happens if we don't follow [the procedures]?

Bob: You risk having your computer compromised by a hacker, and if you develop a problem, you could find yourself on the disabled list.

At the meeting there were a few who felt that the procedures were draconian, but after the group went over the specifics of the procedures, it was established that the procedures consisted of activities that most were already doing.

The procedures were adopted at the following meeting February 9, 2010. They were ratified by the entire Network Managers Group at the monthly meeting. After allowances for
questions and an in-depth discussion of the procedures, the vote to establish them was unanimous.

**Buy-in**

Interview subjects were asked about their thoughts on the procedures to establish the presence of Buy-In. All subjects thought highly of the newly-adopted computer management procedures.

Subject A, the CIO, had long wanted to build a procedure that could be used to get everybody “on the same page.” He recognized that consensus, or Buy-In, was key to an effective security procedure. He stated, “The first strength is [that] it’s ... documented and it’s achieving consensus.” When discussing the security implications, he said, “In regards to security, it’s certainly better than anything we had. One of the goals of this above beyond anything was to get ... some consensus.” He continued, “The ability to come to consensus [and have the] Network Managers group say that this [is a] thing we should be doing [is key]. The compliance of the individual items [exceeded] my expectations. I wasn’t entirely sure if we could come to any consensus on this, but that happened. And that, for me, overshadows any weaknesses.”
Subject B also seemed to have a strong opinion of the importance of Buy-In. He said, “I think it was a big task ... to bring consensus from a large group of people across campus, and so I think it was [a] great effort.” When asked what he thought was one of the most important points of the recommendation, he immediately responded, “Buy-In from the community, because I felt that that was the only way to do it.”

Subject B: Central IT couldn’t come up with those ... we aren’t our service desk guys working with desktops on a day-to-day basis ... The only way we could get what’s going on out there was to get people who were doing this on a day-to-day basis. And that had to go way beyond IT. So Buy-In was part of it, and the other part was to get a broad picture of input.

Subject B provided important insight, as he was involved in approving the procedures.

Subject B: We have some folks, who can sometimes be critical ... They always wanted to challenge something, and I hoped they would take the opportunity to get aboard.

In regard to the process, Subject B thought that using the task force to create the procedures was one of the
contributing factors to Buy-In. He stated, “The committee that made it happen, just made it happen, and there we got an excellent product, excellent product ... I couldn’t [have] been happier.” When asked what specifically made the committee work so well, he said, “what was cool [was that] we had folks representing several of our largest colleges: [the] College of Business, [the] College of HASS, which is our largest college on campus, [the] College of Agriculture which is big, [and] Person X [with the] College of Education. So we had four of the [eight] major colleges represented.”

At the conclusion of the interview, Subject B commented:
“I watched you present this last time, [and] you got Buy-In from the larger group, saying, ‘here are some core areas of must-haves and here is some recommended practices ... and here are some things to think about.’ I was hoping only for the PC stuff. I figured if we [got] to the PC, [then] we [could] put another group together that would take that PC stuff and then interpret it for the Mac. The fact that you came out with Mac’s stuff was just a bonus. The fact that you came up with the idea of ‘Well, we’ve also got to address this for computers who are dealing with sensitive
information ...’ you know, to come up with that was just another bonus. Originally, I was just hoping for that first list.”

Subject C felt that the research done in support of the procedures led to his total approval of the product.

Bob: So, based upon what you read on the final report, how well do you think that the task force evaluated the validity of all the opinions presented to them?

Subject C: Well, I thought that part was actually excellent. You guys brought a strong statistical sense of propriety to the project. I think you did an excellent job of sampling and representing how deep you felt about it.

His next response underscores how difficult it usually was to obtain Buy-In across different branches of a large organization.

Bob: Did the final conclusions match your expectations?

Subject C: I thought they were better than I expected ... I expected you guys to come out of there with broken arms, broken legs ... and one or two of you with a slit throat and some fairly non-specific recommendations. We were very pleased with the result.”
The process of achieving Buy-In can be summed up by Subject A, "You have to be collaborative, you have to be understanding, and you have to work together. You do not have the type of authoritarian dictatorliness (there's a title) that you get in business."

**Implementation**

The approval of the procedures and their acceptance by management was only the first step in the implementation process. If procedures are not implemented, then their existence is of little use. Each part of the implementation process required coordination. Management subjects were asked what they thought about the process of implementation.

Bob: So how do you think that the university will implement the recommendations of the task force?

Subject C: (jokingly) I think we'll all try to ignore that it exists ... That's probably my job. I need to do some kind of major thing: make it part of our weekly scans or look for specific recommendations in there and see if they are getting done.

Subject A thought that the implementation should start with the centralized portion of IT. "[The] service desk ought to be taught how to manage [computers] for the
departments. The service desk [sets] the example at Utah State University."

Subject C also stated that new employees to the organization should be given the new procedures as part of their hire. "We need to keep [the procedures] up in front of [the new hires]. What we need is something that that stands for and represents the Network Managers. [When] new people coming to the Network Managers, [we can say], 'Welcome to [the] Network Managers. Here's everything you need to know right here.' We [didn’t] have that kind of thing, [but now we do]."

One way to implement procedures was to make them a part of a person’s daily routine. Subject A stated, "It becomes something we use and live by, and I think the more we mention it in Network Managers [meeting] and have updates once a quarter and keep this a living document, [the more] it will have a positive impact. We’ve all said a lot of [the] network managers are doing a lot of these things already."

To make the procedures a "living document," they must be kept up to date. As technology changes, some of the procedures may become redundant, not applicable, or simply forgotten. Subject C also thought that part of
implementation included continually revising the documents.

Subject C: So how long do you coast before you look at it and say, ‘Does anything need to be amended, updated, changed, or altered?’

Bob: That’s a good question and I think that’s one of the things I am trying to find out. I think in the conclusion section of the report, it stated that it needs to be periodically updated and reviewed.

Subject C: Yeah, obviously—otherwise, it would just become a misleading document, and then eventually a harmful one. But [it would become] harmful probably three or four or five years down the road.

Subject A wondered about the university as a whole. He stated, “[there are] two directions anything like this can go. [If it gets] filed [away] and nobody looks at it again, bad idea.”

**Ease-Of-Use**

Procedures must be easy for all users to follow, whether the user is responsible for an entire computer lab or just one computer. If the procedures are not easy for everyone to follow, then users will find a way around them,
leading to a breakdown in security. The procedures were published as a checklist on the USU website retrieved January 31, 2013, from http://it.usu.edu/policies/htm/computer-management-policy/computer-management-procedures. Included next to each element is the network managers survey score. The website checklist is located in Appendix B.

Subject B thought that one of the computer management procedures’ strengths was that they were organized as a checklist. “I can easily say, ‘Okay, here’s what I need to do, here’s some I got to have in consideration, and here are some other suggested things.’ I think it’s very simple and in that form the strength is that it’s got a little checklist.”

Subject C also thought that the checklist was helpful. “[If you] got a handout that is available at the service desk [and you made it] part of the Welcome to USU package ... I think it would just become part of the university consciousness. I think that would probably do it. Something to [give to] new students and something to [hand out] at the service desk.”

Subject A also saw the procedures as a checklist. For example, when a non-technical user follows the checklist to
set up a new computer, “it helps human error not be a big part of the equation.”

As Subject A was using the checklist component, he commented:

I actually went through and looked at my own desktop computer here. I was looking through this morning, and I said, “Okay, now what have I done, and what have I not done?” There were some things I hadn’t done. I had not disabled autorun on my computer. I’m like, “Mmm, I better do that.” I have not renamed my local windows [administrator account]. Some of these I either marked to do. Some ... I might not have needed. I just haven’t done some of them. I’m like, “Oh my gosh, I better figure out how to do that one.” So I think to the extent that people will use this as a help for themselves to not forget something, I think it’s going to be fabulous.

Because the procedures were organized like a checklist, they were inherently easy to use. All of the subjects mentioned that the procedures in this form would be easy for students and others with minimal technical knowledge to implement. In a university setting, security procedures needed to be implemented not only by management, but also
by the students who, with their personal computers, compose the bulk of users on the campus network. When a large number of users had implemented the procedures, then security audits would show whether or not the procedures were effective.

**Effectiveness**

Effectiveness of new procedures could only be measured after the procedures had been fully implemented. After the procedures were approved, subjects were asked about how effective they thought the procedures might be.

Subject B thought that for computers that are managed, the procedures would be a labor-saving solution. “This is going to be the difference between staying all night and going home. So people [will want to] put the upfront time into setting that up on those machines.” However, he admitted that it would not be the end of all security problems at USU. “We see computers all the time that are behind in their updates, but 90 percent of them are not from computers that are managed.”

