The Dissertation Committee for Jonathan Reed Sylvie Certifies that this is the approved version of the following dissertation:

Developing Best Practices for Industrial Project Life Cycle Security and a Methodology for Measuring Implementation

Committee:

Carl T. Haas, Supervisor

Stephen R. Thomas, Co-Supervisor

G. Edward Gibson, Jr.

Carlos H. Caldas

Zhanmin Zhang

Arthur Sakamoto, Jr.

Developing Best Practices for Industrial Project Life Cycle Security and a Methodology for Measuring Implementation

by

Jonathan Reed Sylvie, B.S., M.B.A.

Dissertation

Presented to the Faculty of the Graduate School of

The University of Texas at Austin

in Partial Fulfillment

of the Requirements

for the Degree of

Doctor of Philosophy

The University of Texas at Austin

May 2005

Dedication

To my wife, Amanda, and my son, Jacob, for their unconditional love and the immeasurable joy they bring to my life. To my parents, Gloria Sylvie, and Arthur and Kathleen Sylvie, for their love, dedication, and the sacrifices they have made for me throughout my life.

Acknowledgements

I would like to acknowledge the support provided to this research by the United States Army, the National Institute of Standards and Technology (NIST), and the Construction Industry Institute (CII) at the University of Texas at Austin. The US Army granted me the privilege of pursuing a doctorate; I would not have had this tremendous opportunity otherwise. NIST funded the initial research study to determine best practices for project life-cycle security. Additional research was funded by CII and supported by industry experts from its member companies.

My sincere gratitude is extended to my research supervisor, Dr. Stephen R. Thomas. He spent innumerable hours guiding me throughout my research and writing. Dr. Thomas exemplifies a mentor; he has been a role model to me both personally and professionally. His selflessness is a major contributing factor to the success of my research.

I am also grateful for the efforts of my supervisor, Dr. Carl T. Haas. Dr. Haas always made time to meet with me when I needed his guidance, regardless of any other responsibilities competing for his attention. I appreciate that Dr. Haas always encouraged candid discourse, even if it meant that I challenged his views.

I would like to thank the other members of my graduate committee, Dr. G. Edward Gibson, Jr., Dr. Carlos H. Caldas, Dr. Zhanmin Zhang, and Dr. Arthur Sakamoto,

Jr. for their valuable insight and guidance. I am also indebted to Robert Chapman, Ph.D. of NIST for his dedication to this research; his advice and input was invaluable.

Finally, I would like to thank my wife, Amanda, for her support, patience, and encouragement throughout the last two and one-half years.

May 3, 2005

Developing Best Practices for Industrial Project Life Cycle Security and a Methodology for Measuring Implementation

Publication No._____

Jonathan Reed Sylvie, Ph.D.

The University of Texas at Austin, 2005

Supervisor: Carl T. Haas

Co-Supervisor: Stephen R. Thomas

The intent of this research was to establish security-related best practices with respect to the delivery of capital facility projects for the industrial sector. Its purpose was to develop security best practices for implementation during the project phases of front-end planning through startup to enhance facility security throughout its life cycle.

Proven construction industry best practices for project delivery were evaluated and used to identify specific security requirements. After identifying the essential security practices, these practices were categorized by security elements for organization and analysis. The practices were further grouped by project phase to assist with scoring of their use.

A Security Rating Index (SRI) was developed to provide a quantitative means for determining the level of use of the practices and for assessing impacts on cost, schedule, and safety. Use of the SRI requires the selection of consequence levels, which quantify potential results of a security breach over the facility life cycle, and threat levels, which

quantify the intention and capability of an adversary to undertake detrimental actions. These concepts allow comparisons to be made between projects with similar security requirements.

An Internet-based questionnaire was programmed to collect project data for analysis. Following data collection, project information was analyzed to determine the relationship between project characteristics and security practice implementation.

Based upon the research and data analysis, a methodology for implementing security best practices for industrial projects was developed to facilitate the adoption of the security best practices by industry. While it does not provide specific guidance for the implementation of security procedures at the project level, it offers a framework for integrating security into the project delivery process in the context of likely threats facing the facility and consequences of security breaches.

Table of Contents

List of Tables

List of Figures

Chapter 1. Introduction

The terrorist attacks of September 11, 2001 highlighted the need for integrating security into every sector of the national economy. From guarding borders, ports and airports, to protecting critical infrastructure and defending against terror and sabotage, security requires a partnership between the public and private sectors to evaluate and develop systems that will reduce vulnerability to attack (Construction Industry Institute 2004a). While the federal sector has a critical role in spearheading the initiative for enhanced security and decreased vulnerability, the private sector requires considerable latitude in managing its own endeavors (National Institute of Standards and Technology 2004a). The goal of ensuring security for the nation as a whole can only be achieved through the development of a public-private partnership.

The *National Strategy for Homeland Security* (Office of Homeland Security 2002) lists three strategic objectives necessary to meet the nation's goal of security. These are: prevent terrorist attacks in the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur. The first falls largely under the provenance of the federal government. One of the traditional roles of government in a market-driven society is to provide goods and services that benefit the public good, like defense, communications, or transportation infrastructure (Construction Industry Institute 2004a). Such goods and services cannot be provided easily through the market forces of supply and demand because it is difficult to quantify and market the units of goods or services to individual consumers. The second and third objectives, however, cannot be fully achieved without the active participation of the private sector. Among the eight mission critical areas identified in the *National Strategy for Homeland Security* is the protection of critical infrastructure and key assets. Some of the private (or

quasi-private) sector industries included in this area are: water treatment, energy (i.e., oil production and refining, natural gas processing and distribution, and power generation and distribution), chemical manufacturing, and transportation infrastructure (Bush 2003). Reducing vulnerability and minimizing damage can be accomplished by private sector initiatives to evaluate and enhance physical, personnel, and information security during project delivery, thus improving project security through the project life cycle. The aim of physical security is to deter, detect, and delay malicious acts through systems and architectural features. Personnel security includes practices and procedures for screening, hiring, terminating, or addressing workplace issues. Information security is the protection of information systems, including hardware, software, and data, from loss or damage (Center for Chemical Process Safety of the American Institute of Chemical Engineers 2002).

This chapter highlights the need for this research, presents a background of the Construction Industry Institute (CII) and the National Institute of Standards and Technology (NIST), and presents an overview of the CII/NIST study that was the foundation of this research. The research hypothesis is then established, followed by the research objectives, and scope of the research. Finally, the organization of the dissertation is explained, which summarizes the contents of each chapter.

1.1. THE CONSTRUCTION INDUSTRY INSTITUTE

CII is a research institute for engineering and construction that is comprised of more than 90 member organizations, representing leading owners, contractors, and suppliers in both the public and private sectors. The members fund studies at leading universities to identify ways to improve the planning and execution of major construction projects (Construction Industry Institute 2004b). The mission of the Construction Industry Institute is "to add value for members by enhancing the business effectiveness

and sustainability of the capital facility life cycle through CII research, related initiatives, and industry alliances" (Construction Industry Institute 2004c).

1.2. THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

The National Institute of Standards and Technology (NIST) is a non-regulatory federal agency within the U.S. Commerce Department's Technology Administration (National Institute of Standards and Technology 2004c). Its mission is "to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve quality of life" (National Institute of Standards and Technology 2000).

In the aftermath of the attacks of September 11, 2001, NIST has taken a key role in enhancing the nation's homeland security. Through projects spanning a wide range of research areas, NIST is helping millions of individuals in law enforcement, the military, emergency services, information technology, the construction industry, and other areas protect the American public from terrorist threats (National Institute of Standards and Technology 2004d).

1.3. BACKGROUND OF THE CII/NIST STUDY

The genesis of this research, funded by the Demonstration and Technical Assistance Program of the Building and Fire Research Laboratory (BFRL) at NIST, was the recognized need to secure national assets and infrastructure in the wake of the events of September 11, 2001. The goal of BFRL's homeland security effort is to develop and implement the standards, technology, and practices needed for cost-effective improvements to the safety and security of buildings and building occupants, including evacuation, emergency response procedures, and threat mitigation (National Institute of Standards and Technology 2004b).

In November 2002, NIST selected CII to determine best practices for project life-cycle security. Because the membership of CII is heavily weighted in the industrial sector, the first phase of the study focused on industrial projects. Research commenced in January 2003 and the funded research concluded in December 2003.

1.4. PROBLEM STATEMENT

The construction industry does not currently have best practices to integrate security into the project delivery process or measure the implementation of those practices. A best practice is defined as a process or method that, when executed effectively, leads to enhanced project performance (Construction Industry Institute 2002).

Current risk analysis methods are measuring *product* (results) not *process* (tasks and actions), i.e., the objective is to minimize losses versus *avoiding* incidents. Many public and private organizations have developed methods to characterize security threats, but few have published recommended actions or processes to address security vulnerabilities.

1.5. RESEARCH HYPOTHESES

This research is established upon the following hypotheses: (1) that security best practices can be defined and developed for industrial sector projects, and (2) security best practices can be measured given the context of the threat level of security risk and the consequence level of a security breach.

1.6. RESEARCH OBJECTIVES

The objective of this research was to: (1) develop best practices for integrating security into the industrial project delivery process, and (2) to provide a methodology to assess the impacts of these approaches on key business outcomes such as project cost,

schedule, and safety performance. To support the Research Objective, the following sub-objectives were identified:

1. Develop a Security Rating Index (SRI) to measure the implementation of security best practices in the project delivery process.
2. Validate the SRI through expert opinion and data collection
3. Establish the relationship between Threat Level, Consequence Level, and SRI
4. Establish a methodology for assessing the impact of security implementation on project outcomes such as cost and schedule performance
5. Address common security deficiencies based upon data analysis.

1.7. RESEARCH SCOPE

This research is a result of the NIST-funded study to develop best practices for project life-cycle security conducted at CII. This research applies specifically to industrial-sector construction projects; future research will be necessary to validate which practices apply to other sectors, such as infrastructure or building projects.

As security-related enhancements are less costly and more effective when integrated during the early phases of the project life cycle, the research scope includes the following project phases: front end planning, detailed design, procurement, construction, and startup.

1.8. ORGANIZATION OF THE DISSERTATION

Chapter 1 of the dissertation describes the purpose of the research conducted, as well as the research hypothesis, objectives, and scope. Chapter 2 explores the background and motivation of addressing project life-cycle security. The research

methodology is detailed in Chapter 3, including formation of the research teams, review of CII best practices, and the development of the best practices for project lifecycle security. Chapter 4 details the development and interpretation of the Security Rating Index and an overview of data collection. Chapter 5 provides a descriptive analysis of the project data collected. The approach to the statistical analysis of the project data is presented in Chapter 6. Chapter 7 contains the statistical analysis of the project data and the development of a regression model to quantify the relationship between Consequence Level and SRI score. A recommended methodology of implementing project security is presented in Chapter 8. Conclusions and recommendations are found in Chapter 9.

Chapter 2. Background

This chapter presents background information on project security and risk analysis as a means for explaining the context of the research. The definition of security is provided and concepts in risk analysis are explored.

2.1. DEFINITION OF SECURITY

Security, as defined in *Webster's New Collegiate Dictionary*, is "measures taken to guard against espionage or sabotage, crime, attack, or escape" (Merriam-Webster Inc. 1980).

The American Heritage Dictionary of the English Language introduces the concept of risk into its definition of security as "freedom from risk or danger; safety" (Houghton Mifflin Company 2000).

The Practice Development Team (Section 3.2) decided that the definition of security should not only consider the likelihood of an incident, but some measure of the probability or risk of occurrence. Additionally, the team felt that the impact of a security breach should be reflected in the definition as well. After numerous revisions, the team adapted the definition from *Webster's* and brainstormed a more comprehensive definition:

> Security includes all measures taken to guard against *malevolent, intentional acts*, both internal and external (e.g., sabotage, crime, and attack), that result in *adverse impacts* such as project cost growth, schedule extension, operability degradation, safety concerns, transportation delays, emergency response, and *offsite effects/consequences (Construction Industry Institute 2004a).*

2.2. BUSINESS IMPLICATIONS OF SECURITY

According to the American Academy of Actuaries, the events of September 11 caused the largest insured property/causality (P/C) loss ever recorded, estimated to be in

the range of $30-$70 billion (American Academy of Actuaries 2002). While P/C rates had been steadily increasing from Fall 1998 to Fall 2001, the events of September 11 prompted most major reinsurers to exclude or substantially decrease terrorism coverage in commercial insurance policies, resulting in a shifting of the risk exposure from reinsurers and direct insurers to the private sector as "out of pocket" costs (American Academy of Actuaries 2002). This has had tangible negative effects on the economy, particularly in the real estate and construction sectors (American Academy of Actuaries 2002).

Apart from macro-level, national security interests, attention to security throughout the capital facility life cycle has a bottom-line financial impact as well. As the risk of coverage for terrorist attacks is shifted from insurers to companies due to changes in the insurance industry, it is critical that companies focus on security during the front-end stages of project execution. A security focus during planning, design, and even construction may yield tangible benefits in eliminating or mitigating the effects of terror or sabotage during the later operational phases of facilities (Construction Industry Institute 2004a). Consideration of security issues during the project life cycle can provide a valuable indicator of the need for security enhancements as threats or consequences of terror or sabotage change. Insurers are once again looking favorably upon those organizations that are actively seeking to manage the risks they face (Jolly 2003).

2.3. RISK IN THE CONSTRUCTION INDUSTRY

Within construction organizations, the management of risk as it relates to security issues is crucial to business success (Jolly 2003). Construction companies have been limiting new expansion because of increased risk exposure and costs. A study by the National Equipment Register (NER) concluded that stolen heavy equipment alone results

in $300 million to $1 billion each year in losses and indirect costs, such as rentals, downtime, wasted management time and project overrun penalties (National Equipment Register 2004). In a survey by toolmaker DeWalt, 97% of construction industry professionals surveyed said they were concerned about jobsite security, and 60% said that tool theft is the number one concern with the greatest financial impact (The Construction Specialist 2005). National Equipment Register's *2004 Equipment Theft Report* found that as little as 10% of stolen equipment was ever recovered (National Equipment Register 2004).

According to Michael Bardenaro, "People feel they have to protect everybody from everything, but no one has that type of budget, so you have to prioritize" (Bardenaro 2003).

2.4. RISK ANALYSIS

Risk analysis, in the context of security, is a method of identifying the hazards that could lead to security breaches, analyzing the identified hazards, and assessing the risks against defined criteria to determine their tolerability (Redmill 2002).

A properly formed risk analysis: (1) shows current security posture, (2) highlights areas where more or less security is needed, (3) assembles facts to develop and justify safeguards, and (4) increases security awareness by assessing strengths and weaknesses of security (Bardenaro 2003).

With respect to security analysis, risk can be defined as the product of threat, vulnerability, and consequence, as shown in Figure 2.1 (Guthrie et al. 2005).

Risk = Threat (T) x Vulnerability (V) x Consequence (C)

Where:

Threat is a measure of the likelihood that a specific type of attack will be initiated against a specific target;

Vulnerability is a measure of the likelihood that various types of safeguards against a scenario will fail

Consequence is the magnitude of the negative effects if the attack is successful

Adapted from Guthrie et al. (2005)

Figure 2.1. Security analysis risk definition

2.4.1. The Dangers of Risk Analysis

A major problem in assessing risk is the recognition or identification of the complete range of risks to the subject being analyzed (Ansell and Wharton 1992). Risk assessment is a difficult process because the perception of danger is continually being increased, by past events and new technologies (Ansell and Wharton 1992).

There is also the danger that the identification of risks will be seen as solving the problem due to the implicit assumption that mitigation measures will achieve their objective of eliminating the risk (Ansell and Wharton 1992).

Another consideration is that risk analysis can produce results that are completely obvious, or of no practical use. Countless incidents, from the Titanic to September 11, show that the 'very unlikely' does happen (Jolly 2003).

2.4.2. Deficiencies in Risk Analysis

Risk analysis is often assumed to be objective, and its results to be correct, yet all stages of the process, including the techniques used, involve subjectivity (Redmill 2002). This subjectivity is due to uncertainty, the need for judgment, considerable scope for human bias, and inaccuracy – the results obtained by one risk analyst are unlikely to be obtained by others with the same information (Redmill 2002).

Individuals or firms deciding how to best protect themselves are unlikely to take the external costs of consequence fully into account and will generally provide an insufficient level of security on their own (O'Hanlon 2003).

Chapter 3. Methodology

This chapter details the methodology used in performing the research. It discusses the formation of the research teams, identification of the security best practices, and creation of the security questionnaire, as shown in Figure 3.1. Development of the Security Rating Index and collection of the data are detailed in Chapter 4. Subsequent chapters will provide descriptions and analysis of the data.

3.1. THE STEERING TEAM

The Steering Team was formed to frame the methodological approach to developing a security best practice. The Steering Team was composed of industry representatives in policy-making positions within their organizations, the study sponsor, and the principal investigator. Industry representatives were selected to ensure a broad-based industrial perspective from owner and contractor organizations engaged in the engineering, construction, and operation of electrical, oil and gas processing and delivery; and chemical and petrochemical manufacturing. The positions and company affiliations of the Steering Team are listed in Appendix A.

The initial approach was to convene a series of regional workshops and site visits to learn what steps were being taken within the industry to address security following the events of September 11, 2001 with the intention of developing a standalone security best practice. At the first Steering Team meeting, however, discussion led the team members to conclude that security should be a part of all project best practices rather than a standalone best practice. Furthermore, the Steering Team recognized the opportunity to leverage CII‘s extensive library of Best Practices as a foundation upon which security practices could be integrated.