Subject A had a pessimistic view of the probable effectiveness of the procedures due to the biases of the task force that created them. “I think the decisions in the
end were more based on feelings of control and convenience rather than security, as evidenced by the difference in Windows and Mac [procedures]. I think ... their own personal feelings got a little more weight than some of the objectives of good computer management.”

Subject C speculated, “If [the procedures] are followed and we are lucky, I think we will keep ... the amount of compromise [at the same level] as what we have got now.”

**Summary of Qualitative Validation**

The Chain-Link Fence Model was extrapolated from observations of the process of creating the computer management procedures. The subjects interviewed were hired to be the computer managers of the university; they were the experts in their field. The three subjects in this section had no previous knowledge of the Chain-Link Fence Model. In the interviews, the subjects also independently validated and confirmed each component of the Chain-Link Fence Model.

Each of the interviewed subjects stated that they believed the procedures produced a good result to reduce the security threat to the university. They stated that the
procedures followed the components established by the Chain-Link Fence Model and that those components were what helped make the security procedures a successful university process.

**Numerical Support for Effectiveness**

The reason for creating security procedures was to reduce the threat to the organization. Many organizations were required by external policies to conduct security threat analyses. For example, as part of the Payment Card Industry (PCI) standards version 2.0, outside security teams would audit an organization and pretend to present a security threat. They would conduct penetration tests upon the networks of their clients to probe for weaknesses. Such tests are a good measure to evaluate if security procedures are adequate and if they are being followed. Therefore to test the security of the institution, this research used a standard penetration test following the guidelines of PCI 2.0.

USU policy #551 states that all computers connected to the network must be managed. USU’s policy #555 authorizes the USU Security Team to conduct weekly penetration tests. These penetration tests show how well USU will stand up to
an external hacker's attempt to gain access through the public internet.

**Data, Nessus Report**

The product used by USU to facilitate the network tests was Nessus. Nessus is a server-side product that is configured to probe every port and service on every IP address in a network. It discovers potential vulnerabilities by using a steady stream of plug-ins that enable the server to access potential security threats in computer systems. The bulk of these threats are:

- Computers that are hard-coding an IP address that does not belong to the computer.
- Devices that disrupt network operations.
- Computers that are missing critical system patches.
- Accessible “Administrator” or “root” usernames with no password.
- Embedded appliances with critical, unpatched vulnerabilities.
- Printers that are on public (129.123.0.0/16) IP addresses and are not supposed to offer printing services to the internet.
• Computers that expose or compromise USU credentials. This includes:
  o Failing to protect passwords.
  o Failing to protect stored password hashes
  o Computers that take no action in the presence of excessive password guessing

• Other equipment that exposes USU credentials. This includes:
  o Equipment that replicates and transmits USU credential in cleartext.
  o Old vulnerable backup devices.
  o Critical vulnerabilities in older versions of McAfee, Apache web server, SSH, and PHP webservice.
  o Other software with critical vulnerabilities.
  o Unsupported OS. (Retrieved January 31, 2013 from https://it.wiki.usu.edu/20100513_Nessus_Test)

Analysis of the Data

Permission was granted to use the old data from the academic school year 2009-2010. On January 20, 2012, the archives of the Network Managers list was analyzed by pulling out each week’s vulnerability list for the date
ranges of this study. Permission was granted from the USU IT Security Team to use this data, as they deemed it too old to be of any further threat to the organization.

The following are the results of the Nessus penetration test. The USU IT Security Team took the computers that Nessus identified as vulnerable and then purged any false positives from these results.

Upon compilation of the data, there were multiple gaps in the results. There should have been either four or five scans during any one month period. As seen in Figure 4, most months only have two entries per month.

Figure 4. Vulnerable computers on the Nessus report.
On February 11, 2010 the USU Network Managers group approved the computer management procedures. The data prior to February was too incomplete to perform a valid test. As shown in Figure 4, there was a substantial reduction between Late August and Early September 2009 compared to March and April 2010, but too many points of data were lost to make any statistical conclusions.

**Measuring Conclusion**

While there is not sufficient statistical support for any test, there is anecdotal evidence that the implementation of the security procedures did reduce the security threat at USU. Computer managers confirmed through interviews that they believed the procedures were effective and labor-saving. Subject C stated that, “I believe that we are doing a better job [reducing compromise] than we ever have before.” Subject B talked about the labor-savings, “I see people who have got a lot of machines to run, 200 or more, that this [the computer management procedures] is just going to save their bacon.” This helps demonstrate that the Effectiveness component of the Chain-Link Fence Model was necessary to reducing the overall security threat footprint of the organization.
VALIDATION OF THE CHAIN-LINK FENCE MODEL PART 2: USING THE CHAIN-LINK FENCE MODEL TO CREATE SECURITY PROCEDURES AT UTAH STATE UNIVERSITY

Procedure Development Using the Chain-Link Fence Model

Utah State University is unique, given the distributed nature of information technology. While USU has centralized servers, services, and top-to-bottom management, it also has several departments and colleges that maintain their own IT teams. While there are drawbacks to this system, they are overshadowed by the benefits. Subject A stated it best:

"Utah State University will never, if I have anything to say about it, be absolutely fully centralized with IT with absolutely everything and anything that has to do with information technology because it doesn’t make sense. The things that make sense for centralization are those things which are used commonly, relatively equally across, say, 80 to 90 percent of the institution. Those [are the] things that make sense to centralize and pass on [as a] common service. There are a million things at this university and millions and millions of dollars worth of things at this University that are very specific to certain disciplines
and certain processes [that] the rest of the university [couldn’t] care less about. Those situations should not be restricted at all by any form of centralization at Utah State University. Centralization should assist them so they don’t have to focus on some commoditized things, but that’s as far as it should go. Ownership, the funding, the systems, the processes that are specific and not generalizable at the University, I believe should always be at the edge. Otherwise needs won’t be met.”

In order for each department to “be at the edge,” their IT professionals needed to have the freedom to create internal IT security policies and procedures.

The Interview Process

Throughout January of 2011, the Chain-Link Fence Model was taught to four additional subjects, subjects D through G (see Appendix D). They were then asked to use the model to create security procedures for their respective labs. They responded by using the model to create procedures as well as performing other duties related to their jobs. During 2011, Subjects D through G were interviewed about their experiences using the Chain-Link Fence Model.

Subjects were asked about how they used parts of the
Chain-Link Fence Model for their computer labs. Buy-In for a computer lab was more complex than that of an organization. There were two different groups that needed to cooperate with the departmental procedures: Buy-In for the managers was easy because they wrote the procedures and Buy-In for lab consultants was slightly harder because they needed to be taught the hows and whys of the procedures. In the case of a computer lab, the users fit the traditional customer role of a business rather than the service role. This made them more adversarial to the Buy-In process.

In relation to Implementation, questions were asked about training procedures for the labs. For Ease-of-use, subjects were asked how their labs related to a users’ home experience and how they thought their labs were similar or different. Effectiveness for each case is discussed as a whole at the end of the cases.

Case Study 1, Security Incident Response and Time Limit Procedures

Subject D managed all the computers in the computer science department. His computer lab, an open-access lab, consisted of 150 computers. He had a unique challenge among campus lab managers in that his computers needed to be as
open as possible so that students could explore all facets of the computing environment. This created some issues, especially with computer security.

The students in Subject D’s lab often behaved like typical hackers. They tried to learn what was going on in the computer environment. This included attempting to spoof IP addresses, changing root level file structures, and in some cases, attempting to present themselves as a different user.

One of the main differences between his lab environment and all the others was the fact that it was an anonymous lab. There was not a centralized authentication system requirement for entry; most of the computers had root or administrator access set as the default user credentials. Finally, they did not have the usual firewalled and sectioned-off subnets found in other open-access labs on campus. As Subject D stated, “The systems are somewhat open because in computer science, we’ve got students that have to develop a lot of programs where they need a fair amount of resources off the Internet. They need to be able to come back after they’ve worked on it and keep working on a project.”

When a breach in security was detected, Subject D
created (using the Chain-Link Fence Model) a standard procedure for processing the problem computer. He summarized this procedure: “We do let USU computer security indicate if somebody is doing something out of the ordinary, and then we reimage the computers. If we catch anyone doing something that is a security breach we just reimage the computers [and] bring it back to a known operative state. The students are warned before they go in that they do have open computers because of their development platforms, and they have to police themselves.”

While this environment seems like the Wild Wild West of computer environments to most computer security professionals, designed procedures helped keep the chaos to a minimum. “We do have firewalls on each of the systems which we use: standard Windows 7 and Macintosh and Linux firewalls. We allow basically any [outgoing traffic]. [We] usually limit incoming [traffic] so students can’t run their own applications unless we poke a hole in the firewalls. That’s about all we do, because again, they still need to access resources off campus as they’re developing some of their distribution software.”