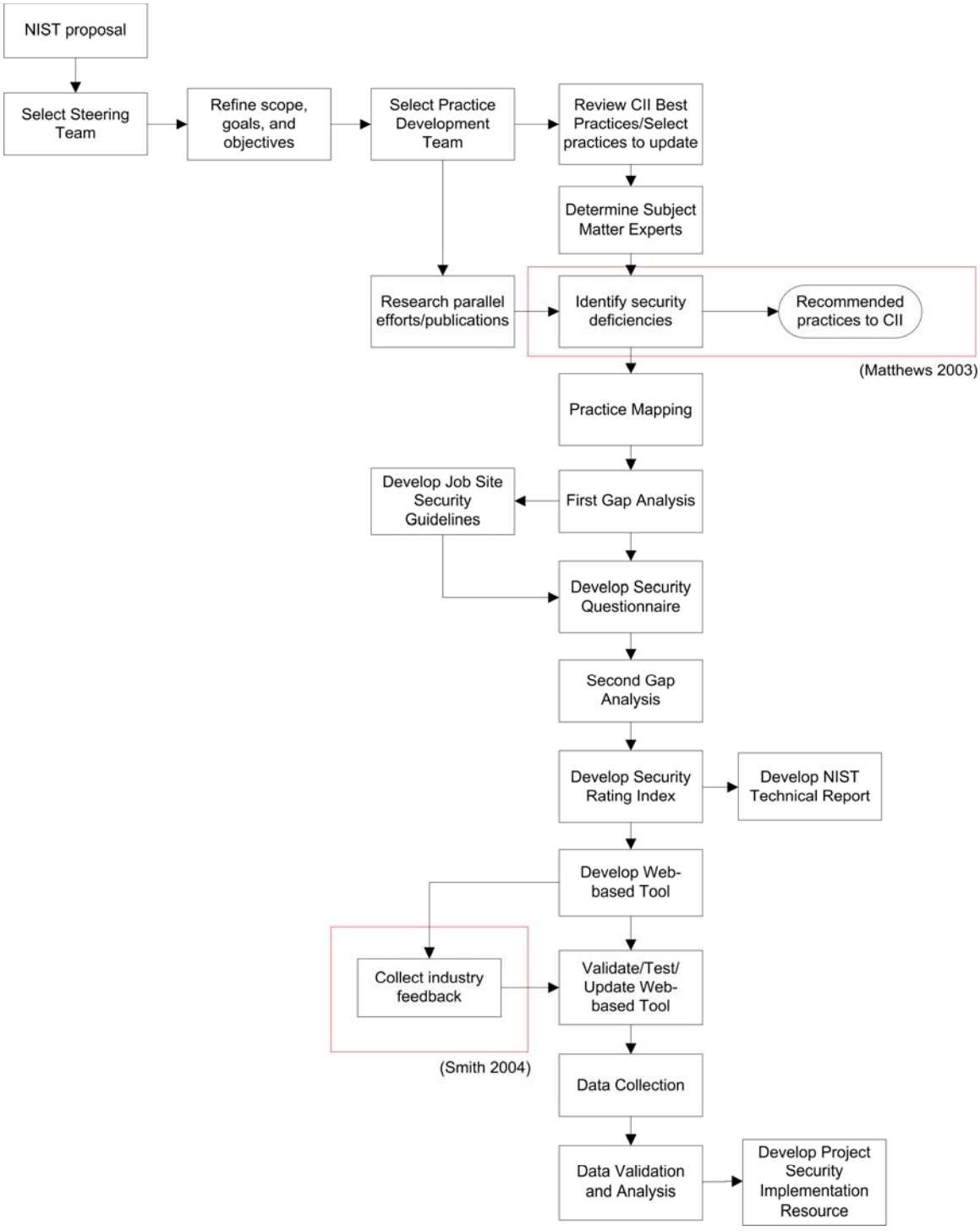


Figure 3.1. Research Methodology

This approach would be likely to provide a more comprehensive solution and assist in making the business case to corporate leaders, which would be of key importance in the acceptance and use of security practices. With this in mind, the Steering Team recommended the establishment of a Practice Development Team, staffed by particular practice and subject matter experts who would be responsible for reviewing CII's existing Best Practices and Proposed Best Practices with the goal of integrating security into them. The Steering Team remained active throughout the study by providing continued guidance to the Practice Development Team and by reviewing the latter team's outputs.

3.2. THE PRACTICE DEVELOPMENT TEAM

The Practice Development Team was charged with reviewing all of CII's existing and Proposed Best Practices, selecting those appropriate for security integration, prioritizing the selected practices, and integrating security. The primary reference documents for the review process were: *A Guide to the CII Implementation Model and Knowledge Structure* (Construction Industry Institute 2001) and *CII Best Practices Guide for Improving Project Performance* (Construction Industry Institute 2002). These documents provide descriptions of each Best Practice, a listing of the essential elements, a summary of the benefits of using the Best Practice, and a checklist for evaluating the degree of implementation. For the review of the Proposed Best Practices, the team relied upon the implementation documentation produced by the CII research team that conducted the original research.

Composition of the Practice Development Team was dynamic. A significant amount of time was spent on deciding what functional positions should be on the team. Business processes, not security, determined selection of the positions so that the practices that were developed would be more likely to be implemented. The team included security representatives from both owner and contractor organizations in order

to consider their differing perspectives of the project delivery process. Core team members from CII member organizations were selected for their functional expertise managing programs, corporate security, business units, plant operations, and risk. Once the core team selected the practices, subject matter experts were identified. The subject matter experts would meet with the core team as necessary to review their practices. The role of the subject matter experts, academics who were responsible for researching and developing the practice, was to provide a thorough review of the selected practice, to answer any questions that the industry representatives might have had about it, and to help identify security deficiencies. The functions and the company affiliations of the Practice Development Team are listed in Appendix A.

3.3. REVIEW AND SELECTION OF BEST PRACTICES

Twenty-six practices, eleven Best Practices and fifteen Proposed Best Practices, were reviewed and discussed to arrive at consensus on the potential impact and applicability that each might have for security. Best Practices have been shown through CII research to provide quantifiable benefits when implemented (Construction Industry Institute 2002). Proposed Best Practices have been thoroughly researched, however, they have not completed the validation process (Construction Industry Institute 2002). Impact was framed by a consequence concept: "If security were omitted from this practice, could its omission result in adverse consequences if the facility were attacked?" (Construction Industry Institute 2004a). Applicability was determined after reviewing each of the practice elements included in the *Best Practices* guide and discussing whether the consideration of security was appropriate to the practice. Each practice was rated separately for high or low impact, and high or low applicability.

The practices measuring high on both impact and applicability were selected for a detailed review to determine how security should be integrated into them. Figures 3.2

and 3.3 show the results of the selection and prioritization process. Five validated Best Practices: (1) pre-project planning, (2) alignment, (3) constructability, (4) design effectiveness, and (5) materials management, along with one Proposed Best Practice, planning for startup, were determined to be high both in impact and applicability. Planning for startup later became a CII Best Practice.

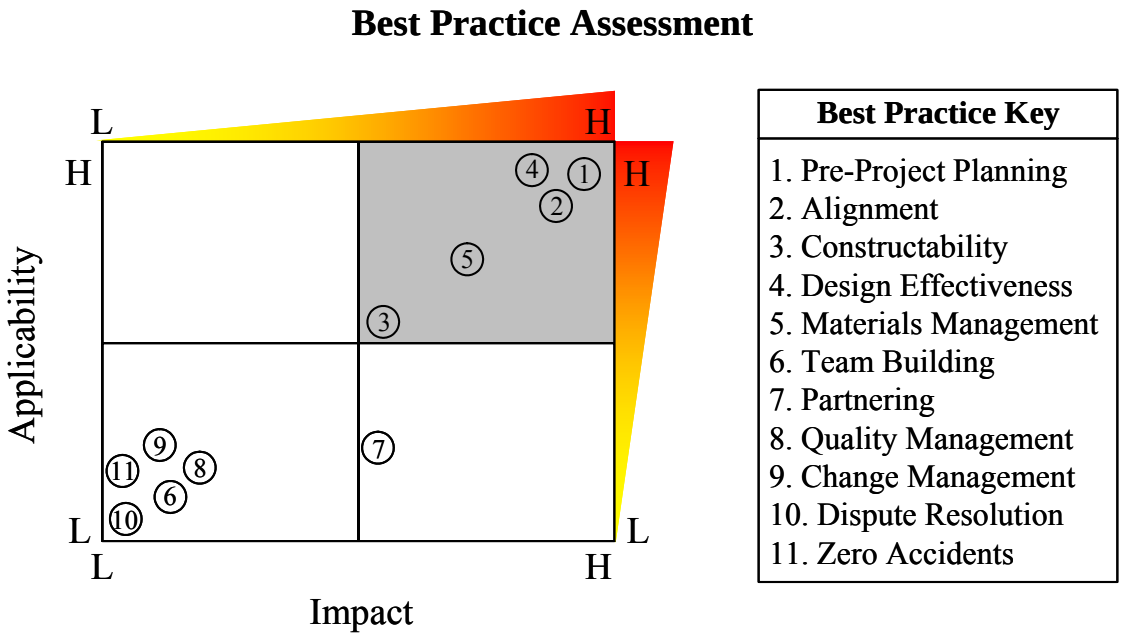


Figure 3.2. Selection and Prioritization of Existing CII Best Practices

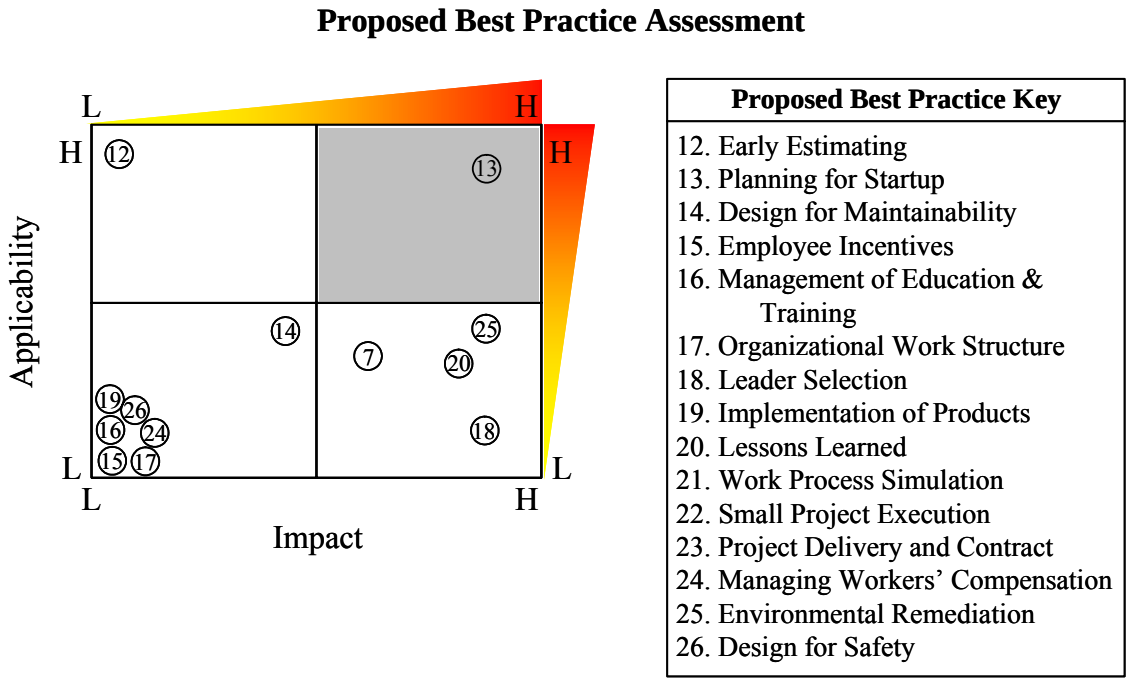


Figure 3.3. Selection and Prioritization of Proposed CII Best Practices

3.3.2. In-depth Review of the Practices

Once the practices were identified, the Practice Development Team held two meetings per practice. At the first meeting, subject matter experts presented the practice and facilitated discussion to identify in-depth, security-specific additions. The subject matter experts, representatives of the academic community, were members of the research teams that initially researched and documented the practice for CII. During this daylong meeting, a page-by-page walk-through of the documentation was conducted to discuss tools and flow processes. Together the subject matter expert and the Practice Development Team identified additional activities or processes that were needed to integrate security into a given practice. Matthews details the process of incorporating

security updates into the Best Practices in *Addressing Security Concerns in the Early Stages of the Project Lifecycle* (Matthews 2003).

The first half of the second meeting was devoted to a review of all changes from the previous meeting in order to close any gaps and to achieve consensus. During the second half of the meeting subject matter experts presented the next practice for review.

3.4. PRACTICE MAPPING

After all of the CII Best Practices had been reviewed and security integrated, the Practice Development Team began practice mapping. The intent was to organize the practices incorporating security components in a logical manner, facilitating the development of the security questionnaire.

In order to map the practices, the team members reviewed each of the security practices by project phase. Since phases within the project execution process typically overlap, organizing by phase assisted the team in identifying those practices to be addressed in multiple phases.

Five phases were used to organize the practices: (1) front-end planning, (2) detailed design, (3) procurement, (4) construction, and (5) startup. As practices were mapped to phases, the team also assessed whether the practices were applicable to physical, personnel, or information security elements. It was found that practices could address multiple elements, with some being applicable to all three.

Mapping practices by project phase and security element permitted the team to chronologically walk through the project execution process and perform gap analysis.

During the first gap analysis (Section 3.5.), the team identified and addressed the lack of security practices documented during the construction phase.

The number of practices mapped in a phase does not indicate whether one phase contributes to security more than another phase, or that one security element is more

influential to project security than another. The practice mapping enabled the team to develop the security questionnaire; the weighting process (Section 3.8.1), following the questionnaire development (Section 3.6), was used to develop relative importance of the respective practices and elements. Appendix B provides the results of the practice mapping exercise.

3.5. FIRST GAP ANALYSIS

Practice mapping served to organize and consolidate security practices, but it also permitted the team to perform gap analysis and identify phases and security elements that had not been well-addressed. It became evident from this analysis that construction site security had been inadequately addressed in the security practices identified. As stolen heavy equipment, tool theft, and jobsite security are major construction industry concerns (National Equipment Register 2004; The Construction Specialist 2005), a subset of the PDT was selected to develop construction site security guidelines.

The team consisted of two security specialists – one representing an owner and one representing a contractor, the principal investigator, and an analyst (National Institute of Standards and Technology 2004a). The team convened a special workshop and the Construction Site Security Guidelines were drafted. The guidelines were reviewed and approved by the Practice Development Team. The author later expanded the Construction Site Security Guidelines based on current security management publications. The revised guidelines are included in Appendix C.

The Construction Site Security Guidelines are intended as a checklist to help owner and contractor organizations incorporate security measures based on assessments of risk. Depending on the type of project and the potential risks that might be faced, certain elements may be more important than others. The guidelines are not an all-inclusive list of security measures, and owner and contractor organizations may find it

necessary to consider other measures as appropriate to the project (Construction Industry Institute 2004a).

3.6. QUESTIONNAIRE DEVELOPMENT

Two important steps necessary to the development of a security assessment tool were completed: (1) identification of specific security practices, and (2) mapping of these security practices by project phase and security element. The next step undertaken was the further consolidation of practices and the construction of a questionnaire for assessing the level of integration of security into project processes.

In an effort to minimize respondent burden while still maximizing information gathering capability, a team consisting of the Principal Investigator, an analyst, and the author further consolidated the practices. The first step was to collapse them into logical groupings. Practices that were related or that were components of a process were combined. An example of this is the grouping of Civil/Structural Requirements, Architectural Requirements, Water Treatment Requirements, and Loading/Unloading/Storage Facilities Requirements from the Front-end Planning phase into the Preparation of Specifications and Requirements group (Construction Industry Institute 2004a).

Collapsing the practices was an iterative process. The team reviewed every practice on the Practice Map for logical groupings. Once the first iteration was complete, the team reviewed the logical groupings to determine whether some of the groups could be consolidated into another group. After numerous rounds of collapsing security practices into logical groupings, the team was able to formulate questions that addressed multiple security requirements with only thirty-three questions. Because of the consolidation process, it is possible to categorize the thirty-three questions by project phase, security element, relevant CII publication, and a logical category. These categories

included: objectives, planning, requirements and specifications, personnel, information, site information, and site security.

The thirty-three questions were then formatted as shown in Table 3.1. The format for each of the questions was, "Security was a consideration in …" followed by an activity appropriate for security integration. The response option was a Likert-type, 5-point scale response category, ranging from strongly disagree to strongly agree (Section 4.1.2). Based on experience from CII's ongoing benchmarking program, the Practice Development Team felt that by structuring the questions in this manner, respondent burden would be kept to a minimum and quality of the data could be maximized (Construction Industry Institute 2004a). Appendix D contains the complete security questionnaire.

Table 3.1. Security Best Practices

#	Activity in which security should be considered:	Phase					Security Element		
		FEP	D	P	CON	SU	Phy	Per	Info
1	Establishing project objectives (e.g., reliability and operating philosophy, affordability and feasibility, constructability, future expansion, etc.)	X					X		
2	Preparation of the specifications and requirements (e.g., civil/structural, architectural, water treatment, loading/unloading/storage facilities, substation/power sources, instrument & electrical, etc.)	X	X				X		X
3	Developing and evaluating design criteria (based on vulnerability assessment)	X	X				X		
4	Developing project scope	X					X		
5	Design and material selection		X	X			X		
6	Developing the engineering/construction plan & approach	X	X	X	X		X		
7	Developing the procurement/materials management procedures and plans (e.g., warehousing, inventory control, key & lock control, hazardous materials)	X	X	X			X	X	X
8	Prequalification/selection of suppliers	X	X	X				X	
9	Developing the pre-comm/turnover sequence/startup requirements/objectives	X	X				X	X	X
10	Technology and process selection	X	X				X		
11	Determining required site characteristics and location	X					X		
12	Preparing the permitting plan	X					X	X	
13	Developing the plot plan (i.e., layout, accessibility, gate configuration, etc.) - retrofit & greenfield	X	X				X	X	X
14	Evaluation of various personnel issues (e.g., education/training, safety and health considerations)	X					X		
15	Development of a distribution matrix for document control (e.g., drawings, project correspondence, CAD, as-built documents)	X	X					X	
16	The project team was in alignment concerning the importance of security issues identified in the project objectives.	X	X		X	X	X	X	X
17	Security-related equipment was defined and purchased with appropriate input (e.g., O&M, Security Manager, etc.)		X	X			X	X	X
18	Identifying stakeholders for the project team (based on vulnerability assessment)	X					X	X	X

#	Activity in which security should be considered:	Phase					Security Element		
		FEP	D	P	CON	SU	Phy	Per	Info
19	Establishing priorities between cost, schedule, and required project features (based on vulnerability assessment)	X	X				X	X	X
20	Identifying and resourcing startup requirements (e.g., procurement, personnel, training)	X					X	X	X
21	Screening of the project team for appropriate level of clearance	X						X	
22	Screening of contractor/subcontractor employees/delivery personnel for appropriate level of clearance	X	X	X	X	X		X	
23	Identifying startup risks	X	X	X	X		X	X	X
24	Developing/implementing startup security plan	X	X	X	X		X	X	X
25	Developing system startup plan (reconciled with security plan)	X	X				X	X	X
26	Developing training plans (e.g., job site, O&M, startup)	X	X	X	X	X	X	X	X
27	Assessing & communicating effects from change orders				X	X	X	X	X
28	Developing/implementing construction site security plan (e.g., fire protection and safety considerations, egress, emergency responder access, process shutdown)				X	X	X	X	X
29	The project had a designated site security coordinator				X	X	X	X	X
30	Developing business partnerships/alliances	X	X	X	X	X	X	X	X
31	Project information systems security plan (e.g., firewalls, wireless security, passwords, access controls)		X	X	X	X			X
32	Security breaches/incidents were routinely investigated				X	X			
33	Developing emergency response plan in coordination with local authorities				X	X			

An examination of Appendix D, Security Questionnaire and Appendix B, Results of Practice Mapping reveals the degree of consolidation required to keep the questionnaire manageable and also illustrates the linkage between the CII Best Practices and the final questions. For example the first question in Appendix D, "Security was a consideration in establishing project objectives, (e.g., reliability and operating philosophy, affordability and feasibility, constructability, future expansion, etc.)," incorporates elements from the

CII Best Practices of Pre-Project Planning (PDRI) IR113-2, Alignment During Pre-Project Planning IR113-3, Constructability Publication 34-1, and Materials Management IR 7-3 (Construction Industry Institute 2004a). The Phase and Source Key included with the practice mapping results in Appendix B can be used to trace linkages for all of the questions in Appendix D.

3.7. SECOND GAP ANALYSIS

Following the consolidation of security practices into the thirty-three questions and questionnaire formatting, the Practice Development Team decided to perform another gap analysis to reexamine the coverage of security issues for each project phase and security element. While discussing approaches for the gap analysis, it became apparent that the team members' responses to the questions and perceptions of gaps were strongly influenced by their views of risk. The team developed a consensus risk profile, which would be used in the second gap analysis. Each team member was asked to consider two types of projects, new construction (greenfield or grassroots) and renovation (retrofit, additions and modernizations), and to list in priority order the major risks confronting heavy industrial projects during each phase of the project. The author then consolidated team member risk profiles into a consensus risk profile in rank order, from highest risk to lowest risk. As risks identified varied considerably among team members, the consolidated profile was a useful tool in reviewing the questionnaire for completeness. The consolidated risk profiles are shown in Appendix E.

It is worth noting that the team felt that information disclosure/compromise was a risk in all phases of construction. This perspective was significant during the question weighting process (Section 4.1).

Following the development of the consolidated risk profile, the team analyzed the thirty-three questionnaire items to determine whether all of the risks identified were

addressed in the questionnaire. With minor additions to some of the thirty-three questions, the team concluded that the risks were adequately covered by the questions.

3.8. THE SECURITY RATING INDEX

An objective of this research was to develop a means of quantitatively assessing the level of implementation of security practices for a project. The Security Rating Index (SRI) provides this means. The SRI score, in conjunction with Threat Level and Consequence Level ratings (Section 4.3) enables comparison of security practice implementation among projects with similar conditions. Chapter 4 details the development and application of the Security Rating Index.

3.9. IMPLEMENTING PROJECT SECURITY PRACTICES

A guide to implementing project security practices was written by the author to facilitate the adoption of the security best practices by industry. While it does not provide specific guidance for the implementation of security procedures at the project level, it offers a framework for integrating security into the project delivery process in the context of likely threats facing the facility and consequences of security breaches.

The implementation procedure consists of a nine-step process of integrating security into the project delivery process. Implementing project security practices is detailed in Chapter 8.

Chapter 4. Development of the Security Rating Index

The Security Rating Index (SRI) provides a means of quantitatively assessing the level of implementation of security practices for a project. This chapter details the development, application, and interpretation of the SRI.

4.1 ESTABLISHING WEIGHTS

Upon completion of the questionnaire, the Practice Development Team discussed the issue of weighting the questions. The team concluded that while all questions were important for assessing project security, not all factors related to the questions contributed equally to this assessment. Since security features that are incorporated early in the project delivery process often have more impact, and are more cost-effective, than those incorporated later in the project (Construction Industry Institute 2004a), the Practice Development Team felt that it was appropriate to weight the project phases. The team also felt that the importance of the security elements varied by phases, as did the individual questions within each element. Weights were therefore developed for security elements within each project phase and for individual questions within each element. For example, to illustrate the importance of practices by project phase, developing a system startup plan was less important to the longer term security of the facility than preparation of specifications and requirements during front-end planning (Construction Industry Institute 2004a).

4.1.1. The Analytic Hierarchy Process

Weights were established using the analytic hierarchy process (AHP) (ASTM International 2002; Saaty 1980; Saaty 1990) and Expert Choice® software (Expert Choice Inc. 2003). AHP is a decision analysis method that considers non-monetary

attributes, both qualitative and quantitative, when evaluating project alternatives. It uses pairwise comparisons to rate the relative importance of alternative elements in a hierarchy. AHP relies upon expert opinions to establish relative importance; the Practice Development Team served as the experts. The author guided the PDT through the AHP comparisons.

Three pairwise comparison matrices were developed. First, weights were established for each project phase from front-end planning through startup using the verbal scale shown in Table 4.1.

Table 4.1. Verbal Scale for the Analytic Hierarchy Process

Verbal Scale	Numerical Scale
Equal importance of one item to the other	1
Moderate importance of one item over the other	3
Strong importance of one item over the other	5
Very strong importance of one item over the other	7
Extremely strong importance of one item over the other	9

Experience led the team to conclude that in most cases security implementation performed earlier in the project was far more likely to favorably impact outcomes, including security, than if performed later in the project delivery cycle. This resulted in higher phase weights assigned to earlier project phases. Next the team weighted the security elements comparing physical, personnel, and information security. The team decided that the relative importance of the elements was phase dependent; therefore, the

weighting process for elements was conducted for each project phase. As a final step the team weighted each of the questionnaire items within each phase. This was an onerous process; however, the Expert Choice® software provided the means to effectively accomplish this. The software also provided an assessment of consistency throughout the decision making process. Appendix F shows the results of the weighting exercise. Note that the sum of the weights assigned to each phase is 1.0, and the sum of the weights for the security elements within each phase also sums to 1.0.

The output, an aggregate of each of the weighting exercises, yielded some surprising results. Once the initial weighting was complete, some questionnaire items, like identifying stakeholders for the project team, were not as relatively important as the Practice Development Team first hypothesized.

Further analysis showed that the framework for weighting physical, personnel, and information security elements incorporated the typical security bias towards physical security, at the expense of information and personnel security elements. Physical security was originally rated as having more importance during the front-end planning phase, but the major risks are more likely to be personnel and information security during this phase since no actual facility exists, at least for greenfield projects. This viewpoint is supported by the consolidated risk profile discussed in Section 3.7.

While the physical security elements of the proposed facility are being addressed during the early phases, the *risks* to the project are mostly due to inadequate team selection or compromise of sensitive information; this can severely impact security later in the project life cycle. Information is considered an economic resource on par with human resources, equipment, materials, and capital (Fay 2002). Because of the security element weights were not representative of the aforementioned considerations, the team re-weighted the three security elements to better address risk during the phases, yielding

the final weights. The final output showed a relative distribution of importance that was more congruent with team member expectations (National Institute of Standards and Technology 2004a). Even though the number of questions related to physical security is greater than the number containing information and personnel security, the highest weighted questions contain information and personnel security elements. This is consistent with the team members' expectations as well as current security management principles. Appendix G shows the final AHP output.

4.1.2. Likert-Type Scales

The Likert-type scale used in this research is modeled after a pattern devised by Rensis Likert to study social attitudes. The scale asks respondents to answer a question in terms of several degrees of agreement or disagreement; each response is then scored so that a response indicative of the most favorable attitude is given the highest score (Selltiz and Kidder 1981).

The typical usage of a Likert-type scale is to add the response scores to develop a total score and then assess if a correlation exists between an individual response and the attitude being measured (Selltiz and Kidder 1981).

The scale used in the SRI questionnaire is not a true Likert-type scale. Its intent is not to measure social attitudes, but as a tool to convert subjective qualitative responses into a quantitative measurement of the level of security best practice implementation.

The Likert-type scale score is used to determine the level of implementation of the security best practice addressed by a particular response. Possible question responses are: (1) strongly disagree, (2) disagree, (3) neutral, (4) agree, (5) strongly agree, and (6) not applicable/unknown.

Values associated with each response are shown below (Table 4.2).

Table 4.2. Likert-type Response Values

Response	Value
Strongly Disagree	0.00
Disagree	0.25
Neutral	0.50
Agree	0.75
Strongly Agree	1.00
NA/Unknown	*

* omitted from calculation

The values indicate a percentage of implementation of a security best practice, with 0 representing no implementation, and 1 representing full implementation. For example, if the respondent selects "Agree" for the item, "Security was a consideration in establishing project objectives," he or she is implementing 75% of that best practice.

An assumption in this methodology is that the level of implementation is equal between the response terms, i.e., the interval between "strongly agree" and "agree" is the same as the interval between "disagree" and "strongly disagree". The intent of the Likert-type scale is not to weight the responses, as each security consideration already has an associated weight, but to establish a reference point along a continuum of implementation.

4.2. THE SCORING ALGORITHM

A scoring algorithm for the SRI was developed by the author to assess use of the security best practices on a scale of 0 to 10, with 0 indicating no use of the practices and 10 indicating full use of the practices.

The SRI score is computed with two algorithms. The first algorithm calculates SRI scores for each of the five project phases; the second algorithm calculates the Project SRI based upon the Phase SRI scores. In order to calculate the Project SRI score, a minimum of three phase scores are required for owners and a minimum of two phase scores are required for contractors.

4.2.1. Phase Scoring Algorithm

The Phase SRI algorithm (Figure 4.1) is used to calculate an SRI score for an individual project phase.

$$P = \left[\frac{\sum_{i=1}^{n} (w_i v_i)}{\sum_{i=1}^{n} w_i} \right] \times 10$$

Where:

P is the project's Phase SRI score;
n is the total number of questions within a phase;
w_i is the question weight (Section 4.1);
v_i is the value of the Likert-type response (Table 4.2); questions answered NA/UNK are omitted from the calculation

Figure 4.1. Phase SRI Algorithm

4.2.2. Project Scoring Algorithm

The Project SRI algorithm (Figure 4.2) is used to calculate an SRI score for an entire project, based upon its Phase SRI scores.

$$S = \frac{\sum_{i=1}^{n} (W_i P_i)}{\sum_{i=1}^{n} W_i}$$

Where:

S is the project's SRI score;
n is the total number of phases within a project;
W_i is the phase weight;
P_i is the Phase SRI score; phases not submitted are omitted from the calculation

Figure 4.2. Project SRI Algorithm

4.2.3. Scoring Example

The following example details the calculation of a Phase SRI score based upon answers to the SRI questionnaire. A Project SRI score is then calculated using the multiple Phase SRI scores.

Table 4.3 lists construction phase questions, the question weights derived using AHP (Section 4.1.1), hypothetical Likert-type responses, and the Likert-type response values (Table 4.2).

Table 4.3. Construction Phase Scoring Example

Security was a consideration in:	Question Weight	Likert-type Response						Likert-type Response Value
		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	NA/UNK	
Developing the engineering/construction plan & approach	0.145					X		1.00
The project team was in alignment concerning the importance of security issues identified in the project objectives	0.024		X					0.25
Screening of contractor/subcontractor employees/delivery personnel for appropriate level of clearance	0.058					X		1.00
Developing training plans (e.g., job site, O&M, startup)	0.024	X						0.00
Assessing & communicating effects from change orders	0.056						X	NA
Developing/implementing construction site security plan (e.g., fire protection and safety considerations, egress, emergency responder access, process shutdown)	0.327				X			0.75
The project had a designated site security coordinator	0.084						X	NA
Developing business partnerships/alliances	0.008		X					0.25
Project information systems security plan (e.g. firewalls, wireless security, passwords, access controls)	0.021			X				0.50
Security breaches/incidents were routinely investigated	0.097				X			0.75
Developing emergency response plan in coordination with local authorities	0.106					X		1.00
Identifying startup risks	0.030			X				0.50
Developing/implementing startup security plan	0.020				X			0.75

Using the Phase Scoring Algorithm (Figure 4.1), the construction Phase SRI score would be calculated as shown in Figures 4.3 to 4.5. Because of space constraints, calculation of the Phase SRI is shown in three steps. Calculation of the first eight questions is depicted in Figure 4.3. Figure 4.4 details the calculation of the remaining

five questions. Questions marked "NA/UNK" are omitted from the calculation as indicated in Figure 4.2. The Phase SRI score is calculated in Figure 4.5.

$$P_1 = \frac{[(0.145)(1)+(0.024)(0.25)+(0.058)(1)+(0.024)(0)+(0.327)(0.75)+(0.008)(0.25)]}{(0.145+0.024+0.058+0.024+0.327+0.008+0.021+0.097+0.106+0.030+0.02)} = 0.528$$

Figure 4.3. Construction Phase SRI Example Part I

$$P_2 = \frac{[(0.021)(0.50)+(0.097)(0.75)+(0.106)(1)+(0.030)(0.50)+(0.02)(0.75)]}{(0.145+0.024+0.058+0.024+0.327+0.008+0.021+0.097+0.106+0.030+0.02)} = 0.257$$

Figure 4.4. Construction Phase SRI Example Part II

$$P = (P_1 + P_2)\times 10 = (0.528 + 0.257)\times 10 = 7.85$$

Figure 4.5. Construction Example Phase SRI Score

The Project SRI for the example will be calculated based upon the Phase SRI scores shown in Table 4.4.

Table 4.4. Example Phase SRI Scores

Phase	Phase Weight	Phase Score
Front-end Planning	0.536	7.31
Design	0.227	8.56
Procurement	0.068	6.59
Construction	0.136	7.85
Startup	0.033	5.27

The Project SRI calculation is shown in Figure 4.6.

$$S = \frac{\left[(0.536)(7.31) + (0.227)(8.56) + (0.068)(6.59) + (0.136)(7.85) + (0.033)(5.27)\right]}{(0.536 + 0.227 + 0.068 + 0.136 + 0.033)} = 7.55$$

Figure 4.6. Construction Example Phase SRI Score

4.3. INTERPRETATION AND USE OF THE SECURITY RATING INDEX

An SRI score may be calculated for a project by completing the security questionnaire and using the scoring algorithms; this, however, is not sufficient to interpret the SRI. Depending on factors such as site location, industrial processes, or environmental effects, some projects may require higher levels of security integration than other similar projects. As an example, a chemical processing facility located in an area where there is no surrounding residential development and minor potential for adverse environmental impacts may require less security integration than one sited close to a densely populated area (Construction Industry Institute 2004a). In order to interpret the SRI correctly, it must be viewed in the context of threats and consequences of potential security breaches.

4.3.1. Threats and Consequences

The Practice Development Team used the Security Vulnerability Assessment (SVA) methodology, developed by the American Petroleum Institute and National Petrochemical & Refiners Association (API/NPRA) (American Petroleum Institute and National Petrochemical & Refiners Association 2004), for guidance on the issue of threats and consequences. An "SVA is the process of determining the likelihood of an adversary successfully exploiting vulnerability, and the resulting degree of damage or impact on an asset" (Center for Chemical Process Safety of the American Institute of Chemical Engineers 2002). Instead of being a quantitative analysis, an SVA is a qualitative risk analysis similar to the qualitative risk analysis used in assessing the risk of accidental damage and injury exposure at a facility.

An SVA also employs the concepts of *threats* and *consequences* to assess security vulnerability. A threat is defined as any indication, circumstance, or event with the potential to cause loss of, or damage to, an asset (Center for Chemical Process Safety of the American Institute of Chemical Engineers 2002). It also includes the intention and capability of an adversary to undertake actions that would be detrimental to valued assets. Adversaries might include: terrorists, either domestic or international; activist or pressure groups; criminals (e.g., white-collar, cyber hackers, organized, opportunists) (National Institute of Standards and Technology 2004a). Sources of threats may include: insider, external, and insiders working as colluders with external sources.

Implicit in the threat concept is likelihood of the event occurring. As the threat increases, the likelihood of the security incident increases, as well. Threat ratings range from 1, very low, to 5, very high. Very high indicates that a definite risk exists and that the adversary has both the intent and capability to breach security possibly resulting in the consequences listed in Table 3.5. It also indicates that the facility, or similar assets, is

targeted on a recurring basis. Very low, on the other hand, suggests no credible evidence of intent or capability, and no history of actual or planned threats against a facility or similar assets.

Using the API/NPRA guidelines as a model, the Practice Development Team developed the threat and consequence rating criteria shown in Tables 4.5 and 4.6. The team expanded upon the API/NPRA ratings to apply to all industrial projects, rather than petrochemical-related projects, and to all phases of the project delivery cycle, rather than the operational phase (Construction Industry Institute 2004a).

Table 4.5. Threat Level

Score	Level	Description
5	Very High	Indicates that a **definite threat** exists against the asset and that the adversary has both the capability and intent to launch an attack or commit a criminal act, *and* that the subject or similar assets are targeted on a frequently recurring basis.
4	High	Indicates that a **credible threat** exists against the asset based on knowledge of the adversary's capability *and* intent to attack or commit a criminal act against the asset, based on related incidents having taken place at similar assets or in similar situations.
3	Medium	Indicates that there is a **possible threat** to the asset based on the adversary's desire to compromise similar assets *and/or* the possibility that the adversary could obtain the capability through a third party who has demonstrated the capability in related incidents.
2	Low	Indicates that there is a **low threat** against the asset or similar assets and that few known adversaries would pose a threat to the asset
1	Very Low	Indicates **no credible evidence** of capability or intent and no history of actual *or* planned threats against the asset or similar assets.

Adapted from API/NPRA (2004)

Threat is not static throughout the project delivery cycle and is linked to consequences of a security breach. As the external environment or indicators (e.g., Homeland Security Advisory System level) change, the threat to the project may change as well.

In addition to threats, the worst-case consequences of security breaches must be evaluated. Consequences are defined as the amount or damage that may be expected from a successful attack against an asset (Center for Chemical Process Safety of the American Institute of Chemical Engineers 2002). Examples of consequences include: injuries to the public or to workers; environmental damage; direct and indirect financial losses to the company, to suppliers, and/or associated businesses; disruption to the national, regional, or local operations or economy; loss of reputation or business viability; evacuation of people living or working near the facility; excessive media exposure and related public hysteria affecting people that may be far removed from the actual event location (National Institute of Standards and Technology 2004a).

Similar to threat, consequence is scored on a 1 to 5 scale with 1 indicating very minor consequences and 5 indicating very severe consequences. Specific criteria for assessment of each level of consequence are provided in Table 4.6.

Table 4.6. Consequence Level

Score	Level	Description
5	Very High	Possibility of any offsite fatalities; possibility for multiple onsite fatalities Extensive environmental impact onsite and/or offsite Extensive property damage Very long-term business interruption/expense
4	High	Possibility of any offsite injuries; possibility for onsite fatalities Significant environmental impact onsite and/or offsite Significant property damage Long-term business interruption/expense
3	Medium	No offsite injuries; possibility for widespread onsite injuries Moderate environmental impact onsite and/or offsite Moderate property damage Medium-term business interruption/expense
2	Low	Possibility for onsite injuries Minor environmental impact onsite only Minor property damage Short-term business interruption/expense
1	Very Low	Possibility for minor onsite injuries No environmental impacts Little/No property damage Little/No business interruption/expense

Adapted from: API/NPRA (2004)

Note that consequence is defined as the worst-case result of a security breach *over the facility life cycle*. The reason for this distinction is that it is neither practical nor economical to redesign a facility to ameliorate consequences as they change over the life cycle. For instance, during the construction phase of an oil refinery, no feedstock is on site, so the potential for offsite injuries as a result of a breach is low. Once the facility is commissioned, however, feedstock and highly combustible products are onsite, greatly increasing the potential for offsite injuries, fatalities, or environmental damage. The

consequence changes significantly, but this is not an unexpected event, since it is known in the front-end planning phase. The project team certainly would not change the design because the consequence escalates throughout the life cycle; the design would address the operational consequence before the facility is constructed. Exceptions to consequence remaining the same would be for unforecasted reasons, for example, if the product or process changes or if the potential for offsite effects changes, perhaps due to demographic change (Construction Industry Institute 2004a).