Subject D used the Chain-Link Fence Model for the creation of a time-limit procedure.
Subject D: If we’ve got someone who is in [the lab] for an extended period of time, the lab managers ... or the consultants ask them what they are doing ... We give them about three hours, mainly because the games players come in, play for like six [hours]. So after about three hours we ask them what they’re doing. Normally, they feel intimidated and get up and leave, but the games players are the worst case. Most of the rest of the students are in and out of the lab in about an hour to two.

**Buy-in.** In his lab, Subject D needed his lab managers to assist him in enforcing these new procedures. “We discuss those at the first of the school year like we did at the end of August. [We review] what’s [been] implemented [and] anything that’s changed in the campus infrastructure during the summer, and they’re basically the policeman of the of the lab operations.”

**Implementation.** One of the primary concerns for Subject D was the students. He wanted to make sure that the students knew what the procedures of the lab included. To that end he has training sessions with the students. “I think we have enough ... training for the incoming students to warn them enough if they ... start doing anything
malicious that they will be out of the program, and they usually watch fairly closely. So ... we’ve had them in the past, but in the last eight years up here we’ve ... not had a documented case of malice.”

When discussing implementation Subject D also stated that he was also implementing the Utah State University security procedures.

“[I implement the procedures outlined by USU] as close as possible, other than possibly the Deep Freeze issue.” Deep Freeze is a program used to prevent anybody from altering any part of a computer system. It is a third-party application that forces the computers to return to a predefined and static state upon reboot. He continued, “Some lab managers use it; Engineering has [used it] a little bit, but they have found the same thing that I have—that the students get limited ... to what they can do in some of their development. And so I’ve opted to move away from it just because we have enough changes during the semester [that] make it just hard for them to manage. But typically, as far as security monitoring, I follow the guidelines that we’ve created on the Managers list... The Deep Freeze is probably the trickiest just because it [doesn’t seem] complicated, but it requires a complete
reimage of the lab. If we need to make any changes or if the students need particular updates and so on so forth, [the lab would have to create a specialized procedure to handle the request under a Deep Freeze environment].

**Ease-of-use.** In Subject D's lab, the systems were as wide open as possible. This gave the student users a chance to explore their systems to further their education. This helped them feel knowledgeable with their use of the systems. Subject D wanted his lab to be run with focus on ease-of-use for his students.

Bob: If you were to compare your lab computers to a user’s home computer, how are they similar? And how are they different? Let’s start with similar.

Subject D: Similar in the fact that they are fairly open. A user’s home computer ... is fairly open. [We have] an unlimited firewall as far as outgoing, so they can go anywhere they want. [There are] some limitations on the incoming [firewall and] on ... the university’s border firewall. Where they [the lab computers] would be different is [that] a home user’s computer probably isn’t monitored for patch updates. People don’t necessarily look down at the [system tray] to see if it’s up to date. With lab computers, the
consultants go around and make sure that the scans are all happening either automatically or [forced]. A home computer user is not necessarily going to look for security updates or virus scanning spyware updates and probably also isn’t necessarily going to look for required updates to the computer that don’t happen automatically. [Also,] some of the optional updates that still could be security related ... may not be updated on a home computer.

Case Study 2, Joining a Central Domain

Subject E managed the computers in the College of Humanities and Social Sciences. His users mostly used the computers for composing papers, creating news stories, or blogging. In contrast to the computer science department, Subject E’s users were complete novices in computer security.

Bob: How would you rate your users’ knowledge of information security?

Subject E: I would probably say close to zero. As new freshman are coming in, I’m not sure that they have much knowledge of security and policies regarding that [security].
Consequently, he felt that it was his duty to keep his systems secure for the users, which resulted in his computers being some of the most locked down systems on campus. He achieved this by following these procedures created using the Chain-Link Fence Model:

1. All computers were connected to the college domain.
   This ensured that accounts and print counts could be managed centrally.

2. All computers were required to have Deep Freeze installed on them.

3. All computers were connected to the System Center Configuration Manager (SCCM) server. This ensured that most of the university computer management procedures were being met.

4. All computers were reimaged at the beginning of each academic school year.

All of these steps ensured that none of the systems had any trace of customization by the users of the systems. This had the added benefit of forcing most of the configuration work upfront. This type of lab management comes from a belief that the greatest security threat is from within.

Bob: What would you say is the greatest security threat
to your lab?

Subject E: The greatest security threat to our lab is a knowledgeable student that might know how to disable Deep Freeze and install things.

Bob: You’re saying an internal hacker?

Subject E: Yeah. I don’t foresee an external hacker getting in too easily and permanently making any changes.

**Buy-in.** The use of the utility Deep Freeze forces the computers to not have the ability to save any data to the hard drive. This caused Subject E the most difficulty in terms of buy-in from the users. He stated that the extreme security measures that they take cause some complaints. “Once in a while we get a complaint that ... they [the users] can’t save anything to the computers.”

**Ease-of-use.** Subject E's labs were closed tight, only allowing very limited use of the computer environment. This could have an effect on the abilities of the users to operate the computer.

Bob: If you were to compare your lab to a user’s home computer how, is the experience similar, and how is the experience different?

Subject E: Let’s start with how it’s different. Most
home computers don’t need to log in; that’s just how it is. There is generally no password on a home computer, and here you have to have a login to get into it. Also on our lab computers, [users] can’t save anything at all. On a home computer, you can save whatever you want, including viruses and malware and everything. Those are the main differences. How it’s similar is [that] they can browse the web [and] they can print just like they would be able to at home. So that pretty much covers it.

**Implementation.** When a computer was joined to the university domain, the user account lost the ability to have administrative privileges. This caused the user to not be able to install software, printers, and other advanced computers settings. Subject E was asked him how this affected the implementation of his procedures:

Bob: Do you follow all of the [procedures] as created?

Subject E: I would say 90 percent of them.

Bob: Okay, which procedures are the most difficult for you to maintain or follow?

Subject E: I would say the one we’re having the most difficulty with is having users not have administrator privileges. We’re doing okay on Windows machines, but
on Mac, people tend to have a mentality that they should have complete control over their Macintosh system. So I would say that is the top of the list of [procedures] that are difficult to follow.

**Case Study 3, Standard Security Response Procedures**

Subject F's situation was unique given that he was the sole manager at the departmental level. While the other subjects had lab consultants, Subject F was the sole administrator for his lab. His lab consisted of 30 Macintosh computers. The users of his lab had a unique log-on that was enforced by an Open-Directory Domain. The computers were unique due to the fact that he had them set in dual boot configurations with Microsoft Windows. Each of his Windows installations was a stand-alone workstation without access to a central server.

Subject F kept the default guest account on his computers to help facilitate sharing of information between registered and non-registered users of his lab. The guest account could not save to either the server or locally to the computer itself. The use of the guest account was for log-on purposes only.

The majority of his users were students that
specialize in using technology in the education field. He had about 150 people use his lab in a given week. In addition, many classes were held in the lab.

His approach to security was as follows: “I kind of look at security as [encompassing] both information [security] and physical [security]. So [on] the physical security side, there [are] locks on both doors, and the only people who are allowed in there are those who have access codes, which they are given the first day of school. I don’t hand out the codes. The codes are handed out by either by the instructor or the office staff so they can verify that they are a student, because I don’t have access to that information.”

“Information security--I guess I don’t really worry too much about it just because of the way I’ve got these accounts set up so that they can’t do anything. But if they do, then I usually catch it ... I can know who is logged in when they are logged in. If anything goes wrong with [the computers], it’s just a reboot that refreshes it. So there’s not a whole lot there that I worry about, mostly ‘cause they are using [the] Mac side.” When questioned why he did not worry about information security, he responded, “I just let the university handle most of that because I am
not really equipped to do it.”

In his office, Subject F set up a computer workstation with multiple displays. On each display were 30 open windows. Each window corresponded to one of the computers in the lab. He was able to see at a glance what is being displayed on each computer.

His specialized setup was created in response to the lab’s greatest threat, Bit Torrent. Bit Torrent is a peer-to-peer file sharing protocol that can be used to quickly distribute copyrighted material.

Subject F: Bit Torrent was the issue we had last year [when] one of our instructors was teaching and using Windows. [A student] discovered that [the lab] has a really fast internet connection in there. What they did is they’d log in as just as a standard user. They logged in as a student and they used about twelve machines and started downloading all kinds of crap. I got the message from [the copyright compliance security team member] and he said ‘[we got a DMCA violation],’ and I said, ‘It’s a lab. I’ve no idea who’s logged in there, and all I can do is just clean them up.’ And he says ‘Okay.’ But what created the problem [was Windows being able] to log into the
servers. [I need to] have them connected to a domain so that I can restrict those users as I do the Mac users. [I have the computer set up to] log in and they’re standard users now, [but] sometimes the student needs the ability to do some installations. I have to allow that on a case-by case-basis. [With] Windows, most things you install you have to restart. Bob: So can you just run Deep Freeze? Subject F: If you’ve got Deep Freeze installed it just wipes out everything they have, so it’s a different animal. But ... I need to know who’s logged in and when, so that’s what I’ve been trying to solve. Subject F created the following procedure to help manage his lab:

1. create Location Based Names,
2. create DNS entries on Aggies domain,
3. create deployment image,
4. re-image the computers,
5. verify with [RADIUS server administrator] that authentication works, and
6. verify that Aggies Domain services are correct.