4.4. THE SECURITY-INFLUENCE CURVE

The number of questions used to produce the SRI by project phase is shown in Figure 4.7.

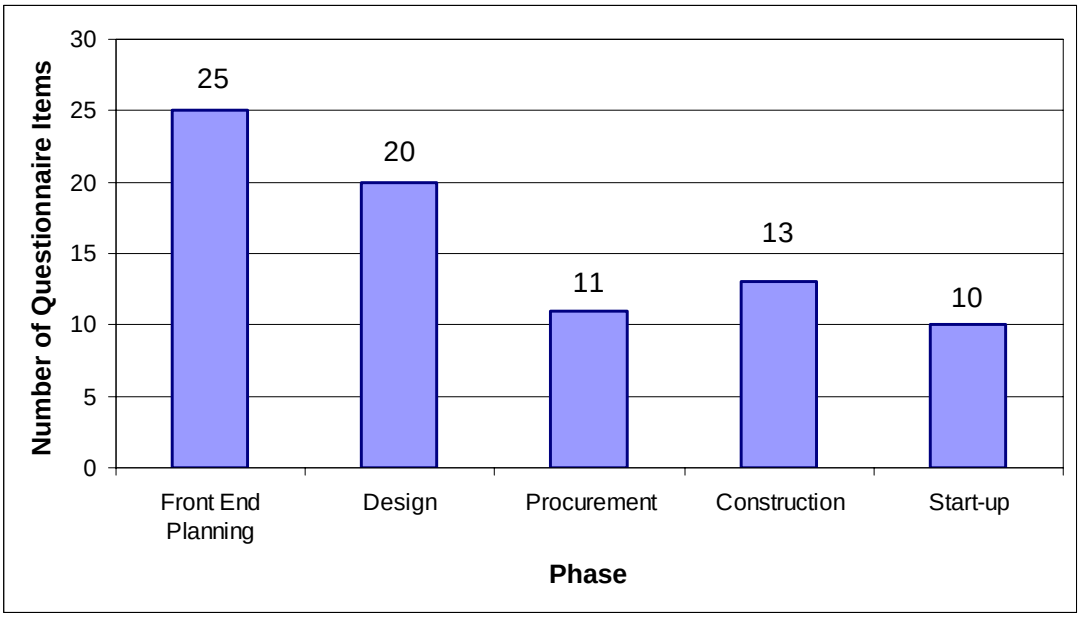


Figure 4.7. Security-Related Questions by Project Phase

While the number of unique questions is thirty-three, some are applicable to more than one phase, and are therefore repeated, resulting in seventy-nine total questions.

Including recurring questions, nearly 32% (twenty-five of seventy-nine questions) address front-end planning, and slightly over 25% (twenty of seventy-nine questions) address design (Construction Industry Institute 2004a). More than 60% of the activities relating to security occur before construction begins. This was an observation apparent to the Practice Development Team, although security activities were not intentionally front-loaded.

Since the weights assigned to security activities in the front-end planning and design phases (Appendix F) were greater than those assigned to activities in later phases, the relative importance of the activities is even greater than would be indicated by Figure 4.7 when project cost is considered.

CII has long postulated a relationship between the ability to influence project cost as the project proceeds from planning through execution (Construction Industry Institute 2004a). This relationship, known within CII as the Cost-Influence curve, suggests that the ability to influence project cost decreases rapidly when the execution phases of procurement and construction commence (Construction Industry Institute 1995). Similarly, there exists a security-influence relationship as shown in Figure 4.8. The curve indicating ability to influence security is fitted to the weights of the questions occurring in each phase of the project from front-end planning through startup.

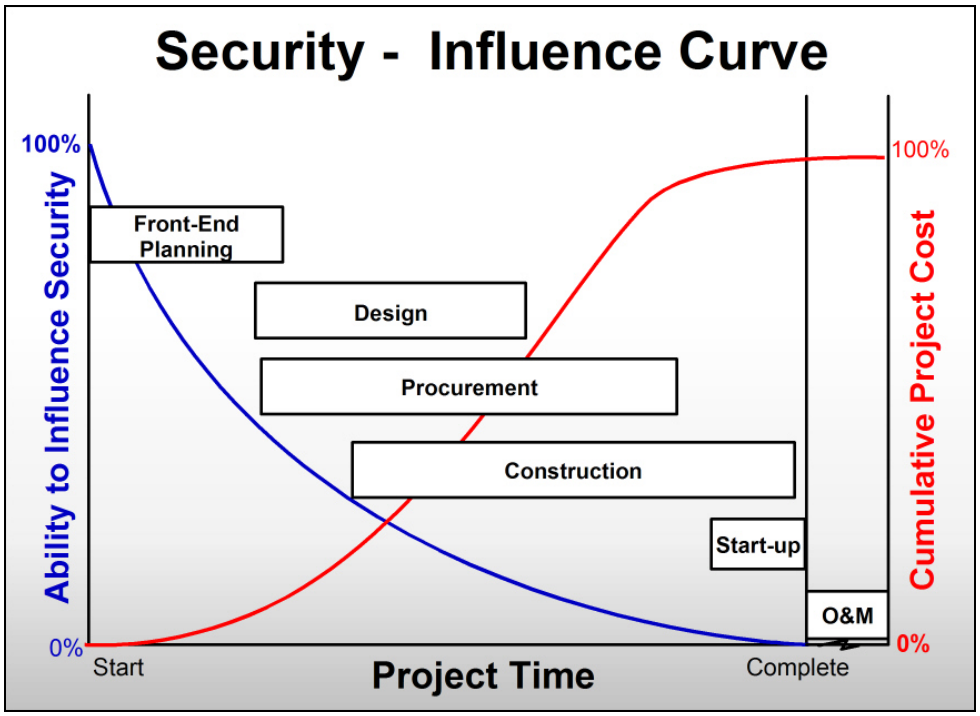


Figure 4.8. Security-Influence Curve

Facility security, like many other facility attributes, can be enhanced most cost-effectively when addressed early in the planning and design phases of a project. While this assertion may seem obvious, this research identified specific activities during project delivery that can be used to improve facility security and provide a quantitative assessment of the integration of security into established processes.

4.5. DATA COLLECTION

Once the framework of the research was completed, the next step was to collect data in order to establish the relationship between Threat Level, Consequence Level, and SRI, and assess the impact of security implementation on project outcomes such as cost and schedule performance. To fulfill these research objectives, data was collected through the use of a Web-based data collection tool.

4.5.1. Conceptual Model of SRI Use

The Conceptual Model of SRI use provides an example of how the data can be used. As the database is populated, quartiles of security integration can be developed. The quartiles will enable comparisons to be made between an individual project SRI score and scores from similar projects in the database. Quartiles are a means to describe some of the characteristics of a distribution, in this case a distribution of projects. The first quartile is the point below which 75% of all other projects fall. The second quartile represents the point below which 50% of all other projects fall. The third quartile is above the last 25% of the projects, which is represented by the fourth quartile.

Figure 4.9 illustrates a hypothetical project with Threat Level 3 and Consequence Level 3. Its SRI score of slightly less than 6 is in the middle of the distribution for all projects at the same consequence and threat level, i.e., 50% of all similar projects have a higher level of security implementation, and 50% have a lower level of security implementation.

Based upon Threat Level, the hypothesized threat curves for the Conceptual Model of SRI may vary. For example, the slope of the curve for Threat Level 1 is expected to be linear and somewhat flat (slope ~ 0), as SRI score would probably not vary much as the Consequence Level increases for a very low level threat. Conversely, the curve for Threat Level 5 may increase exponentially, resulting from high SRI scores for even a low threat. The hypothesized threat curves are expected to be of increasing slope for Threat Levels 2 through 5.

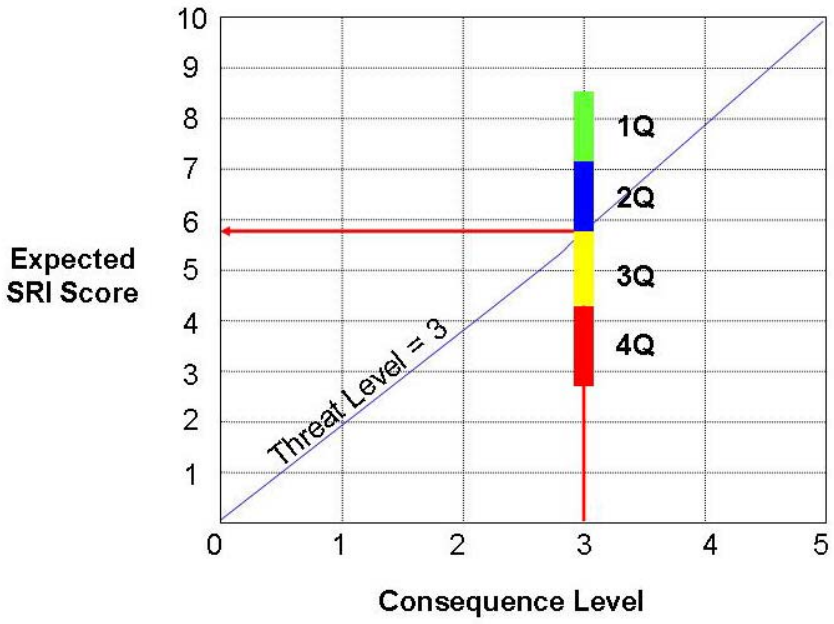


Figure 4.9. Conceptual Model of SRI Use

Corporate management can use this model to determine the level of security implementation they feel is appropriate for their project. For example, one organization may feel that the median SRI, or industry "norm" for the same Threat Level and Consequence Level is sufficient for its project; any SRI score in the second quartile or above would be acceptable. Another organization might prioritize security as the most important characteristic of its project. In that case, the organization may undertake additional measures to improve the SRI score so that it lies within the first quartile.

4.5.2. The Web-based Data Collection Tool

The Web-based data collection tool was programmed by the author between October-December 2003. It used an Internet browser front-end to interface with a database hosted on the CII Benchmarking and Metrics server.

The Web pages were designed with Macromedia Dreamweaver MX and used the Macromedia ColdFusion application to process data and read from and write to a Microsoft Access 2003 database. Screenshots from the Web-based data collection tool can be found in Appendix H.

The data collection tool went live at URL http://www.construction-institute.org/sri in December 2003. Access was initially restricted to CII member companies. In March 2005, non-CII member companies were permitted to enter project data. Based upon feedback from participants in the data collection process (Smith 2004), some usability improvements were made to the tool.

In February 2005, the author began data analysis on the data collected with the Web-based data collection tool.

4.5.3. Project Data

Data collected for each project included general information, project description, project nature, typical project, project delivery system, project complexity, project cost information, project schedule information, and project participant information. The responses to each of the Likert-type scales for phase questions were also collected in the database.

4.5.3.1. General Information

Project general information was required to determine the name and location of the project as well as to collect contact information for the respondent. The general information data collected was:

- Project Name
- Project Location
- Contact Person

- Contact Phone
- Contact Fax
- Contact E-mail
- Respondent Type – owner or contractor
- Owner Type – public agency or private company

4.5.3.2. Project Description

For the project description, the respondent was instructed to describe the project from four given types: (1) buildings, (2) heavy industrial, (3) light industrial and, (4) infrastructure. If the project was a mixture of two or more of the listed types, the respondent was instructed to select the principle type. If the project type did not appear in the list, to respondent was instructed to select "other" under the appropriate industry group and specify the project type. The project types were:

- Buildings – Communications Center, Dormitory/Hotel, Lowrise Office (less than three floors), Highrise Office (greater than three floors), Hospital, Housing, Laboratory, Maintenance Facilities, Parking Garage, Physical Fitness Center, Restaurant/Nightclub, Retail Building, School, Warehouse, Residential, Prison, Movie Theater, Other Buildings
- Heavy Industrial – Chemical Manufacturing, Electrical (Generating), Environmental, Metals Refining/Processing, Mining, Natural Gas Processing, Oil Exploration/Production, Oil Refining, Pulp and Paper, Other Heavy Industrial
- Light Industrial – Automotive Assembly, Consumer Products Manufacturing, Foods, Microelectronics Manufacturing, Office Products Manufacturing, Pharmaceutical Manufacturing, Other Light Industrial

- Infrastructure – Airport, Electrical Distribution, Flood Control, Highway, Marine Facilities, Navigation, Rail, Tunneling, Water/Wastewater, Pipeline, Gas Distribution, Telecom/Wide Area Network, Other Infrastructure

4.5.3.3. Project Nature

Project nature was limited to four choices: (1) Grass Roots, (2) Modernization, (3) Addition, and (4) Other.

Grass roots, or Greenfield, projects occur at previously unimproved sites, i.e., new construction. Modernization refers to upgrading an existing facility or its capital equipment. Addition is the extension of an existing facility or the introduction capital equipment to expand production capacity. If the respondent selected other, a text box was provided to describe the project nature.

4.5.3.4. Typical Project

The respondent was instructed to indicate whether the project was typical or representative of most of the projects his or her company performs. The choices presented were typical or not typical.

4.5.3.5. Project Delivery System

This item required the respondent to select the delivery system used to execute the project. The choices and their descriptions were:

- Traditional Design-Bid-Build – Serial sequence of design and construction phases; owner contracts separately with designer and constructor
- Design-Build (or EPC) – Overlapped sequence of design and construction phase; procurement normally begins during design; owner contracts with Design-Build (or EPC) contractor

- Construction Manager at Risk (CM @ Risk) – Overlapped sequence of design and construction phases; procurement normally begins during design; owner contracts separately with designer and CM @ Risk (constructor)
- Multiple Design-Build – Overlapped sequence of design and construction phases; procurement normally begins during design; owner contracts with two Design-Build (or EPC) contractors, one for process and one for facilities
- Parallel Primes – Overlapped sequence of design and construction phases; procurement normally begins during design. Owner contracts separately with designer and multiple prime constructors

4.5.3.6. Project Complexity

The respondent was instructed to choose a value that best described the level of complexity for the project as compared to other projects from the same industry sector. For example, if the project was a heavy industrial project, the respondent was to indicate how it compared in complexity to other heavy industrial projects. Respondents were presented a scale ranging from 1 to 10, with 1 representing low complexity, 5 representing average complexity, and 10 representing high complexity. The definitions below were furnished as general guidelines:

- Low – characterized by no use of unproven technology, small number of process steps, small facility size or process capacity, previously used facility configuration or geometry, proven construction methods, etc.
- High – characterized by the use of unproven technology, an unusually large number of process steps, large facility size or process capacity, new facility configuration or geometry, new construction methods, etc.

4.5.3.7. Project Cost Information

The respondent was asked to enter the project authorized budget and total installed cost, if known. If the respondent didn't know the project cost information, he or she was directed to select "unknown".

4.5.3.8. Project Schedule Information

The respondent was asked to enter the project planned start and finish dates, as well as the actual project start and finish dates. The dates for the planned schedule were specified as those in effect when the project was authorized to proceed. If the respondent could not provide an exact day for either the planned or actual dates, he or she was directed to estimate the respective dates to the nearest Monday.

4.5.3.9. Project Participant Information

Project participant information was collected for contractor respondents only. The intent was to determine in which phases of the project the contractor participated, as well as what percentage of those phases the contractor was involved in. If the respondent was a contactor, he or she was asked to enter the percentage of company involvement in the front-end planning, design, procurement, construction, and startup phases.

Chapter 5. Descriptive Analysis

This chapter presents a descriptive analysis of the project data collected with the Web-based data collection tool. A total of eighty-one project phases, from twenty-three unique projects, were collected in the database. When the non-industrial projects were removed, a total of seventy-four project phases from twenty-one unique projects remained for data analysis. Due to the fact that there were a small number of projects, the majority of the data analysis was conducted by project phase.

The data collected was for predominantly domestic projects, as shown in Figure 5.1. Approximately 95%, or twenty of the twenty-one projects were located in the

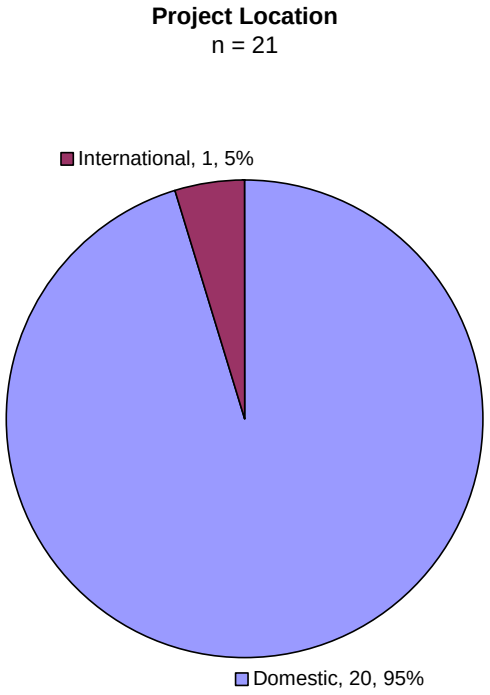


Figure 5.1. Graph of Project Location

United States. One international project, with five project phases, was located in the Middle East.

Of the seventy-four project phases collected (Figure 5.2), the majority were in the front-end planning phase, with nineteen project phases, or 26% of the total project data. The design, procurement, and construction phases were approximately equally distributed, comprising 20%, 20%, and 19%, respectively, of the total. Startup represented 16% of the distribution, with twelve project phases. Eleven of the twenty-one projects contained data for all five phases.

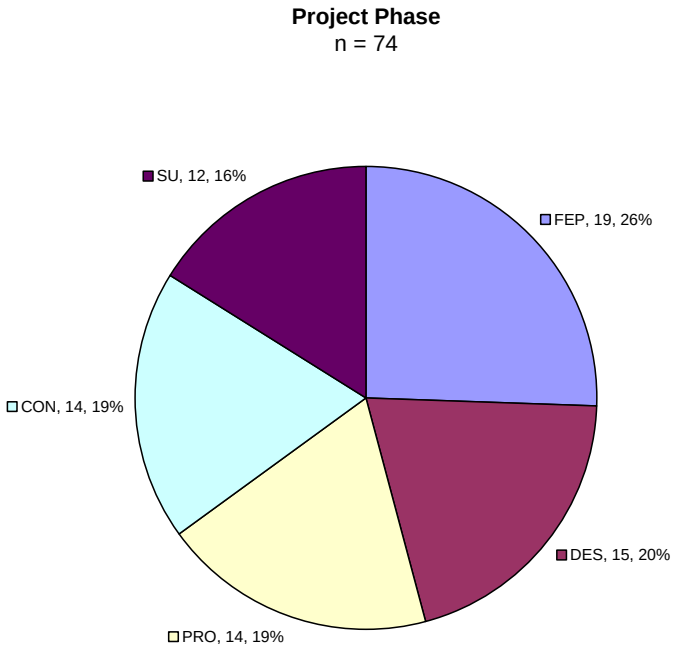


Figure 5.2. Graph of Project Phases

Project nature, shown in Figure 5.3, was evenly balanced among the project data collected. The modernization and addition categories each contained twenty-five project phases, representing 34% of the data collected. Twenty-four grass roots project phases, were submitted, comprising 32% of the project phases.