**Buy-in.** As with Subject E, Subject F joined the Windows installations to the university domain, once again
removing administrative privileges from the computers.

Subject F recalled a problem with Buy-In.

Subject F: I would say those who want to use Windows don’t like the fact that they can’t do installations or make some changes to tweak stuff. We have [suggestion cards] from the students [saying] they like to do things that are more advanced that they can’t do in a regular lab. So my lab gets used as a guinea pig quite a bit. They [may not] like the fact that they have to come ask me to install something ... but they get it over it ... they kind of understand.

Bob: How many complaints do you get in any given week?

Subject F: I’d say maybe one or two per semester.

Bob: Ok, so one or two per semester.

Subject F: It’s really low--I think ... with the advanced understanding of the students and faculty, they understand what the issues are [and] why it needs to be that way.

**Ease-of-use.** The computer lab that Subject F managed catered to two different groups of users. The first was the traditional student users (i.e., students who used the lab to work on their projects, papers, and other school work). The second user group was the instructors. They used the
lab to teach students and, as a result, had a different standard for ease-of-use. Subject F's computer lab was Macintosh based.

Bob: If you were to compare your lab to one of your users' home computers, what would you say are their similarities and their differences?

Subject F: Biggest difference is my machines are clean--very clean. There's no extraneous software, there's no orphans there's no stuff left behind. The similarities: I try to create an environment that looks and acts as much like a home computer as possible. So the only difference is when they're logged in, they're working off a server. But it doesn't look that way, so that's the thing ... you'd call it a similarity, but yet it's a difference at the same time. But as far these machines compared to their home machines? These ones run a lot better.

**Implementation.** Due to the fact that Subject F ran the lab alone, the implementation of policy was very straightforward. However, teaching his users how this policy would affect them was a little more difficult.

Bob: How much training do you provide your users?

Subject F: I’ll meet with [the instructors] before the
semester starts and let them know what’s happening, and then I’ll expect them to [see] if it affects the students. [I] let them explain it to [the students] and let them do it. [As a result], the normal users hardly at all ... knock on my door and ask for some help.

Bob: So you train the faculty in any new things, changes, or anything [else] to the lab, and you expect the faculty then teach their students who are using the lab those changes?

Subject F: Because it seems like the information gets to the students a lot better that way.

Subject F stated that the total amount of time to train the faculty was around an hour, while the first day of classes was spent training the students.

**Case Study 4, Computer Refresh Policy**

Subject G had the largest number of computer labs and the largest number of computers. His labs accounted for 80 percent of all the open access labs across the campus. He created policies to deal with the sheer volume of students that used his lab computers. Over 3500 students used his system every day. With that many users, he needed
procedures that ensured that students could always have access to a computer to complete their work.

Bob: So how many people help you manage all of your labs?

Subject G: There are 82 of them.

Bob: Are there assistant lab managers? What are their job titles and responsibilities?

Subject G: There are 82 consultants that man the facilities throughout the area. Then I have six peer managers. And these peer managers help me out with the PC, the Mac, HR, supplies, training, [and] public relations.

Subject G articulated the greatest security threat to his lab: “From my point of view, it’s the physical security, but from the student’s point of view, it’s being compromised.”

After reading the university’s computer management policy, Subject G realized that he needed to create specific procedures. He was asked to use the Chain-Link Fence Model to guide their creation. He agreed and came up with the following procedures:

**Computer cycle between users policy.** It became the policy of this lab that computers not in use for more than
15 minutes would be recycled to a refreshed state.

This policy was supported by the following procedures:

1. the computers will have a self-timer installed so they reboot automatically after 15 minutes of idle,
2. the computer will use Deep Freeze to ensure that the state of the computer is free from any user’s customization, and
3. lab consultants will make sure that any computer not in use will be at the log-on screen.

Subject G reported that these new procedures accomplished his goal of making more computers available to users.

**Buy-In.** Subject G had multiple lab consultants, and he indicated no problems with their Buy-In to the program. He also stated that most of the issue with lab consultant Buy-In was handled in the multiple training sessions that they conducted.

Bob: Do your lab managers support your lab policies?
Subject G: Yes.

Bob: I mean, and I’m not talking about forcible [acceptance]. Overall, do they understand why you’re doing what you are doing?

Subject G: Yes, they are trained. We do training quite heavily at the first of the year.
Ease-of-use. Each student who used an on-campus computer lab had a different computing experience, depending on which departmental lab they chose to use. Because all of the lab managers had some students using their computers, they were then questioned about the students’ experiences.

Lab managers made their computers easy for students to use by making them look and feel as much as possible like a home computer. To make a lab easy to use and manage for consultants, lab managers needed to provide proper training.

Subject G had the most lab consultants. We discussed how he trained his consultants in order to make the labs easy for them to use and manage.

Bob: You mentioned previously that [for lab manager training] you’ve got the four hours once a month and on Saturdays, and you’ve got the eight hours at the beginning of the semester.

Subject G: Correct

Bob: how much of that training time is dedicated to security? And so, what I’m asking is how long does it take to train your managers, your lab managers, in regards to security-related issues?

Subject G: I would say out of those first two
meetings ... about an hour in the first meeting in September, and another hour in the second meeting in September for everyone. So the first one is for new consultants only, they get about an hour, I’d say maybe an hour and a half training on security. Then the next week with all the staff, you get about an hour of security training. Then every month there is probably ... ten to fifteen minutes of discussion about security.

**Implementation.** The labs were a vital part of the university's overall mission to educate its students. The university adopted security policies and procedures to ensure that students had the most secure environment possible in which to work. Procedures could not be effective unless they are implemented. Subjects were asked how closely they followed the university’s computer management procedures.

Bob: Your lab managers, do they support your lab policies?

Subject G: Yes.

Bob: I mean, and I’m not talking about forcible, I’m talking about like overall, do they understand why you’re doing what you are doing?
Subject G: Yes, they are trained. We do training quite heavily at the first of the year. We do ... a whole bunch of training.”
Subject G: “The first staff meeting we have, we have [name] come in from Affirmative Action and talk about sexual harassment prevention. We have [name] come in and talk about PCI compliance and [personally identifying information], and all of that. We talk about that. Then we have [name] from the registrar’s office to talk about FERPA [Family Educational Rights and Privacy Act]. And those are some [of the] trainings that we bring people in to do to talk about certain things. Then we have our own training on security. How [we] handle certain things. The first training meeting is about six hours on the first Saturday for the new staff. Then we have the six hour training again the following Saturday for all of the staff, returning and new. And we continue ... training ... and security has been one [of the topics] that, over the years, has come to the top all of the time. It just, keeps coming up higher and higher and been talked about almost every time on different parts of security for the students.
Bob: So how much training do you provide your staff versus how much do you have to provide all the way down to the user level?

Subject G: The staff ... is trained heavily the first month. Thereafter, it’s four hours, once a month on Saturday mornings. And what was your second part of your question?

Bob: How much training do you provide to your users?

Subject G: [I wish we could do more]. [The University IT] fair ... that was wonderful. That was good training... We have some tutorials out there for them. Other than that, I don’t think there is much training at all.

Bob: Your user base is 16,000 students. So, what resources do you provide to train your students?

Subject G: Oh ok, yeah we do a little bit. We do have Connections (USU’s freshman and new student orientation program). We do Connections where we get ... 1800 hundred students [mostly] freshman. We have an hour with them at the beginning before school starts in the fall, where we have an hour of training on IT technology, and we go over a whole bunch of things ... Security is a big part of that [training].
We go over emails, what to watch for in [email]. We go over a whole bunch of stuff that covers IT, more than just security. [We also discuss] IT technology and what’s offered [as services to the students] and where to go find things and look for things.

**Review of the Effectiveness of the Chain-Link Fence Model in Procedure Creation of All Four Cases**

As stated previously, the effectiveness of security procedures could only be measured after the procedures had been fully implemented. This could be accomplished using an audit system. The university used the Nessus product to conduct a weekly penetration test on every computer connected to the university network.