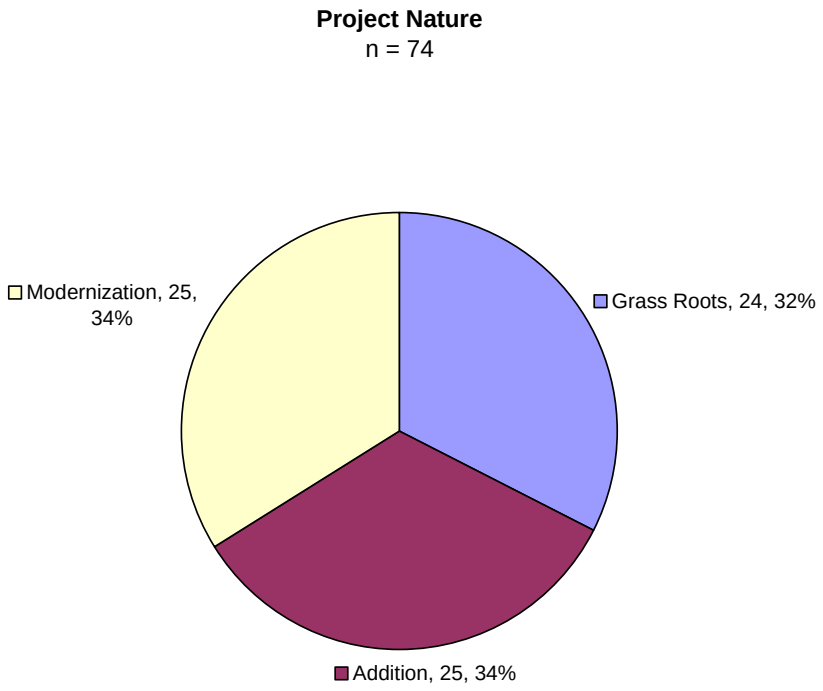


Figure 5.3. Graph of Project Nature

No projects of Threat Level 4 or Threat Level 5 were input into the database (Figure 5.4). Threat Level 1 was selected for thirty-one project phases, representing 42% of the total. Threat Level 2 followed with 31% of the total. Threat Level 3 contained twenty project phases, or 27% of the distribution.

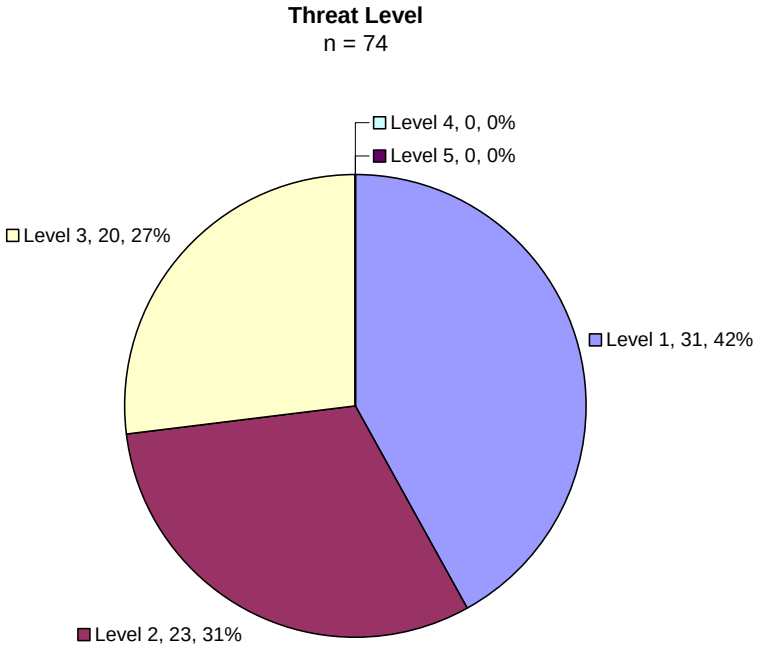


Figure 5.4. Graph of Threat Level

As in the case of Threat Level, not all levels of consequence were selected for the project data collected. No projects in Consequence Level 5 were entered. Consequence Level 2 had the most project phases, containing twenty-seven project phases representing 36% of the distribution. Consequence Level 4, with twenty project phases (27%), and Consequence Level 3, with seventeen project phases (23%), followed.

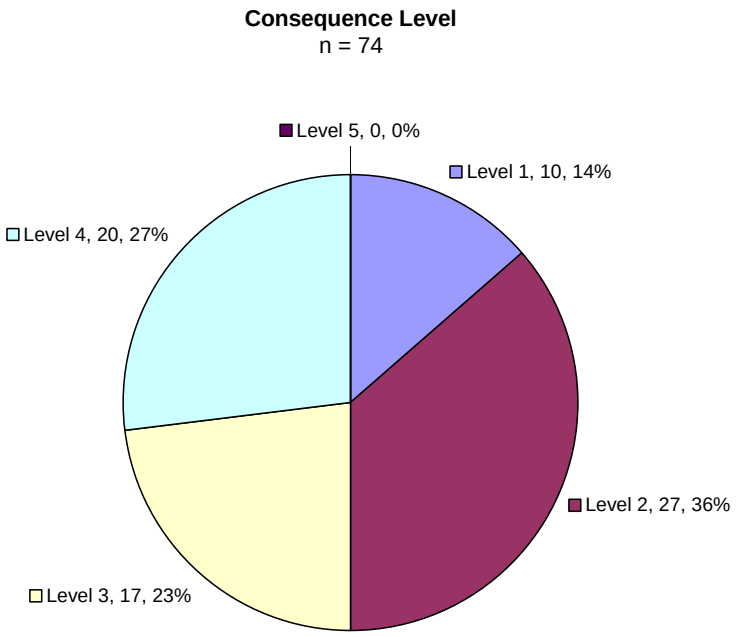


Figure 5.5. Graph of Consequence Level

The majority of the respondents (Figure 5.6) were project owners. Forty-nine project phases were entered by owners, representing 66% of the phase respondents. The remaining twenty-five phase respondents were contractors, representing 34% of the total.

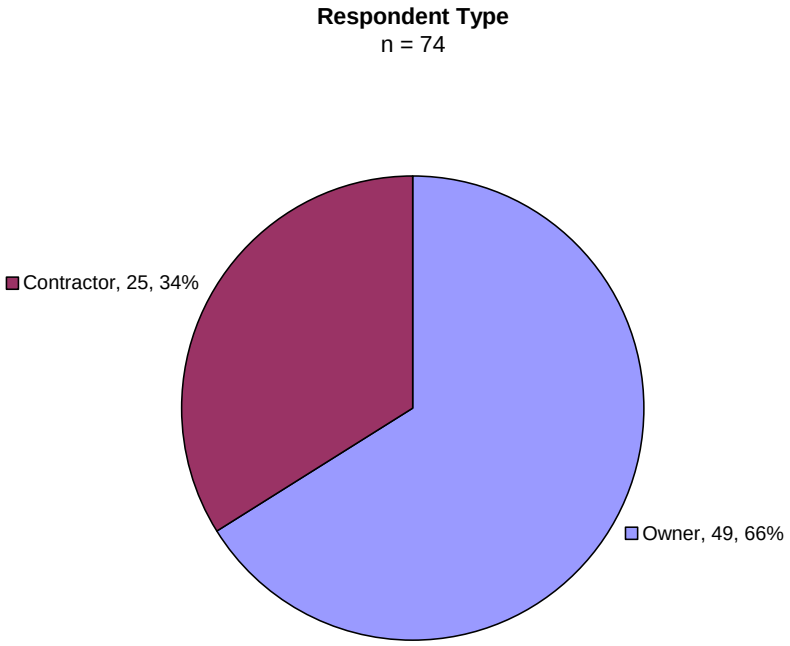


Figure 5.6. Graph of Respondent Type

Heavy industrial projects represented nearly three-fourths of the phase data collected for industrial category (Figure 5.7). Fifty-four of the seventy-four project phases (73%) were heavy industrial, followed by twenty light industrial projects phases (27%).

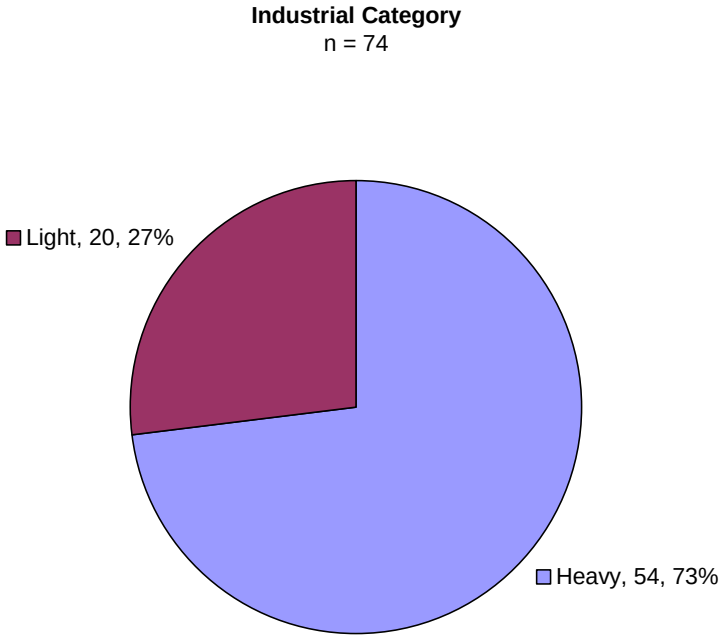


Figure 5.7. Graph of Industrial Category

The traditional design-bid-build project delivery system was the most commonly selected among the project phases in the database. As Figure 5.8 shows, traditional design-bid-build represented 60% of the project delivery systems. Design-build was the second most common project delivery system, with sixteen project phases representing 22% of the total. Multiple design-build and construction manager at risk were both selected for five project phases, or 7% of the total. Parallel primes was the least utilized project delivery system, with three project phases (4%).

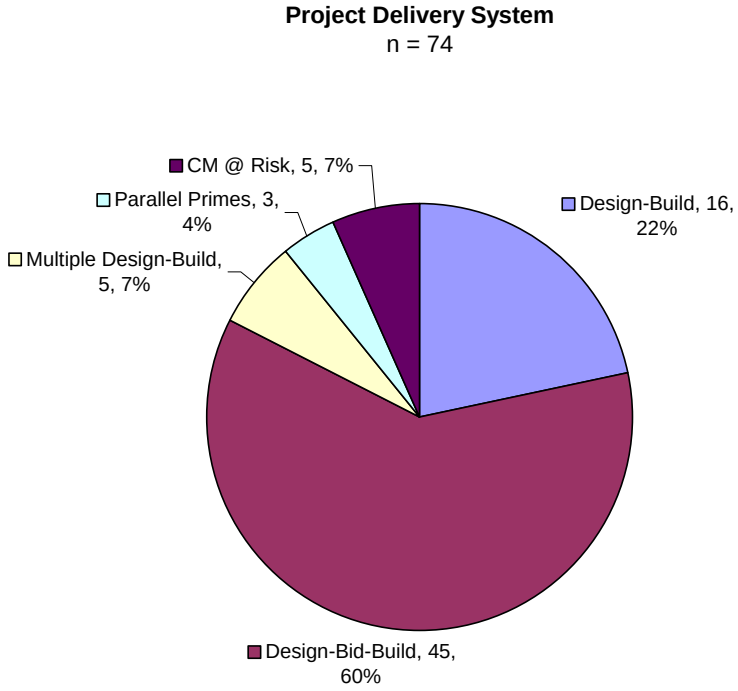


Figure 5.8. Graph of Project Delivery System

Chapter 6. Data Analysis Approach

Objective 3 of this research was to determine if a relationship could be established between Threat Level, Consequence Level, and the SRI score. Exploratory data analysis was performed to start the process of ascertaining relationships from the collected project data.

6.1. Observed Relationships

The SRI scores for projects in Threat Levels 1, 2, and 3 are depicted in a boxplot in Figure 6.1.

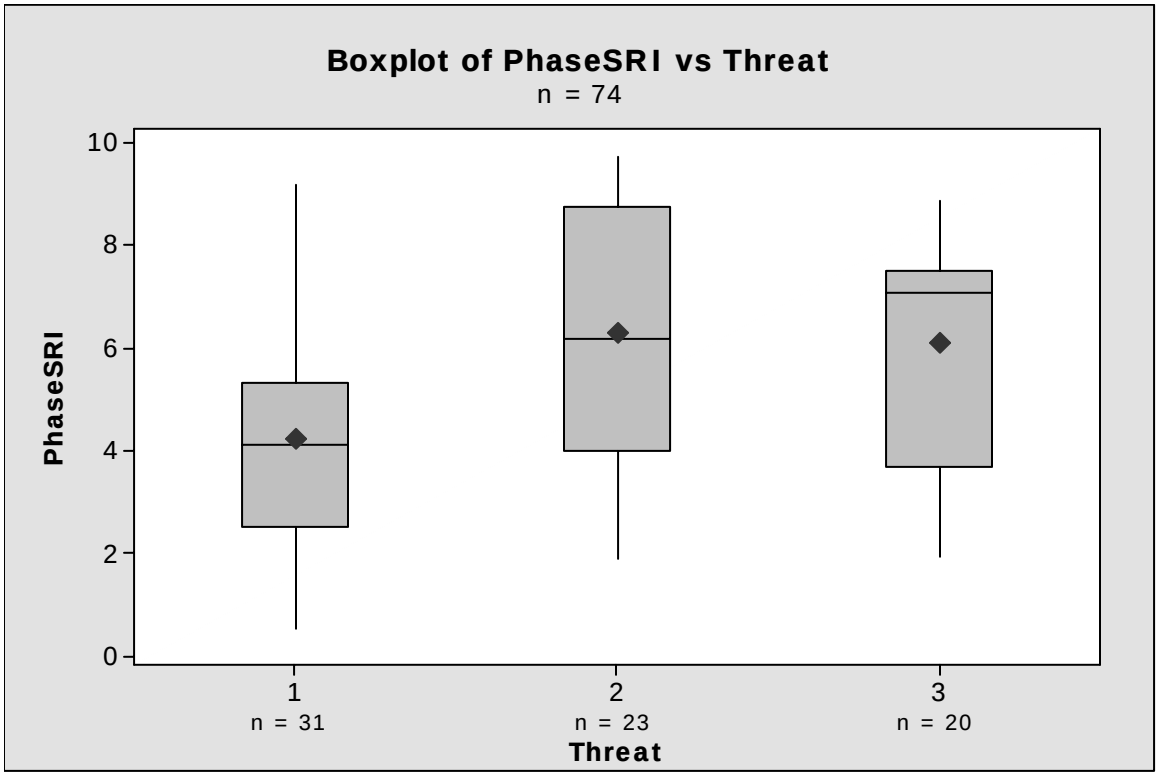


Figure 6.1. Boxplot of SRI Versus Threat

The median SRI score for a given Threat Level, represented by the horizontal line within the gray box, appears to increase as the Threat Level increases. The variance in the data is indicated by the vertical lines above and below the gray boxes. The variance of SRI scores for Threat Level 1 is the greatest. The boxplot for Threat Level 3 indicates that the distribution is skewed, as the horizontal line indicating the median SRI score is towards the top of the gray box rather than in the center of the box. In a normal distribution, the median and mean, indicated in the boxplot by a shaded diamond, should be in the same vertical position. The relationship indicated by the boxplot is intuitive; as the threat to a project increases, the SRI score would be expected to increase as well.

The boxplot of SRI versus Consequence Level, shown in Figure 6.2, indicates that SRI score tends to increase as the Consequence Level increases.

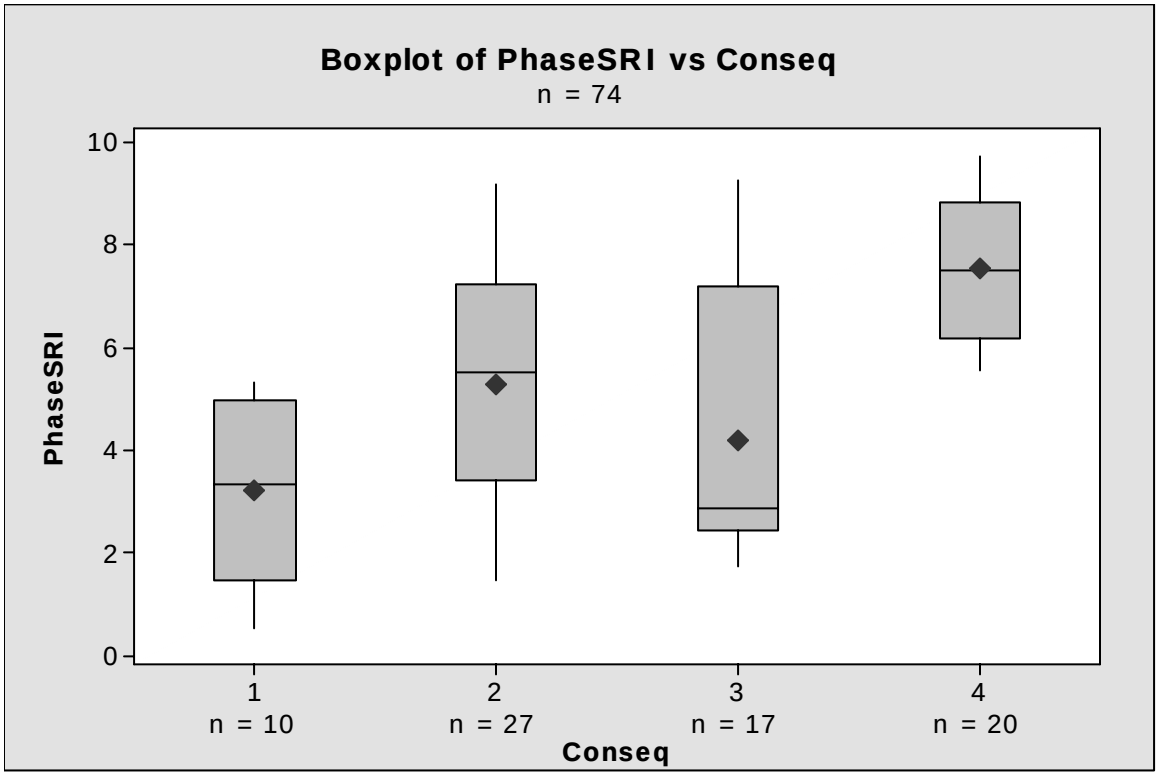


Figure 6.2. Boxplot of SRI Versus Consequence

Variance of the SRI scores is high for Consequence Levels 2 and 3. The distribution of SRI scores is skewed for Consequence Level 3, as the horizontal line indicating the median SRI score is towards the bottom of the gray box rather than in the center of the box, and the median and mean indicators are displaced. The apparent increase in SRI score as Consequence Level increases, similar to the observed relationship between SRI score and Threat Level, is expected.