Each lab manager was asked how often his computers are listed as “vulnerable” or “problem” computers on the Nessus scan. This data helped indicate whether or not their security procedures were working. All of the interviewed subjects stated that over the past year, none of their lab computers had come up on the Nessus scan. They were then asked if any of the other computers that they maintained for their departments came up on the scan. Everyone reported that about one or two per month.
The issues that most commonly caused the subjects’ computers to appear on the Nessus scan were mostly resolved by the implementation of their new procedures. Subjects were asked if they currently had any compromised computers that they knew about. Subject D had a major issue with one of his main servers. It was discovered that a computer that was used to submit homework had its root username and password hacked by an IP address originating in China. The USU IT Security team discovered this compromise using a statistical analysis to find anomalies in SSH patterns. SSH is a program used to remotely control a computer running the Unix operating system.

The compromised server acted as a rogue IRC bot and tried to infect other computers across the campus. More than 30 man-hours went into resolving this problem. Subject D reported that, luckily, this server did not include any personal identifying information.

It is important to note that this security episode was the only report of a compromised computer (out of the four subjects questioned) during the course of an entire year. That single computer was out of the 150 lab computers and 100 faculty and staff computers that Subject D managed. This supports the supposition that the procedures created
using the Chain-Link Fence Model created a safe computing environment.

**Conclusion of the Case Studies**

Computer security is a goal for any size organization. The labs in these case studies, while part of a larger organization, demonstrated how effective procedures could help reduce the exposure of small computing environments to security threats. The use of the Chain-Link Fence Model in these labs helped the lab managers come up with solutions to security problems. They found the model to be effective in producing the results that they were aiming to achieve. These new security procedures were recognized by the managers as beneficial and helped reduced their overall security footprint. The procedures were used by the managers and users to great success. As more of these new security procedures come on line, the entire organization’s IS security will likely increase both from the reduction of threats and also from user awareness. While some users complain about the less convenient use of some computers, the users of these labs see these new security procedures and are educated about the benefits of good information technology security.
A final comment about the case study is that the Chain-Link Fence Model was a useful tool to help design and create security procedures. The Chain-Link Fence Model helped users realize their unstated goal of wanting to ensure that their computer use was protected and secure.
FINAL CONCLUSIONS AND DISCUSSION

Summary of the Chain-Link Fence Model and its Validation

The Chain-Link Fence Model (CLFM) is a four component model to help information technology security specialists design and implement new, effective, and creative security procedures for their organizations. Information technology security once concerned only hard-wired computers. In the recent past, it has ballooned to encompass wired and wireless computers, as well as other wireless consumer devices that have a primary function other than that of a computer. Televisions, video games, cell phones, and even books in the form of electronic readers have now become devices that are able to transmit data over the internet. As technology continues to change, there will continue to be a need for security procedures to be created and revised.

The Chain-Link Fence Model was developed to be replicable. Each of the components, Buy-In, Implementation, Ease-of-use, and Effectiveness, were derived from both previous research and knowledge gained over lifetimes of experience. The model and its components, when used as a framework, help create information technology security procedures.
This model was validated in two parts. The first part validated the individual components using expert knowledge. The second part validated the entire model and the capabilities thereof. The first validation helped give cohesion to the model as a whole.

The managers' experience with the Chain-Link Fence Model, as stated in the interviews, showed that the components of the Chain-Link Fence Model, Buy-In, Implementation, Ease-of-Use, and Effectiveness, facilitated the creation of the new security procedures that in turn were well understood by both the users of the systems.

Conclusions

Conclusion 1: The usefulness of the CLFM is a consequence of its origin in theory, observation, and IT professional insight.

The Chain-Link Fence Model was a valuable tool in helping create and implement security policies and procedures. The model and its components were developed based on careful study of related literature and on the author’s personal observations. The synthesis of previous theoretical results and the author’s practical experiences resulted in the parsimonious model where all components
were essential, interconnected, and sufficient to achieve the stated goal of providing guidelines for the development of new security policies and procedures.

The experts stated that each component would help the culture of the university accept the security procedures. In the second validation part, some experienced members in information technology security at Utah State University used their training in Chain-Link Fence Model to develop new security policies for their specific situations. They stated that CLFM was useful in helping them form the new security procedures. These managers, using their expertise to create procedures using this model, were instrumental in determining the model’s usefulness in their individual domains.

**Conclusion 2:** The Chain-Link Fence Model is a scalable model for the creation of security procedures in large or small computer environments.

Through the creation of a set of four new, diverse examples of security procedures it was demonstrated that one could use the Chain-Link Fence Model to create procedures for labs and networks of varying sizes. Lab managers at USU used the Chain-Link Fence Model to create
procedures for small computing environments with one lab composed of only 25 computers. The computer lab managers stated that the computers they managed did not appear on the weekly vulnerability assessment with the help of their security procedures they developed using the Chain-Link Fence Model. In both the large and small cases, the policies and procedures were positively correlated with the reductions of the security threat footprints that appeared on the university’s security tests and measures.

**Conclusion 3:** The Chain-Link Fence Model may reduce the effort needed to create and implement procedures.

The computer lab managers using the Chain-Link Fence Model stated that once they had created the procedures, they were able to train their staff and faculty in as little as one or two training sessions and no training whatsoever in one case. This helped get the procedures out to the front lines in less time, resulting in quicker, more effective security threat reduction. These four examples suggested that using the Chain-Link Fence Model can reduce the time and perhaps cost required to develop security procedures.
Weaknesses

While it is clear from the interviews that the users of the Chain-Link Fence Model found the model effective, the design and nature of this study does not provide statistical evidence to support that claim. A new study design could focus upon gathering hard data to establish quantitative evidence. For such an undertaking to be effective, data collection will need to concentrate on gathering sufficient data from before and after the implementation of newly developed security policies.

A second weakness of the study arises from the nature of the university environment where the study was conducted. Any security breach related data collected between the months of May and August would be biased, due to the fact that usage rate falls dramatically during the academic break period. There are significantly fewer students on campus during the summer, and therefore, far fewer computers are connected to the network. This would cause any samples from those dates to bias the results. However, this could be partially offset by a seasonally adjusted usage rate. Any such considerations were outside of the scope of this study.
A final weakness is that the Chain-Link Fence model was validated and tested at only one university environment. While this creates an excellent environment for conducting research, any conclusion drawn from the research can only be directly applicable to that one university. For a full, complete evaluation, the Chain-Link Fence Model needs to be tested on other types of organizations.

**Future Research**

In the future, this study could be replicated in different organizational settings. The CLFM was used in large and small environments, but because the small environments tested were a part of the larger, there was only a relatively small variation in organizational culture and management structure. The university studied was a large public university. Smaller private universities and colleges face different overall threats to their external security. Most small private universities focus on a traditional liberal arts education. As a result, external hackers would mainly see them as a source of computing resources rather than as a source of a large body of research. Other environments such as hospitals, secure laboratories, and other large entities could benefit by
applying the Chain-Link Fence Model for IT security to their institutions. These institutions could be selected due to the similar requirements of data on their institutions. After applying the Chain-Link Fence Model at these institutions, the research could then be expanded to broader business and industry environments as well.

Additionally, the Chain-Link Fence Model could be studied further: refinement of each of the four components, path analysis of each of the components and how they relate to each other, and finally, exploration of possible additional components that may emerge in different environments than the one presented.

Each component of the Chain-Link Fence Model could be analyzed to see whether there are any sub-points within each component. Additionally, future studies could identify possible overlapping points in subcomponent. These subcomponents could include instructions or provisions for testing each of the main components during the creation of the procedures. These subcomponents could be used to design a more detailed outline for the creation of security procedures.

The Chain-Link Fence Model is a model to help organizations reach their security goals. This model is
just one tool that information technology security professionals can use to help accomplish their goals. Models and security research only explain human behavior. The true goal of any security professional is to understand how humans interact and to realize that technology is just part of the communication of human society.
REFERENCES


APPENDICES
APPENDIX A: Timeline of events

Figure 7, Timeline of Events

Feb 2008 - Computer Policy SSI Adopted
Aug 2009 - Task Force Created
Sept 2009 - Buy-in emerges as component based upon Task Force meetings
Nov 2009 - Reviewing academic literature spurs creation of other three components
Feb 2010 - Task Force creates security procedures
March 2010 - security procedures approved
April-June 2010 - Interviews with Subjects A-C: Validation of completeness of CLFM (Part 1)
January 2011 - CLFM Training
Aug-Dec 2011 - Interviews with Subjects D-G: Validation of CLFM in procedure creation (Part 2)
APPENDIX B: Security Setup

Windows Standard Setup

*Note: Only the procedures in the top tier (Required) are considered minimum requirements; the inclusion of any other steps is left to the discretion of the IT professional.*

<table>
<thead>
<tr>
<th>Required</th>
<th>Rating Average</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install/configure anti-virus software</td>
<td>4.95</td>
</tr>
<tr>
<td>Configure automatic Windows updates</td>
<td>4.80</td>
</tr>
<tr>
<td>Register IP address in OpenIPAM</td>
<td>4.55</td>
</tr>
<tr>
<td>Install/configure firewall software</td>
<td>4.37</td>
</tr>
<tr>
<td>Update drivers</td>
<td>4.27</td>
</tr>
<tr>
<td>Disable the local Windows Guest account</td>
<td>4.12</td>
</tr>
<tr>
<td>Disable auto-run</td>
<td>3.94</td>
</tr>
<tr>
<td>Recommended</td>
<td></td>
</tr>
<tr>
<td>Employ secure user password policies (complexity, length, expiration)</td>
<td>3.91</td>
</tr>
<tr>
<td>Convert file system to NTFS</td>
<td>3.79</td>
</tr>
<tr>
<td>Uninstall &quot;bloatware&quot;</td>
<td>3.79</td>
</tr>
<tr>
<td>Install/configure anti-malware software</td>
<td>3.79</td>
</tr>
<tr>
<td>Install/configure SCCM</td>
<td>3.29</td>
</tr>
<tr>
<td>Reformat hard drive and install Windows from scratch</td>
<td>3.11</td>
</tr>
<tr>
<td>Configure least necessary privileges for the computer owner's account</td>
<td>3.05</td>
</tr>
<tr>
<td>Configure automatic third-party software updates, when available (e.g., Adobe Updater)</td>
<td>3.05</td>
</tr>
<tr>
<td>Disable all unnecessary services (e.g., utilize Windows Baseline Security Analyzer)</td>
<td>2.94</td>
</tr>
<tr>
<td>Rename local Administrator account</td>
<td>2.52</td>
</tr>
<tr>
<td>Disable Administrator account</td>
<td>1.85</td>
</tr>
<tr>
<td>Optional</td>
<td></td>
</tr>
<tr>
<td>Employ a backup solution (e.g., shadow copy, store-to-network, portable external drive)</td>
<td>2.94</td>
</tr>
<tr>
<td>Configure services to use non-default ports (e.g., Remote Desktop)</td>
<td>2.88</td>
</tr>
<tr>
<td>Employ security-related group policies via Active Directory (i.e., join Windows domain)</td>
<td>2.82</td>
</tr>
<tr>
<td>Install/disallow certain web browsers</td>
<td>2.82</td>
</tr>
<tr>
<td>Install security protections specific to installed web browser(s) (e.g., FireFox No Script plug-in)</td>
<td>2.69</td>
</tr>
<tr>
<td>Configure power management options</td>
<td>2.68</td>
</tr>
<tr>
<td>Employ security-related local group policies</td>
<td>2.60</td>
</tr>
<tr>
<td>Install/configure third-party software update notifiers (e.g., Secunia Personal Software Inspector)</td>
<td>2.52</td>
</tr>
<tr>
<td>Install Windows from an actively maintained image (e.g., Ghost)</td>
<td>2.50</td>
</tr>
<tr>
<td>Install Windows from scratch with slipstreamed service packs and/or patches</td>
<td>2.41</td>
</tr>
<tr>
<td>Rename the local Windows Guest account</td>
<td>2.41</td>
</tr>
<tr>
<td>Remove local administrator privileges from computer owner's user account</td>
<td>2.40</td>
</tr>
</tbody>
</table>
Configure browser to automatically purge browsing history | 2.20  
Encrypt the hard drive | 1.33

**Windows High Security Setup**

*Note: Only the procedures in the top tier (Required) are considered **minimum requirements**; the inclusion of any other steps is left to the discretion of the IT professional.*

<table>
<thead>
<tr>
<th>Required</th>
<th>Rating Average</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install/configure anti-virus software</td>
<td>4.95</td>
</tr>
<tr>
<td>Configure automatic Windows updates</td>
<td>4.80</td>
</tr>
<tr>
<td>Register IP address in OpenIPAM</td>
<td>4.55</td>
</tr>
<tr>
<td>Install/configure firewall software</td>
<td>4.37</td>
</tr>
<tr>
<td>Update drivers</td>
<td>4.27</td>
</tr>
<tr>
<td>Disable the local Windows Guest account</td>
<td>4.12</td>
</tr>
<tr>
<td>Employ secure user password policies (complexity, length, expiration)</td>
<td>3.94</td>
</tr>
<tr>
<td>Convert file system to NTFS</td>
<td>3.91</td>
</tr>
<tr>
<td>Install/configure anti-malware software</td>
<td>3.79</td>
</tr>
<tr>
<td>Disable auto-run</td>
<td>3.39</td>
</tr>
<tr>
<td>Reformat hard drive and install Windows from scratch</td>
<td>3.11</td>
</tr>
<tr>
<td>Remove local administrator privileges from computer owner's user account</td>
<td>2.40</td>
</tr>
<tr>
<td>Configure browser to automatically purge browsing history (e.g., temp Internet files, cookies, history, form data, passwords)</td>
<td>2.20</td>
</tr>
<tr>
<td>Disable Administrator account</td>
<td>1.85</td>
</tr>
<tr>
<td>Encrypt the hard drive</td>
<td>1.33</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Recommended</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Uninstall &quot;bloatware&quot;</td>
<td>3.79</td>
</tr>
<tr>
<td>Install/configure SCCM</td>
<td>3.29</td>
</tr>
<tr>
<td>Configure least necessary privileges for the computer owner's account</td>
<td>3.05</td>
</tr>
<tr>
<td>Configure automatic third-party software updates, when available (e.g., Adobe Updater)</td>
<td>3.05</td>
</tr>
<tr>
<td>Disable all unnecessary services (e.g., utilize Windows Baseline Security Analyzer)</td>
<td>2.94</td>
</tr>
<tr>
<td>Rename local Administrator account</td>
<td>2.52</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Optional</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Employ a backup solution (e.g., shadow copy, store-to-network, portable external drive)</td>
<td>2.94</td>
</tr>
<tr>
<td>Configure services to use non-default ports (e.g., Remote Desktop)</td>
<td>2.88</td>
</tr>
<tr>
<td>Employ security-related group policies via Active Directory (i.e., join Windows domain)</td>
<td>2.82</td>
</tr>
<tr>
<td>Install/disallow certain web browsers</td>
<td>2.82</td>
</tr>
<tr>
<td>Install security protections specific to installed web browser(s) (e.g., FireFox No Script plug-in)</td>
<td>2.69</td>
</tr>
<tr>
<td>Configure power management options</td>
<td>2.68</td>
</tr>
<tr>
<td>Requirement</td>
<td>Rating</td>
</tr>
<tr>
<td>----------------------------------------------------------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>Employ security-related local group policies</td>
<td>2.60</td>
</tr>
<tr>
<td>Install/configure third-party software update notifiers (e.g., Secunia)</td>
<td>2.52</td>
</tr>
<tr>
<td>Install Windows from an actively maintained image (e.g., Ghost)</td>
<td>2.50</td>
</tr>
<tr>
<td>Install Windows from scratch with slipstreamed service packs and/or patches</td>
<td>2.41</td>
</tr>
<tr>
<td>Rename the local Windows Guest account</td>
<td>2.41</td>
</tr>
</tbody>
</table>

### Macintosh Standard Setup

*Note: Only the procedures in the top tier (Required) are considered minimum requirements; the inclusion of any other steps is left to the discretion of the IT professional.*