The boxplot of SRI versus Consequence and Threat, Figure 6.3, does not indicate that for a given Consequence Level, the SRI score will increase as Threat Level increases. Phase SRI scores varied from 0.51 (Consequence Level 1, Threat Level 1) to 9.71 (Consequence Level 4, Threat Level 2).

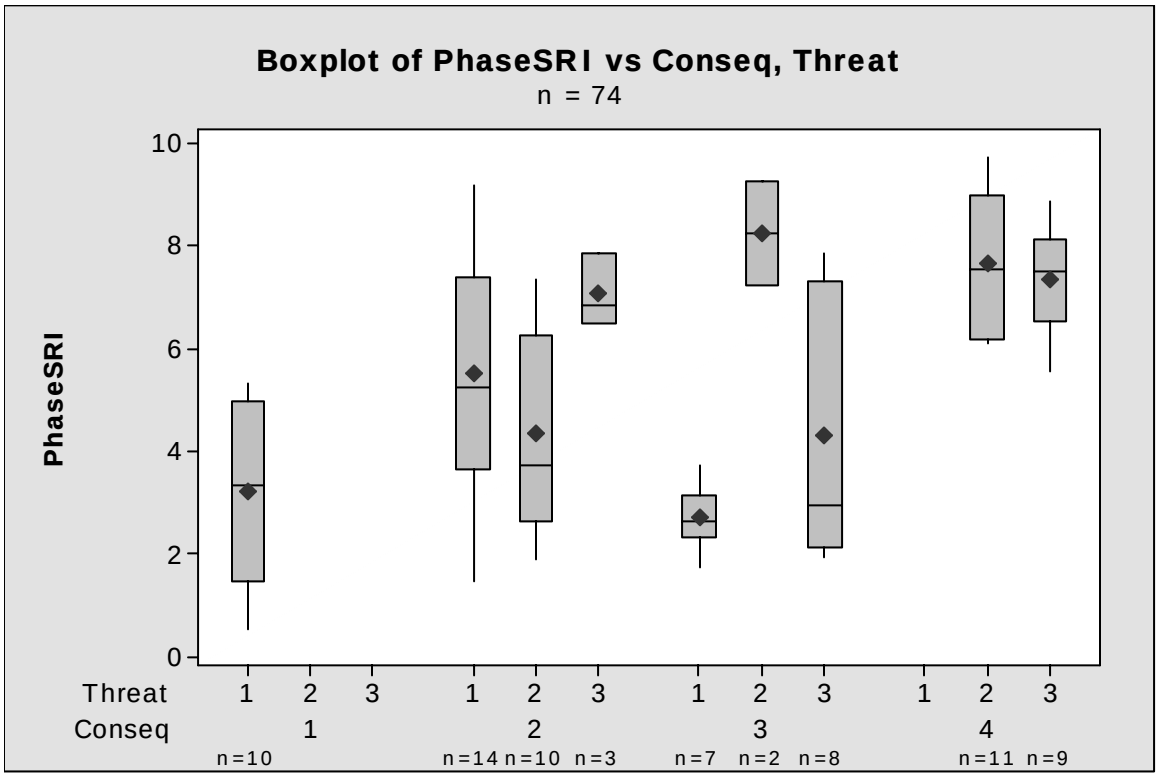


Figure 6.3. Boxplot of SRI Versus Consequence and Threat

For Consequence Level 2, the median SRI score decreases from Threat Level 1 to Threat Level 2, and then increases from Threat Level 2 to Threat Level 3. Variance of SRI score is high at Threat Level 1.

For Consequence Level 3, the median SRI score dramatically increases from Threat Level 1 to Threat Level 2, and then greatly decreases from Threat Level 2 to Threat Level 3, almost to the same median SRI score as Threat Level 1. Variance of SRI score is extremely high for Threat Level 3.

For Consequence Level 4, the median SRI score is nearly equal for Threat Levels 2 and 3. The variance of the SRI score for Threat Level 1 is greater than the variance of the SRI score for Threat Level 2.

Based upon the observed relationships in Figures 6.1 and 6.2, the expectation was that the median SRI scores would increase as the combinations of Threat Level and Consequence Level increased. The reason that the expected relationship is not evident could be related to the small data set, as SRI score does tend to increase in most of the combinations of increasing Threat Level and Consequence Level.

6.1.1. Scatterplots

Scatterplots were generated for the data to examine the relationship between Consequence Level and the Phase SRI scores for each Threat Level. Regression lines were fit to the scatterplots to see if they conformed to the hypothesized curves detailed in the Conceptual Model of SRI Use (Section 4.5.1). *The regression lines are not intended to illustrate a significant fit*; they were selected to quantitatively establish the relationships instead of subjectively estimating the slope from the small amount of data available.

Figure 6.4 depicts a scatterplot of SRI score versus Consequence for Threat Level 1. The regression line fit to the data points is nearly horizontal, suggesting that for Threat Level 1, SRI score is constant as Consequence Level increases from Level 1 to Level 3. This is a somewhat surprising result, as the median SRI scores appear to increase from Consequence Levels 1 and 2, yet decrease from Consequence Levels 2 to 3. This anomaly may be due to the fact that there are few project phases (n = 4) with a combination of Threat Level 1 and Consequence Level 3.

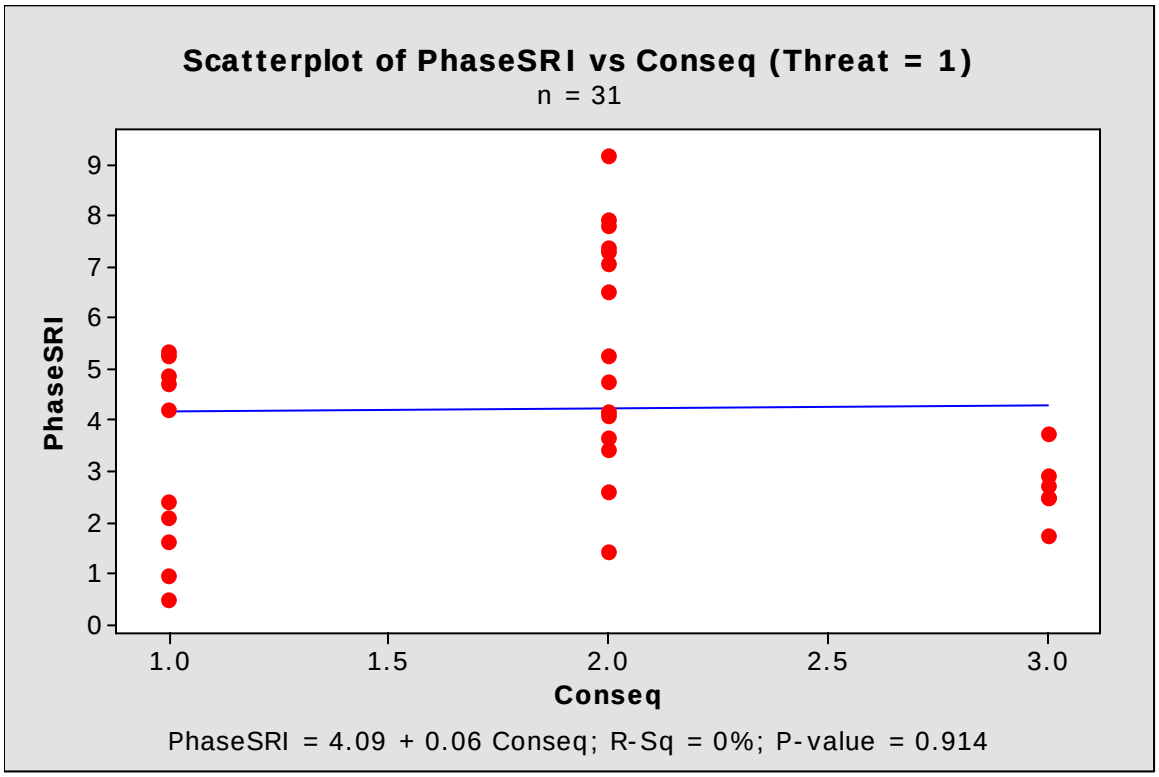


Figure 6.4. Scatterplot of SRI Versus Consequence for Threat Level = 1

Figure 6.5 depicts a scatterplot of SRI score versus Consequence for Threat Level 2. The regression line fit to the data points slopes upwards as Consequence Level increases, indicating that SRI score increases as Consequence Level increases. The exhibited relationship is as expected.

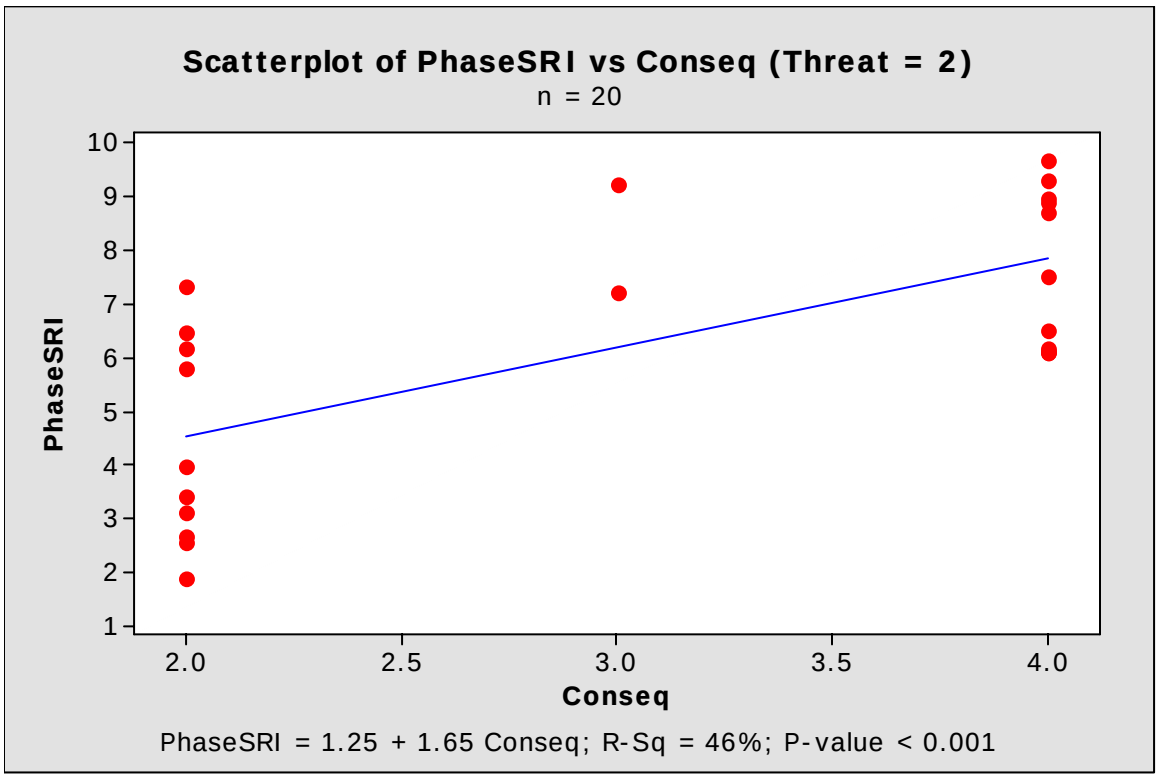


Figure 6.5. Scatterplot of SRI Versus Consequence for Threat Level = 2

The scatterplot of SRI score versus Consequence for Threat Level 3, shown in Figure 6.6, slopes upwards as Consequence Level increases as expected, similar to that of Threat Level 2. The regression line for Threat Level 3 indicates a higher initial SRI score than Threat Level 2 (~5 vs. ~4.5), yet its slope is less than the slope of the regression line for Threat Level 2.

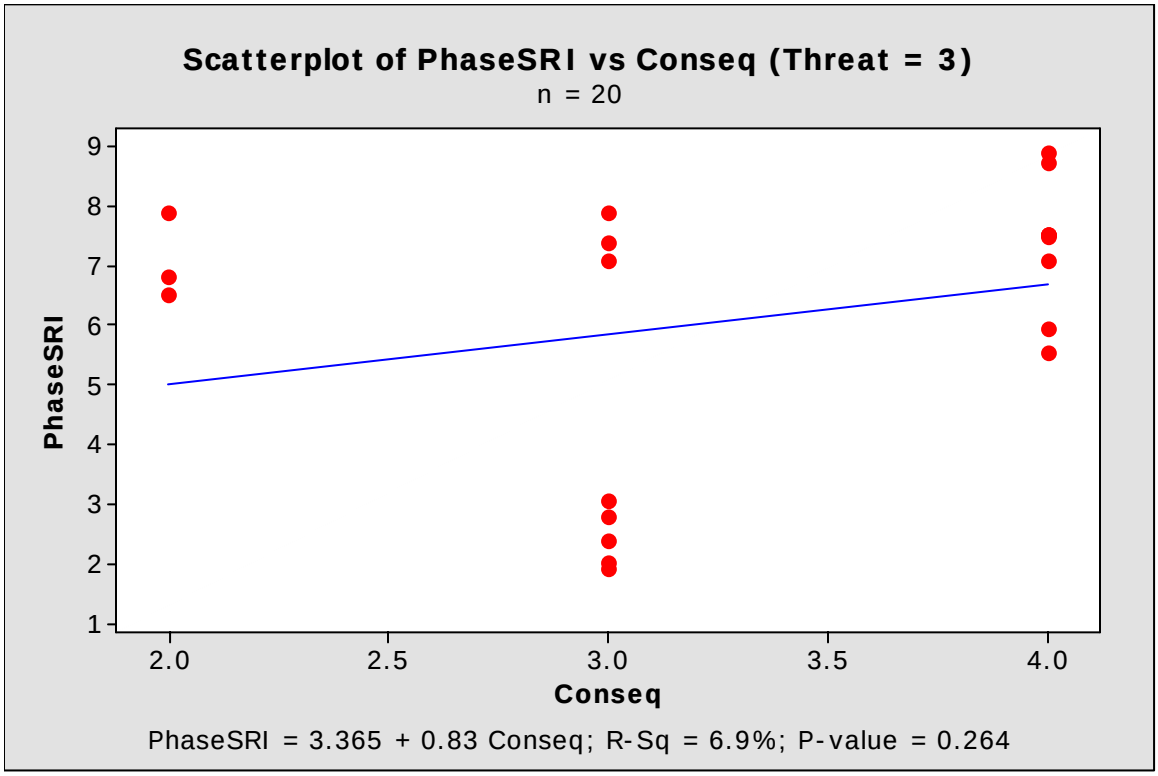


Figure 6.6. Scatterplot of SRI Versus Consequence for Threat Level = 3

When comparing Figure 6.6 to Figure 6.5, it is apparent that the SRI score for Threat Level 2 increases much more rapidly than the SRI score for Threat Level 3 as Consequence Level increases. This is apparently caused by five project phases with Consequence Level 3 and SRI scores below four. Four of the five phases are from one project, which also skews the boxplot in Figure 6.3. With the project phases from that

project eliminated, the scatterplot would look like the one depicted in Figure 6.7. The regression line shown is more in line with expectations and highlights the effects of having a small data set.

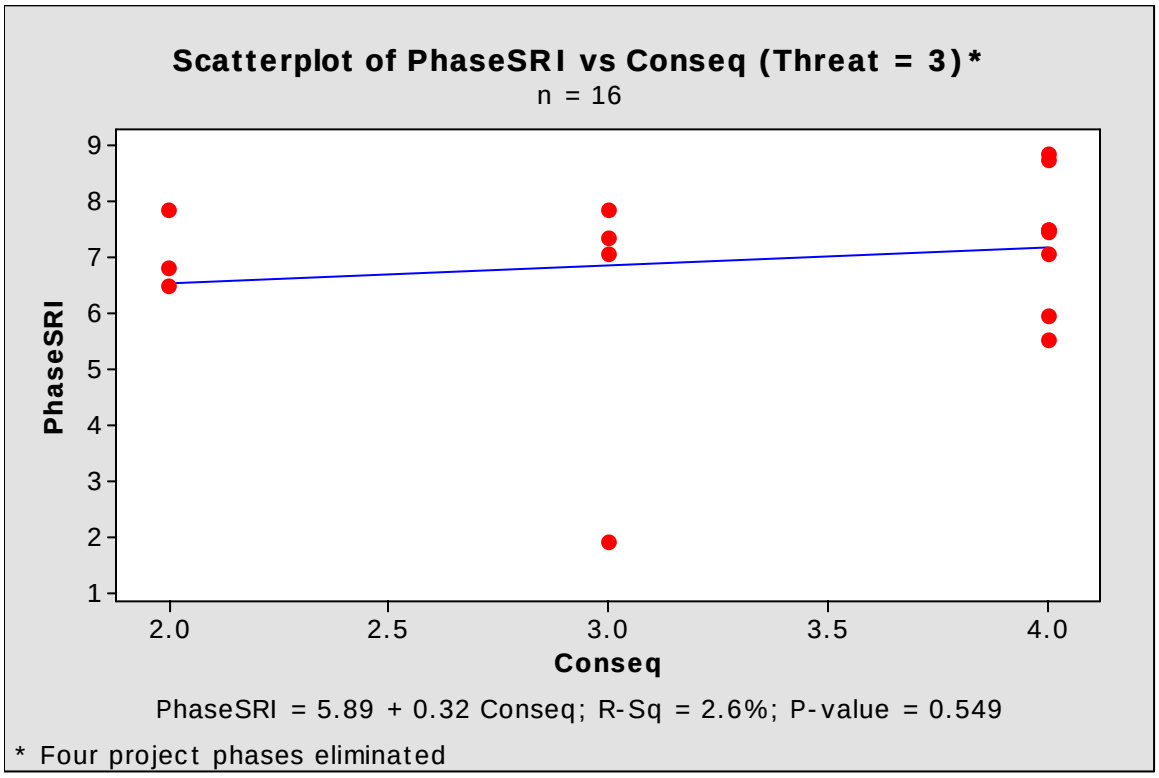


Figure 6.7 Scatterplot of SRI Versus Consequence for Threat Level = 3 With Four Phases Eliminated

The conceptual model of SRI use, detailed in Section 4.5.1, provides an example of the benefit of establishing the relationship between Threat Level, Consequence Level, and SRI score. Ideally, simple linear regression could be used to show that for a given Threat Level, there is a significant relationship between Consequence Level and SRI score. As evidenced by the exploratory data analysis, specifically Figures 6.4 through 6.6, this goal can not be achieved with the current data set.

Multiple regression was used to more fully explain the relationship between consequence and SRI score. Given the small sample size, statistically significant results were not expected; the method of analysis is presented to assist in the identification of variables and to illustrate future analyses when more data are available. The SRI score was designated the dependent, or response variable, while the other project variables, such as project phase and project delivery method were considered independent, or explanatory variables

6.2. MULTIPLE REGRESSION

According to Albright et al., multiple regression is the process of fitting a plane to data in three-dimensional space. There is one dimension for the response variable and one for each of explanatory variables (Albright et al. 2003).