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Required</td>
<td></td>
</tr>
<tr>
<td>Perform Software Updates</td>
<td>5.00</td>
</tr>
<tr>
<td>Configure automatic Software Updates</td>
<td>4.75</td>
</tr>
<tr>
<td>Register IP address in OpenIPAM</td>
<td>4.46</td>
</tr>
<tr>
<td>Install/configure firewall software</td>
<td>4.40</td>
</tr>
<tr>
<td>Configure automatic third-party software updates, when available (e.g., Adobe Updater)</td>
<td>3.73</td>
</tr>
<tr>
<td>Disable the local Guest account</td>
<td>3.43</td>
</tr>
<tr>
<td>Install computer owner's various software products</td>
<td>3.17</td>
</tr>
<tr>
<td>Employ secure user password policies (complexity, length, expiration)</td>
<td>3.00</td>
</tr>
<tr>
<td>Remove local administrator privileges from computer owner's user account</td>
<td>2.65</td>
</tr>
<tr>
<td>Configure least necessary privileges for the computer owner's account</td>
<td>2.50</td>
</tr>
<tr>
<td>Rename local administrator account</td>
<td>2.50</td>
</tr>
<tr>
<td>Disable administrator account</td>
<td>2.00</td>
</tr>
<tr>
<td>Recommended</td>
<td></td>
</tr>
<tr>
<td>Install/configure anti-virus software</td>
<td>3.64</td>
</tr>
<tr>
<td>Employ a backup solution (e.g., Time Machine, store-to-network, portable external drive)</td>
<td>2.83</td>
</tr>
<tr>
<td>Configure services to utilize non-default ports (e.g., Remote Desktop)</td>
<td>2.80</td>
</tr>
<tr>
<td>Install/configure third-party software update notifiers (e.g., Secunia)</td>
<td>2.58</td>
</tr>
<tr>
<td>Employ security-related group policies (i.e., join Open Directory domain)</td>
<td>2.57</td>
</tr>
<tr>
<td>Configure power management options</td>
<td>2.57</td>
</tr>
<tr>
<td>Install/configure anti-malware software</td>
<td>2.56</td>
</tr>
<tr>
<td>Install security protections specific to installed web browser(s) (e.g., FireFox No Script plug-in)</td>
<td>2.48</td>
</tr>
<tr>
<td>Install/configure SCCM</td>
<td>2.47</td>
</tr>
<tr>
<td>Configure Permitted Applications</td>
<td>2.20</td>
</tr>
<tr>
<td>Configure browser to automatically purge browsing history</td>
<td>2.14</td>
</tr>
<tr>
<td>Optional</td>
<td></td>
</tr>
<tr>
<td>Install third-party web browsers (e.g., FireFox)</td>
<td>3.52</td>
</tr>
<tr>
<td>Reformat hard drive and install Mac OS X from scratch</td>
<td>2.89</td>
</tr>
<tr>
<td>Task</td>
<td>Rating</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>Convert file system to other file structure (e.g., UFS)</td>
<td>1.92</td>
</tr>
<tr>
<td>Install Windows via virtual machine (e.g., Parallels, VMWare Fusion)</td>
<td>1.92</td>
</tr>
<tr>
<td>Rename the local Guest account</td>
<td>1.89</td>
</tr>
<tr>
<td>Configure Simple Finder</td>
<td>1.71</td>
</tr>
<tr>
<td>Install Windows via BootCamp</td>
<td>1.63</td>
</tr>
<tr>
<td>Encrypt the hard drive</td>
<td>1.13</td>
</tr>
</tbody>
</table>

**Macintosh High Security Setup**

*Note: Only the procedures in the top tier (Required) are considered **minimum requirements**; the inclusion of any other steps is left to the discretion of the IT professional.*

<table>
<thead>
<tr>
<th>Task</th>
<th>Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perform Software Updates</td>
<td>5.00</td>
</tr>
<tr>
<td>Configure automatic Software Updates</td>
<td>4.75</td>
</tr>
<tr>
<td>Register IP address in OpenIPAM</td>
<td>4.46</td>
</tr>
<tr>
<td>Install/configure firewall software</td>
<td>4.40</td>
</tr>
<tr>
<td>Configure automatic third-party software updates, when available (e.g., Adobe Updater)</td>
<td>3.73</td>
</tr>
<tr>
<td>Disable the local Guest account</td>
<td>3.43</td>
</tr>
<tr>
<td>Install computer owner’s various software products</td>
<td>3.17</td>
</tr>
<tr>
<td>Employ secure user password policies (complexity, length, expiration)</td>
<td>3.00</td>
</tr>
<tr>
<td>Remove local administrator privileges from computer owner’s user account</td>
<td>2.65</td>
</tr>
<tr>
<td>Configure least necessary privileges for the computer owner’s account</td>
<td>2.50</td>
</tr>
<tr>
<td>Rename local administrator account</td>
<td>2.50</td>
</tr>
<tr>
<td>Disable administrator account</td>
<td>2.00</td>
</tr>
<tr>
<td>Configure Simple Finder</td>
<td>1.71</td>
</tr>
<tr>
<td>Encrypt the hard drive</td>
<td>1.13</td>
</tr>
<tr>
<td>Configure Permitted Applications</td>
<td>2.20</td>
</tr>
<tr>
<td>Install/configure anti-virus software</td>
<td>3.64</td>
</tr>
<tr>
<td>Employ a backup solution (e.g., Time Machine, store-to-network, portable external drive)</td>
<td>2.83</td>
</tr>
<tr>
<td>Configure services to utilize non-default ports (e.g., Remote Desktop)</td>
<td>2.80</td>
</tr>
<tr>
<td>Install/configure third-party software update notifiers (e.g., Secunia)</td>
<td>2.58</td>
</tr>
<tr>
<td>Employ security-related group policies (i.e., join Open Directory domain)</td>
<td>2.57</td>
</tr>
<tr>
<td>Configure power management options</td>
<td>2.57</td>
</tr>
<tr>
<td>Install/configure anti-malware software</td>
<td>2.56</td>
</tr>
<tr>
<td>Install security protections specific to installed web browser(s) (e.g., FireFox No Script plug-in)</td>
<td>2.48</td>
</tr>
<tr>
<td>Install/configure SCCM</td>
<td>2.47</td>
</tr>
<tr>
<td>Configure browser to automatically purge browsing history</td>
<td>2.14</td>
</tr>
<tr>
<td>Task</td>
<td>Rating</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>Install third-party web browsers (e.g., FireFox)</td>
<td>3.52</td>
</tr>
<tr>
<td>Reformat hard drive and install Mac OS X from scratch</td>
<td>2.89</td>
</tr>
<tr>
<td>Convert file system to other file structure (e.g., UFS)</td>
<td>1.92</td>
</tr>
<tr>
<td>Install Windows via virtual machine (e.g., Parallels, VMWare Fusion)</td>
<td>1.92</td>
</tr>
<tr>
<td>Rename the local Guest account</td>
<td>1.89</td>
</tr>
<tr>
<td>Install Windows via BootCamp</td>
<td>1.63</td>
</tr>
</tbody>
</table>

**Windows & Macintosh Ongoing Maintenance**

Note: The following recommendation is generic for both Windows and Macintosh systems, but some procedures may be OS-specific. Only the procedures in the top tier (orange) are considered minimum requirements; the inclusion of any other steps is left to the discretion of the IT professional.

<table>
<thead>
<tr>
<th>Task</th>
<th>Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patch OS with available updates</td>
<td>4.95</td>
</tr>
<tr>
<td>Patch third-party software with available updates</td>
<td>4.37</td>
</tr>
<tr>
<td>Perform automated / scheduled anti-virus scans</td>
<td>4.03</td>
</tr>
<tr>
<td>Disconnect unused network connections</td>
<td>3.79</td>
</tr>
<tr>
<td>Perform regular data backups</td>
<td>3.67</td>
</tr>
<tr>
<td>Check for unknown file shares</td>
<td>3.59</td>
</tr>
<tr>
<td>Check for unknown user accounts</td>
<td>3.50</td>
</tr>
<tr>
<td>Perform automated / scheduled anti-malware scans</td>
<td>3.46</td>
</tr>
<tr>
<td>Check and confirm the integrity of data backups</td>
<td>3.34</td>
</tr>
<tr>
<td>Remove unused programs</td>
<td>3.26</td>
</tr>
<tr>
<td>Regularly defragment the hard drive</td>
<td>3.17</td>
</tr>
<tr>
<td>Perform manual anti-malware scans</td>
<td>3.00</td>
</tr>
<tr>
<td>Free up wasted space (e.g., Disk Cleanup)</td>
<td>2.94</td>
</tr>
<tr>
<td>Perform manual anti-virus scans</td>
<td>2.83</td>
</tr>
<tr>
<td>Regularly run hard drive repair utilities (e.g., chkdsk)</td>
<td>2.66</td>
</tr>
<tr>
<td>Clear cache, cookies, and browser history and temporary Internet files</td>
<td>2.59</td>
</tr>
<tr>
<td>Audit available anti-virus logs</td>
<td>2.58</td>
</tr>
<tr>
<td>Audit available operating system logs</td>
<td>2.39</td>
</tr>
<tr>
<td>Audit available anti-malware logs</td>
<td>2.38</td>
</tr>
<tr>
<td>Audit available firewall logs</td>
<td>2.27</td>
</tr>
<tr>
<td>Utilize third-party registry maintenance tools (e.g., Registry Mechanic)</td>
<td>2.11</td>
</tr>
</tbody>
</table>
APPENDIX C: Interview Questions

1. What are the goals for the task force?
2. What do you think the task force produced?
3. Why do you think that USU needs the computer security standards?
4. To what end do you think the task force can:
   A. Achieve the common task?
   B. Work as a team?
   C. Meet individual (department) needs?
5. How do you think the task force used the following ideas?
   Effective groups? evaluated the validity of opinions
   Effective groups? analyzed possible solutions thoroughly
   Based their decisions on reasonable premises
   Leaders encouraged constructive arguments
6. Did the final conclusions match your expectations?
7. Did you agree with the final conclusions?
8. Where were the final conclusions lacking?
   A. Where was their strength?
9. Is there anything you would change about the group or its interpretation of the needs of the
university?

10. How do you think that the university will change because of these recommendations?

11. How do you think the university will implement these recommendations?
APPENDIX D: Biography of Subjects

These subjects came from a variety of backgrounds: one was a musician in the military for 20 years; one was an electrical engineer who started fiddling with computers in his later life; another was a traditional computer science major who always knew that working in computing environments was what he wanted to do.

Subject A was the CIO of the organization. His executive responsibilities included providing strategic information systems direction to the institution, as well as focusing the efforts of approximately 90 full time employees and a multimillion-dollar budget in support of the University’s mission. He held a doctoral degree in Education, specializing in Management Information Systems, a Business masters degree, and a Bachelors degree in Computer Engineering. His focus over the past three years was a strategic and comprehensive restructuring of all information systems, services, and policies, focusing on benefit to the overall institution. This effort created a successful unified approach to a broad range of information systems and services. In addition to his executive roles, he enjoyed teaching strategic IS management, technology, e-commerce, and financial topics, presenting by invitation
nationally, as well as teaching at USU and the University of Phoenix. His approach to management was to simply have his employees call him by his first name. He describes himself as “an average father of five, who just happens to be able to explain a lot of acronyms. People enjoy [his] humor and ability to share useful information with everyone, especially non-techies!”

Subject B was formerly the director of information technology marketing and was promoted to director of special projects. He was previously responsible for the marketing, communication and training with Information Technology at Utah State University. In this role, he coordinated the Network Managers meetings, encompassing all the IT Professionals at the University. He held a Bachelors degree in Computer Science and a Masters in Instructional Technology. Since 2001, he was the Senior Instructional Designer at the Faculty Assistance Center for Teaching, a technology center for faculty. He enjoyed working with faculty to help them integrate technology into their teaching.

As director of special projects, Subject B was chair of the committee to search for new technology solutions to ongoing organizational problems. His project was the
development of a campus-wide voice over IP system.

Subject C was the head of university information technology security. He started one of the first full-time dedicated information technology security teams in the state. He fondly recalled childhood memories of riding a tricycle back and forth on the USU campus. He wanted to stay at USU for as long as he could remember, and as a result, most of his reward was simply participating at USU. To quote: “I pestered the people who were IT years and years ago, checked on them every month asking if they had a job or so. Every week or two for several months until they finally offered me an entry-level job, and that was almost thirty years ago. So I’ve been doing IT ever since.”

Back in the days when Subject C got that first job, computers were still using punch cards. He started at the mainframes, helped run the early forms of the USU help desk, and helped manage the earliest computer labs, CPM machines, MS-DOS machines, and Windows machines. At the time of his interview he used Linux as his primary operating system. At one time, he was involved in telecommunications. That was where he finally learned the basics of the scientific method—how to test things and how to do diagnostics and debugging. That revelation strongly affected his career,
leading him into more complicated environments and the management of more complicated systems at USU. He stated: “So I’m not here, for the most part, not because they pay me, or because that’s where I could get work. I’m here because this is where I wanted to be.”

Subject D was with the organization for over 20 years. He graduated from USU with a Bachelor in Computer Science. He loved computer science so much that he stayed with the department and formed one of the first college-specific IT departments. At the time of his interview, he managed a lab with over 150 computers. Of those 150, the majority used the Microsoft Windows operating system, four were Apple Mac OS X based Mackintoshes, and eight used different distributions of Linux. He also managed all the computers for the computer science department.

As part of his duties, Subject D also oversaw student lab managers. They helped him run the day-to-day operations of his computer lab. He stated that they are responsible for maintaining a sense of presence to help keep the users of the lab mindful of their actions. He described his faculty as “knowledgeable,” and because there are concerned experts in the field, they maintained their own systems. His hobbies included amateur radio and telecommunications.
Subject E managed the labs in the College of Humanities. He was with the college for five years. His training happened mainly on the job, starting when he was a student intern with the research laboratory performing desktop support for the scientists. His current responsibilities included managing two major computer labs in the English Department consisting of 48 computers and one major lab in the Journalism department consisting of 20 computers. He also managed various small labs for other departments, each with 2 to 5 computers. His labs were split 90 percent Microsoft Windows to 10 percent Apple OS X, with no installations of Linux. Subject E oversaw two student interns that not only helped out in his lab but also covered some basic desktop support for the employees of the college. He was still working on his undergraduate degree and continued to dabble in computer gaming.

Subject F came into computers through a very different path. After completing 18 years in the Marines as a musician, he realized that he would need a new skill set for civilian life. He used the G.I. Bill to formally train as a musician and found himself attending the Open Source and Free Software Club at Utah State University. He stated that he always had an attraction to technology, which
started in the military and grew once he came to college. He added computer science as a major and graduated with degrees in both music and computer science. The focus of his undergraduate studies was open source software.

During his undergraduate studies, Subject F was hired by the College of Education as a second to the primary technology specialist. He quickly became the go-to guy in the college for Unix-based operating systems. His use of Unix-based operating systems led him to become the server and lab manager for the Instructional Technology department. Subject F’s computer lab consisted of 30 Apple Macintosh computers. He stated, “Education has always been predominantly Mac; it seemed only natural to provide a Mac-based solution for our education environment.” While the primary use of these computers was to run Mac OS X applications, he also configured them to dual boot with Microsoft Windows. However, the Windows side was not directly connected to the servers. Subject F was the only support for his lab, and he used Apple-based security tools to help him manage it. He recently was married and was expecting a new child in May 2012.

The final subject, Subject G, was the manager for all the open access labs on the Logan campus. His 369 computers
were spread across 7 computer labs with another 20 computers coming on-line in the upcoming year. Most of the computers were Windows-based PCs, while 60 of the lab computers were Apple Macintosh computers.

Subject G was also the Manager of Information Technology Services for Utah State University. He graduated from Utah State University with a degree in Administrative Systems and Business Administration with an emphasis in Computer Science. For the past 24 years, Subject G managed, maintained, and provided technical and customer services to students, faculty, and staff at Utah State University.

As a part of his position, Subject G maintained the responsibility of managing and maintaining seven open-access computer labs, in which he hired and managed 85 student workers. Subject G continued to dedicate his time in assisting Utah State University students, in pursuit of their academic goals, by providing state-of-the-art computing technology, software, and hands on experiences.
Robert F. Houghton  
838 Hillcrest Ave  
Logan, Utah 84321  
(435) 363-7451  
E-mail: bob.houghton@gmail.com

OBJECTIVE

To obtain a position where I can use my expertise to support all facets of computer networks, domains, and workstations.

WORK EXPERIENCE

Utah State University, Vice President for Information Technology  
February 2011 – Present

Network Security Specialists

- Created and implemented system of NetFlow data generators and collectors using open-source tools across the entire USU Network
- Created and implemented internal PCI audit procedures including virtual and physical penetration testing.
- Created and implemented an Intrusion Detection System using Snort
- Created custom Snort rules for USU sensitive systems
- Implemented upgrade to Nessus scanner and created new scan policies
- Installed and configured custom border firewall rules

Utah State University, Caine College of the Arts  
July 2010 – January 2011

Systems Administrator

- Led division of IT resources between the College of Humanities and Social Sciences and the Caine College of the Arts
- Created College IT five-year plan using limited budget resources, including outsourcing most IT needs from the college to the central IT teams

Utah State University, College of Humanities, Arts and Social Sciences  
January 2006 – June 2010

Associate Systems Administrator

- Composed university wide security policies
- Co-chaired university committee to standardize policies across colleges
- Installed, configured, and administered System Center Configuration Manager in a trusted multi-domain environment
- Installed, configured, and administered Apple Remote Desktop and Task Server across Windows 2003 Active Directory Domain
- Analyzed, documented and tracked security events across the College
- Configured and deployed new VMWare-based solutions for our server needs
- Integrated Mac OS X and Linux into a Windows 2003 Domain Environment
- Created and maintained Group Policies for Windows 2003 Active Directory
Utah State University Research Foundation, North Logan, UT
July 2003 – December 2005

IT Support
- Provided fast and reliable desktop support
- Installed and configured workstations
- Troubleshot network problems
- Advised and performed workstation upgrades

Computer Solutions, Santa Rosa, CA
May 1999 – January 2002

Head Technician
- Built custom computers for clients
- Provided support for client computers and networks
- Installed and maintained various database programs for clients
- Built and installed Microsoft NT 4.0 and 2000 networks and servers
- Advised and performed network upgrades
- Maintained Novell 5.0 server

CERTIFICATION
Systems Security Certified Practitioner (SSCP)

MCSE:S certification on Windows Server 2003

EDUCATION
2013. Utah State University, Logan Utah
Doctor of Philosophy in Management Information Systems

2008. Utah State University, Logan, Utah
Masters of Science in Management Information Systems

2006. Utah State University, Logan, Utah
Bachelors of Music in Music, Cum Laude

2001. Santa Rosa Junior College, Santa Rosa, California
Graduate, Associates of Arts with Honors