The equation of the plane determining the response variable is estimated by the least squares method, which minimizes the distance between the fitted plane and the sum of the squared residuals, with the equation of the residual shown below (Figure 6.8).

$$Residual = Observed\ Value - Fitted\ Value$$

Figure 6.8. Equation of the Residual

6.2.1 Interpretation of Regression Coefficients

The general form of the multiple regression equation is shown below (Figure 6.9).

$$Y = a + b_1X_1 + b_2X_2 + \cdots + b_kX_k$$

Figure 6.9. General Form of the Multiple Regression Equation

In this equation, Y is the response variable, X1 through Xk are the explanatory variables, and b_1 through b_k are the slopes. Collectively, a and b_1 through b_k are known as the regression coefficients (Albright et al. 2003).

The intercept *a* is the expected value of *Y* when X_1 through X_k equal 0. Each slope coefficient is the expected change in *Y* when a particular *X* is incremented by one unit and all other *X*'s in the equation remain constant. The estimates of the *b*'s depend on which other *X*'s are included in the regression equation (Albright et al. 2003).

6.2.2. The Coefficient of Determination

The coefficient of determination, or R^2, is a measure of the goodness of fit of the least squares plane. It is the correlation between the observed *Y* values and the fitted $\hat{Y}$ values (Albright et al. 2003). With a value that ranges between 0 and 1, the coefficient of determination can be interpreted as the fraction of variation of the response variable explained by the regression (Albright et al. 2003). The statistical analysis output from MINTAB® expresses R^2 as a percentage, which may be interpreted as a percentage of variation explained by the regression. The formula for R^2 is shown below (Figure 6.10).

$$R^2 = 1 - \frac{\sum e_i^2}{\sum \left(Y_i - \overline{Y}\right)^2}$$

Figure 6.10. Formula for R^2

The variable e_i is the residual, the difference between the observed value of Y and the fitted value $\hat{Y}$. The standard deviation of Y is represented by the expression $(Y_i - \overline{Y})$. The equation indicates that when the residuals are small, R^2 will be close to 1 or 100%, but when they are large, R^2 will be close to 0 (Albright et al. 2003).

6.2.3. Adjusted R^2

There is a serious drawback to the coefficient of determination in multiple regression – R^2 can only increase when extra explanatory variables are added to an equation (Albright et al. 2003). According to Albright et al., this can lead to "fishing expeditions," where we keep adding variables to an equation, some of which have no conceptual relationship to the response variable, just to inflate the R^2 value (Albright et al. 2003).

An adjusted R^2 value is typically used to monitor when extra explanatory variables that do not really belong are added to the regression equation. It is an adjustment to R^2 for the number of explanatory variables in the equation. If potential explanatory variables are added and the adjusted R^2 value decreases, then the extra variables most likely don't belong in the equation and should be omitted from the regression (Albright et al. 2003).

6.2.4. Dummy Variables

Some of the potential explanatory variables in the model are categorical, and therefore cannot be measured on a quantitative scale. Since the categorical variables are possibly related to the response variable, SRI, they need to be included in the regression equation. This was accomplished by utilizing dummy variables.

Dummy variables indicate the category a given observation is in. If a dummy variable for a given category equals 1, the observation is in that category; if it equals 0, the observation is not in that category (Albright et al. 2003).

6.2.5. Statistical Significance

In order to determine whether or not the observed relationship between the response and predictors is statistically significant, the p-value needs to be calculated and compared to α.

The p-value indicates whether or not the association between the response and predictor(s) is statistically significant (MINITAB Inc. 2003). In other words, it is the probability of finding a significant association when one does not exist. It is calculated by comparing the t statistic on a given predictor variable with values in the Student's t distribution (Princeton University 2004).

The t statistic is the coefficient divided by its standard error. The standard error is an estimate of the standard deviation of the coefficient, the amount it varies across cases. It can be thought of as a measure of the precision with which the regression coefficient is measured. If a coefficient is large compared to its standard error, then it is probably different from zero (Princeton University 2004).

The Student's t distribution describes how the mean of a sample with a certain number of observations is expected to behave. If 95% of the t distribution is closer to the mean than the t-value of the coefficient of the predictor variable, then the p-value is 5%. This is also referred to a significance level of 5% (Princeton University 2004). The p-value is the probability of seeing a result as extreme as the one observed in a set of random data in which the variable had no effect. A p-value of 5% or less is the generally accepted point at which to reject the null hypothesis. With a p-value of 5%, there is only a 5% chance of concluding that the explanatory variable has an effect on the response variable when it does not.

Once the p-value is determined for a predictor variable, it is compared to α. If the p-value is smaller than the α selected, the association between the predictor and response variables is deemed statistically significant (Princeton University 2004).

The α is selected based upon the desired significance level, or the chance of making a Type I error. This type of error results in concluding that there is a relationship between the predictor and response variables when no relationship actually exists. In this research, an α of 0.05 is used. In other words, there is the possibility that 5% of the time when there is no relationship between predictor and response variables, the conclusion will be that there *is* a relationship (Trochim 2002).

6.3. ASSUMPTIONS

Multiple regression relies on certain assumptions about the variables used in the analysis. When these assumptions are not met, the results may not be trustworthy, resulting in a Type I or Type II error, or over- or underestimation of significance or effect size(s) (Osborne and Waters 2002).

The assumptions are: (1) normality, (2) linearity, (3) reliability, and (4) homoscedasticity.

6.3.1. Normality Assumption

Regression assumes that variables have normal distributions. Non-normally distributed variables (highly skewed or kurtotic variables, or variables with substantial outliers) can distort relationships and significance tests (Osborne and Waters 2002).

This research uses a normal probability plot along with the Anderson-Darling test statistic at a significance level of 0.05 to verify a normal distribution of the data. A normal probability plot of the regression residuals indicates whether the data are normally

distributed, other variables are influencing the response, or outliers exist in the data (MINITAB Inc. 2003).

The null hypothesis of a normality test is that there is a significant departure from normality. When the p-value is more than 0.05, it fails to reject the null hypothesis and thus the assumption holds (Yu 1998).

6.3.2. Linearity Assumption

Standard multiple regression can only accurately estimate the relationship between dependent and independent variables if the relationships are linear in nature. If the relationship between the predictor variables and the response variable is not linear, the results of the regression analysis will underestimate the true relationship. This underestimation carries two risks: increased chance of a Type II error for that response variable, and an increased risk of Type I errors (overestimation) for other predictor variables that share variance with that response variable (Osborne and Waters 2002).

In this research, visual examination of a plot of residuals versus fitted values is used to indicate whether a nonlinear relationship exists. Residuals scattered randomly around zero indicate a linear relationship (MINITAB Inc. 2003).

6.3.3. Reliability Assumption

Avoiding measurement errors is a consideration since the goal of research is to accurately model the "real" relationships evident in the population. In the case of multiple regression, effect sizes of other variables can be overestimated if the covariate is not reliably measured because the full effect of the covariate(s) would not be removed (Osborne and Waters 2002).

6.3.4. Homoscedasticity Assumption

Homoscedasticity means that the variance of errors is the same across all values of the predictor variables. When the variance of errors differs at different values of the predictor variables, heteroscedasticity is indicated (Osborne and Waters 2002). Slight heteroscedasticity has little effect on significance tests; however, when heteroscedasticity is marked, it can lead to serious distortion of findings and seriously weaken the analysis, thus increasing the possibility of a Type I error (Berry and Feldman 1985).

In this research, visual examination of a plot of residuals versus fitted values is used to check the assumption of homoscedasticity. Residuals scattered randomly around zero indicate an even distribution.

Chapter 7. Data Analysis

Once the statistical analysis approach was determined, the next step was to develop a regression model to establish relationships between the project data and SRI score. The intent of regression analysis was not to develop a predictive model, but to explore which variables contribute to project life-cycle security.

7.1. Regression Model Development

The model for SRI score was developed using forward stepwise regression. In each iteration of the model, The Phase SRI score (variable name *PhaseSRI)* was used as the response variable. Explanatory variables were selected based upon their correlation with *PhaseSRI.* A correlation matrix (Appendix I) was produced using MINITAB® Release 14 statistical software. Using criteria developed in previous CII research, variables correlated at the 0.40 level or greater, and with an $\alpha \leq 0.10$, were considered to be potential explanatory variables (Thomas 1996). The variable *US*, representing project location (Section 4.5.3.1), with a correlation with *PhaseSRI* of -0.382, was selected even though its correlation was less than 0.40. This was due to its correlation being close to 0.40, as well as its having a P-value of 0.001, indicating significance.

An interesting finding was that Threat Level (variable name *Threat*) was not statistically significant. A possible explanation can be found in the correlation matrix in Appendix I. The correlation between *Threat* and Consequence Level (variable name *Conseq*) was 0.596 with a p-value of < 0.001. This indicates a strong, statistically significant relationship between Threat Level and Consequence Level. This suggests that collinearity exists between *Threat* and *Conseq*, with *Conseq* measuring some of the relationship between *Threat* and *PhaseSRI*.

Another potential explanation for *Threat* not being correlated to *PhaseSRI* can be found in an interview given on *National Public Radio* by Homeland Security Secretary Michael Chertoff outlining a risk-based approach to homeland security. He stated:

> If we simply react based on threat, we are going to be chasing our tails. We can not drive our investment in security based on a particular threat… We have to look holistically – what are the consequences, where we are vulnerable, and there where the threat seems to be…as we manage the most significant risks, we drive down the consequences of an act. …by targeting high-priority elements of where they [organized crime] were creating the most damage to society…we drove the consequences down to a level which was still bad, but was not as bad as it had been. Likewise, in the area of terrorism, what we seek to do…is drive down, again to protect the most important, most valuable things, against the greatest risks, so that the consequences of an act are less serious… (Inskeep 2005)

Table 7.1 summarizes the potential explanatory variables selected using the correlation matrix. The variable *Owner* represents respondent type (Section 4.5.3.1). The variable *CM* represents the Construction Manager at Risk project delivery system (Section 4.5.3.5).

Table 7.1. Potential Explanatory Variables

Potential Explanatory Variable	**Correlation with *PhaseSRI***	**P-Value**
Conseq	0.479	< 0.001
Owner	-0.465	< 0.001
CM	-0.419	< 0.001

Multiple regression was performed with MINITAB® Release 14 statistical software. The procedure entailed introducing one of the potential explanatory variables to the model and conducting an initial regression analysis.

Following the regression analysis, residual plots were reviewed to determine if the model met regression assumptions. The explanatory variables were checked for

significance using an α of 0.05, those with a p-value of < 0.05 were deemed significant and retained, those with a p-value of ≥ 0.05 were removed from the model. The adjusted R^2 was examined to determine if the added explanatory variables belonged in the model.

Additional explanatory variables were then added to the model and the process repeated until the effect of all explanatory variables on the response variable was investigated.

Note that even though the variables *US* and *CM* were selected as potential explanatory variables, they were not included in the regression modeling due to their extremely small sample sizes. Data collected for *US* and *CM* consisted of one unique project with five project phases for each variable. With more data, the potential relationships between these variables and SRI score could be explored.

7.2. MODEL ITERATION ONE

The first iteration of the regression model was to investigate the relationship between Consequence Level and the SRI Score.

7.2.1. Check of Normality of Variables

PhaseSRI was examined using a normal probability plot (Figure 7.1). Since the p-value was less than α, the null hypothesis was rejected and the distribution of *PhaseSRI* was determined to be normally distributed. *Conseq* is a discrete variable and can not be normally distributed (Sakamoto 2005).

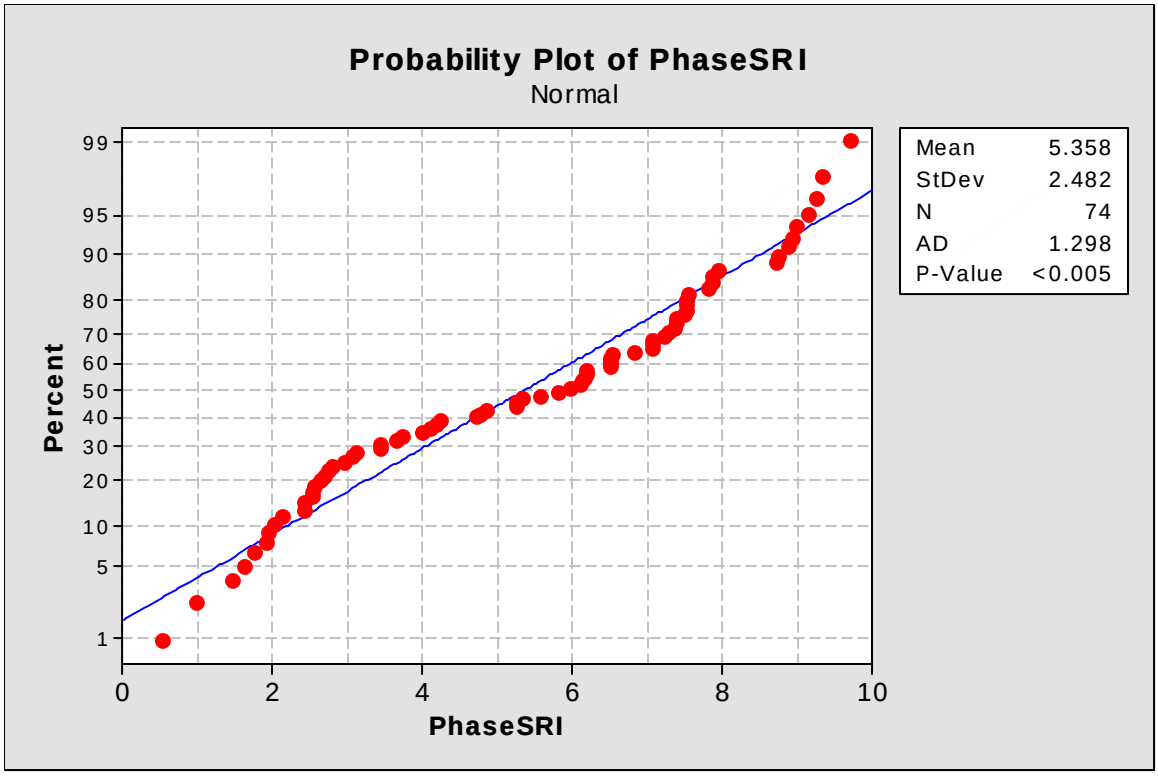


Figure 7.1. Normal Probability Plot of SRI Score

7.2.2. Regression Results for Model Iteration One

A portion of the regression output for *PhaseSRI* versus *Conseq* is shown below (Figure 7.2). Since the p-value of *Conseq* was less than α; it is considered a statistically significant predictor of SRI score and was retained for the next iteration of the regression model.

Regression Analysis: PhaseSRI versus Consequence

```
The regression equation is
PhaseSRI = 2.33 + 1.15 Conseq

Predictor    Coef  SE Coef     T      P
Constant   2.3305   0.7017  3.32  0.001
Conseq     1.1550   0.2494  4.63 <0.001

S = 2.19393   R-Sq = 23.0%   R-Sq(adj) = 21.9%
```

Figure 7.2. Regression output for *PhaseSRI* versus *Conseq*

7.2.2.1. Check of Regression Assumptions

The residual plots for *PhaseSRI* versus *Conseq* are shown below (Figure 7.3).

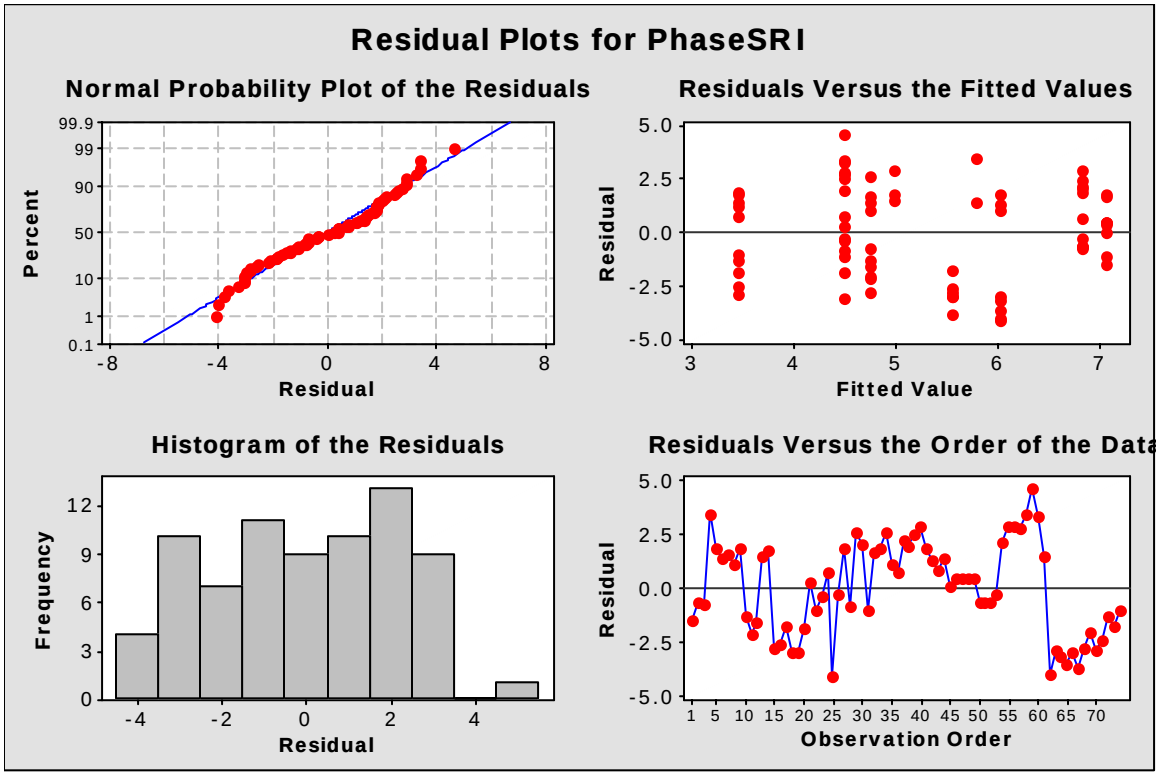


Figure 7.3. Residual plots for SRI score vs. Consequence Level

The normal probability plot of the residuals indicates that the data is normally distributed. Visual examination of the plot of residuals versus fitted values shows residuals scattered randomly around zero, indicating a linear relationship as well as homoscedasticity. The plot of residuals versus the order of the data does not indicate autocorrelation.

7.3. MODEL ITERATION TWO

One additional model iteration was analyzed in accordance with the procedures explained in Section 7.1; the regression output is included in Appendix J. A summary of the regression equations, significant variables, adjusted R^2, and R^2 for each iteration is shown in Table 7.2.

Table 7.2. Summary of Regression Models

Model	Regression Equation	Significant Variables	Adj. R^2	R^2
1	*PhaseSRI* = 2.33 + 1.15 *Conseq*	*Conseq*	21.90%	23.00%
2	*PhaseSRI* = 4.13 + 0.985 *Conseq* - 2.04 *Owner*	*Conseq* , *Owner*	36.00%	37.80%

7.4. INTERPRETATION OF THE REGRESSION MODEL

The regression equation for SRI score (Figure 7.4) can be used to estimate the SRI score for a project phase based upon the selected Consequence Level and whether the respondent is an owner or contractor. As was previously stated, the regression model is not intended to be used for predictive purposes, but as a tool to explore the relationships between the phase SRI score and the variables correlated with it.

PhaseSRI = 4.13 + 0.985 Conseq - 2.04 Owner

Figure 7.4. Regression equation for SRI score

The intercept of 4.13 is not useful by itself, as the Consequence Level, and respondent must be selected for each project, altering the regression equation.

The slope for Consequence Level means that for each incremental consequence level selected, the SRI score will increase by 0.985 *holding all other variables constant*. This finding is expected, since it is reasonable to assume that as the consequence of a security breach increases, the level of security practice implementation would increase.

The negative slope for *Owner* indicates that when a project owner is the respondent, SRI score *decreases* by 2.04 *holding all other variables constant*. If the respondent is a contractor, the value for *Owner* is 0, and there is no net effect.

This is not an intuitive finding considering that one would suspect the owner of a facility to have a greater interest in its security over its life cycle than a contractor. The industry trend towards reducing engineering staff may be one reason that an owner respondent negatively impacts the SRI score. A large amount of capital facility work is now outsourced by owner organizations (Gibson et al. 1998).

Depending upon the project delivery system selected by the owner, the contractor may be heavily involved in all phases of the construction project. As the trend in construction moves away from traditional design-bid-build to design-build, the owner focus shifts from coordination to scope definition; the contractor assumes the coordination responsibility (Design-Build Institute of America 1994). A review of the AHP output in Appendix G shows that the contractor may be involved in nearly all of the thirty-three security practices identified in this research. Nine of the first ten practices,

totaling 63% of the SRI score, are coordination-related, and may be performed by the contractor.

Another consideration is that the experienced project managers retained in-house at owner organizations are nearing retirement age (Davis-Blake et al. 1999). This suggests that the slope for *Owner* may become even more negative in the future as the project managers retire and the owner organizations become even more reliant upon the contractor.

7.5. LIMITATIONS OF THE REGRESSION MODEL

There are limitations to the SRI regression model. While the model conforms to multiple regression assumptions (Section 6.3), it can not be applied in all cases.

A fundamental limitation of the model is that it uses a small sample size to estimate a population. There are many rules-of-thumb that suggest how many data points are needed to estimate a population, but no conclusive number. Sample sizes recommended for behavioral research include: (1) at least 100 subjects, (2) at least 200 subjects, (3) $N > 50 + m$, where m is the number of predictors, (4) $N \geq 50 + 8m$, where m is the number of predictors, and (5) a minimum subject-to-predictor ratio ranging from 15-to-1 to 25-to-1 (Green 1991).

Under these rules-of-thumb, the amount of data points required would be: (1) 100, (2) 200, (3) 53, (4) 74, and (5) 45 to 75. The seventy-four project phases in this research meet rules-of-thumb 3, 4, and 5, indicating that it is possible that the seventy-four project phases are sufficient for estimating the multiple regression.

A direct limitation of the SRI regression model is that the equation can not be extrapolated to Consequence Level of 5, as none of the projects in the database had that Consequence Level. The model may also not account for the fact that Threat Levels 4 and 5 may be significant, as there were no projects with that magnitude of threat.

Because the regression model can not be extrapolated, it may not be used to predict individual project phase SRI scores.

The regression model was also developed using phase SRI scores. It may not be interpreted at the project level. A separate model would need to be developed in order to examine relationships at the project level.

The nature of the data collection process also presents limitations. Responses to the questionnaire, which determine SRI score, are subjective. One respondent's interpretation of "strongly agree" may vary from another respondent's, leading to different SRI scores for the same level of security integration.

The memory of respondents may also have an impact on the model. The majority of the data collected was from previously completed projects. Data submitted from memory may not be accurate, e.g., respondents may not be able to recall past conditions, such as the Department of Homeland Security Threat Advisory Level, when selecting Threat Level

7.6. ASSESSING THE IMPACT OF SECURITY IMPLEMENTATION ON PROJECT OUTCOMES

The regression model developed in this chapter can be expanded to assess the impact of security implementation on project outcomes such as cost and schedule performance.

Project cost data and project schedule data were collected in the Web-based tool as detailed in Sections 4.5.3.7 and 4.5.3.8, respectively. From this data, the cost performance (amount over or under project budget) as well as the schedule performance (number of days over or under schedule) could be calculated. Using the methodology in Section 7.1, a correlation matrix could be generated for SRI score, cost performance, and schedule performance.

If the correlations between the project outcomes and the SRI score were statistically significant, a regression model could be developed to determine if the relationship could be described and if it was statistically significant. This model, if significant, would facilitate assessment of the impacts of security implementation on project outcomes.

Chapter 8. Implementing Project Security

The author wrote a guide to implementing project security practices to facilitate the adoption of the security best practices by industry. While it does not provide specific guidance for the implementation of security procedures at the project level, it offers a framework for integrating security into the project delivery process in the context of likely threats facing the facility and consequences of security breaches.

The implementation procedure consists of a nine-step process of integrating security into the project delivery process.

8.1. Approach to Implementing Project Security

This chapter provides an approach for the incorporation of security practices into all phases of industrial project planning and execution, resulting in increased security throughout the project life cycle, which includes the operational phase of the project. Decisions made during the planning and execution of a project, e.g., site selection, will continue to impact the security of that facility until decommissioning.

While implementing the security practices in this chapter does not guarantee that a project will be free of security breaches, it will increase the security posture of that project. In many cases, the additional cost and effort of incorporating security practices into the project planning and execution processes are minimal.

This process of integrating security into the project delivery process leverages CII research to present an efficient approach for project teams, whether owner or contractor, to increase security implementation on their projects. The security practices and questionnaire are not intended to be stand alone tools. They are best used in conjunction with risk assessments and SVAs to provide integrated security analysis and to incorporate security throughout the project life cycle.

8.2. INTENDED USERS

This process is intended for both owner and contractor project team members. The project owner will operate and maintain the facility throughout its life cycle. In order to maximize the return on investment, the owner's project team must ensure that security is incorporated during the project planning and execution process. When security is "built in" to a project, it reduces the need to retrofit security improvements later in the project life cycle, which results in greater cost. Some security considerations, such as site location, may be impossible to address in the future.

For the contractor, increased project security pays large dividends. A jobsite free of security incidents increases profitability. Greater security can result in less theft of tools and equipment, less rework due to sabotage and vandalism, reduced employee absenteeism, and fewer accidents due to drug and alcohol abuse. A contractor that gains a reputation for knowledge and implementation of security practices has another means to differentiate the firm from that of its competitors. Experience following the events of 9/11 indicates that any firm involved in a facility confronted with a major incident may become a target of litigation; a contractor that better implements security may also have less exposure to liability resulting from a breach.

8.3. HOW TO USE THE SECURITY BEST PRACTICES

Before beginning a project, it is recommended that all project team members read this entire chapter for an understanding of the implementation process. Not only will it give each team member an overall view of project security, but it will facilitate the implementation of project security since all members will have an understanding of the process.

It is critical to continually review security practices as a project progresses. Threats to a project may change at any time, such as when the Department of Homeland

Security Threat Advisory is raised or lowered. Recent criminal activity may also necessitate revising security practices as well. For example, recent thefts of heavy equipment from local construction projects may prompt a project team to reevaluate the security plan for a storage yard.

Implementing project security requires integrating security activities into the project planning and execution processes that normally occur during project delivery. For clarity of illustration, this manual presents implementation at the phase level as depicted in Figure 8.1. Since phases have significant overlap, the reader should realize that the process shown would be implemented concurrently with similar processes for other overlapping phases. By following the nine-step process, it is possible to integrate security in a thorough and structured manner that should provide a comprehensive solution.

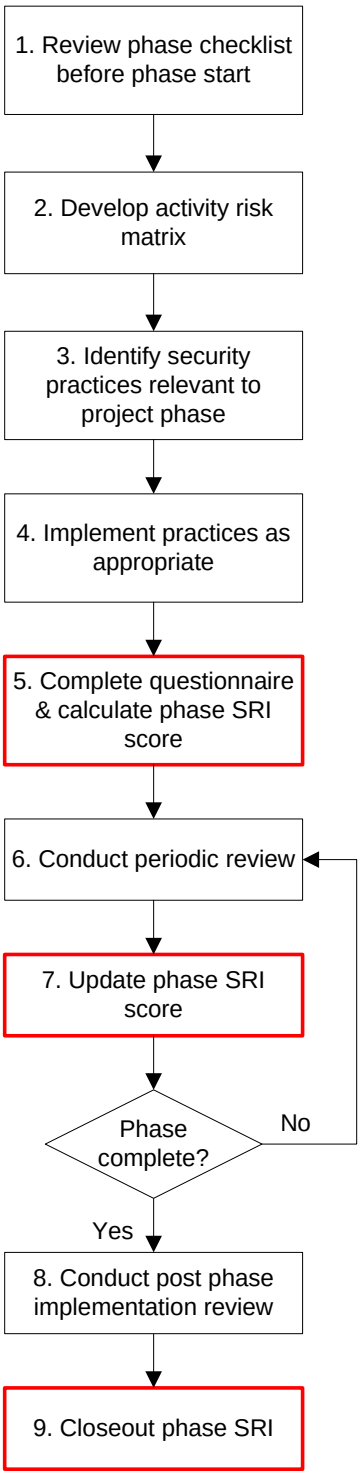


Figure 8.1. Security Best Practices Implementation Process

Figure 8.1 is provided primarily as a roadmap for security implementation at the project phase level, but it also serves as an introduction to scoring the level of implementation for comparative purposes. Scoring of the practices in steps five, seven, and nine which address use of the SRI are optional if implementation is the only goal. The SRI Web-based data collection tool, detailed in Section 4.5.2, is an electronic tool that organizes the security practices into a questionnaire that can be quantitatively scored to assess the level of implementation. Section 8.4 explains the SRI and scoring in more detail, however, if the project team is only interested in security implementation, they may skip steps five, seven, and nine. It is expected that most teams will quickly realize the benefits of using the electronic tool for assessment and will also desire to have quantitative feedback on their level of implementation.

The following sections present a discussion of the nine-step process for implementation and then address implementation by project phase. The practices relevant to each phase are presented along with discussion of the security elements addressed by these practices.

8.4. THE NINE-STEP PROCESS

1. Review phase checklist before phase start.

Prior to the start of a project phase, review the phase's security practices identifying the activities for that phase for which security should be considered. This will give the project team a detailed understanding of the types of activities for which security risk should be addressed.

2. Develop activity risk matrix.

To determine which of the security practices are relevant to their project, the project team should develop an activity risk matrix for the upcoming project phase. At a minimum, the matrix should include specific identified security risks, the security element (i.e., physical, personnel, or information), and the planned means of minimizing or eliminating the security risk. An example risk matrix is provided later in this section.

The team should include corporate security management and risk management personnel in the process. The activity risk matrix should be compared against the SVA prepared by corporate security management to ensure that all foreseen risks are addressed.

Prior to developing the risk matrix, the project team should assess the Threat Level and Consequence Level for the project. An understanding of the level of threat against the facility to be constructed and an appreciation for the consequences of a security breach will better enable the team to develop its risk matrix. It is during these assessments that corporate security and risk management input is essential. The

SVA prepared by corporate security personnel should be used in the threat and consequence assessments as well as preparation of the risk matrix.

Following the threat and consequence assessments, the project team is prepared to develop their activity risk matrix. The activity risk matrix can be substantial for the typical project, but by focusing on a phase at a time, the project team can better address the task. As previously noted, the activity risk matrix should be produced with the assistance of corporate security and risk management specialists. Figure 8.2 shows an excerpt from an activity risk matrix for illustrative purposes.

Project Name:	**Chemical Plant B**	
Project Phase:	**Construction**	
Risk	**Risk Type (Phys, Pers, Info)**	**Measures to address risk**
Equipment Theft	Pers, Info	Conduct background check of all employees
		Ensure vendors submit verification of background check for all employees
		Establish 100% identification requirement for site
		Require written authorization to remove tools/equipment from site
		Ensure visitors are escorted at all times
		Establish emplyee parking area off site
		Ensure entrances to site 100% secured
Accidents Due to Drug/Alcohol Abuse	Pers	Conduct background check of all employees
		Train supervisors to recognize signs of drug/alcohol abuse
		Conduct random drug screenings
		Require employees to show prescriptions for any drugs brought on site

Figure 8.2. Activity Risk Matrix

3. Identify security practices relevant to project phase

Following development of the activity risk matrix, the project team is prepared to identify security practices relevant to the upcoming project phase. This task should be performed with the participation of the entire project team or at least with key team members. The team should address each security practice sequentially and determine how the practice is pertinent to their particular project. Once again the team may seek the input of corporate security management and risk management personnel, as their expertise may give additional insight for the team.

4. Implement practices as appropriate

One relevant security practices are identified, the team needs to implement the practices during the current project phase.

5. Complete questionnaire and calculate Phase SRI score

This step, while not essential for implementation of security practices, is important for determining a baseline security implementation score for future comparisons. A designated member of the project team should enter the project data and receive a Phase SRI score. This score will allow the project team to compare their security implementation within a phase as it progresses. An overview of the Web-based tool is given in Section 4.5.2.

6. Conduct periodic review

As implementing security is rarely a static activity, the project team will need to conduct an iterative review and adjustment process throughout each project phase. The team should establish a scheduled security implementation review meeting throughout the project planning and execution process. The most efficient method is to conduct the meeting in conjunction with another meeting in which the project team will convene, such as a quarterly review meeting. Corporate security management and risk management personnel should participate in this review process as well.

The objective of the periodic review is to determine if security risks to the project have changed, whether security practices should be added or deleted, and whether planned activities to address risk need to be updated. The team should utilize their threat level and consequence level matrices and their activity risk matrix from Step 2 in conjunction with their responses to the security questionnaire from Step 4. Identified changes in the security risks should be reflected on an updated activity risk matrix.

Security incidents that have occurred on the project should be investigated immediately. Following the initial investigation, the project team should determine if modifications must be made to the threat level, consequence level, the activity risk matrix, and security procedures to preclude a repeat or similar incident from occurring on the project in the future. The discussion can be by teleconference for a minor incident or may require a special meeting for a serious incident.

7. Update Phase SRI score

Following the periodic reviews, the project team member designated to enter information in the Web-based Security Rating Index tool should validate the current phase responses and make changes as necessary. This will improve the accuracy of data being tracked.

Note that the questions address practices that have occurred in the past, therefore, the project team has the benefit of hindsight in answering the questions. If an event occurred that suggested that the project team either did not consider security as thoroughly as they had previously thought, or that the implementation of security was much greater than previously thought, the question responses should be revised accordingly.

The updated SRI score can then be compared to the previous SRI score(s) as in indicator of the phase security implementation trend.

8. Conduct post phase implementation review

Once the current phase is completed, the project team and security management and risk management personnel should conduct a review of the security implementation process for that phase. The intent is to determine how to improve performance for the upcoming phase(s). The team should assess whether the previous identification of security practices was sufficient, whether the security risk matrix was comprehensive enough, and whether unforeseen security incidents (if any) could have been identified in the planning process. Findings should be documented and utilized during security risk assessments for follow-on phases.

9. Closeout phase SRI

Assuming that the team is using the SRI, the final step in each phase is for the designated project team member to make any necessary changes to the responses previously entered, closeout the phase input, and view the final Project SRI score.

8.5. IMPLEMENTATION OF PRACTICES BY PROJECT PHASE

In order to implement the security best practices as intended, the team must have an understanding of the participants, milestones, typical activities, and products that define the phases. These items will be discussed and the relevant security elements will be expanded upon in this section.

8.5.1. Front-end Planning

Front-end planning is the phase in which the project team can have the greatest impact on project life-cycle security. Front-end planning represents approximately 54% of the security practice implementation on a project (Construction Industry Institute 2004a).

Table 8.1 summarizes the typical participants, start and finish milestones, and typical activities and products of the front-end planning phase.

Table 8.1. Front-End Planning Phase Summary

Typical Participants	Owner Personnel
	Planning Consultants
	Constructability Consultant
	Alliance/Partner
Phase Start	Defined business need that requires facilities
Phase Stop	Total project budget authorized
Typical Activities & Products	Options Analysis
	Life-cycle Cost Analysis
	Project Execution Plan
	Appropriation Submittal Package
	Piping & Instrumentation Diagrams (P&ID)
	Site Layout
	Project Scoping
	Procurement Plan
	Architectural Rendering

Personnel and information elements dominate the activities that occur in the front-end planning phase. As an example, the activities of identifying stakeholders, ensuring alignment among the project team members, developing business partnerships and alliances, screening project teams, and pre-qualifying and selecting suppliers, all have personnel considerations. They form the foundation of project success as well as present the greatest opportunities to compromise project life-cycle security. If the wrong individuals are selected, or if they lack alignment concerning the importance of security, the life-cycle security of the project can be compromised before it is even designed.

Information security is crucial because of the amount and type of information that is distributed in the front-end planning phase. Personnel files, specifications and

requirements, plot plans, and security plans are all being circulated. It is critical to safeguard this information, as additional opportunities to compromise project life-cycle security are introduced if control is not maintained. Although there are actually more practices in this phase addressing physical security elements, when weighted for relative importance using the weights from Appendix F, personnel and information elements have a much greater bearing on life-cycle security. In fact, physical security is the least influential security element for project life-cycle security. Personnel security, with a 53% influence, and information security, with a 33% influence, far outweigh physical security at 14% influence (Construction Industry Institute 2004a).

8.5.2. Design

The design phase is the second most influential phase on project life-cycle security representing approximately 23% of security practice implementation on a project (Construction Industry Institute 2004a). Table 8.2 summarizes the typical participants, start and finish milestones, and typical activities and products of the design phase.

Table 8.2. Design Phase Summary

Typical Participants	Owner Personnel
	Design Contractor
	Constructability Expert
	Alliance/Partner
Phase Start	Design Basis
Phase Stop	Release of all approved drawings and specs for construction (or last package for fast-track)
Typical Activities & Products	Drawing & Spec Preparation
	Bill of Material Preparation
	Procurement Status
	Sequence of Operations
	Technical Review
	Definitive Cost Estimate

The shift from greater personnel security influence in the front-end planning phase to the greater influence of information security in the design phase is due to the information-centric nature of design. While there is significant overlap in the types of information being distributed in the front-end planning and design phases, the recipients of that information are much more diverse in the design phase. Plans, specifications and requirements, and CAD drawings are being widely circulated between A/E firms, the owner, and various consultants and contractors. It is absolutely critical that this information be controlled through the development of distribution matrices and enforcement of information security policies and procedures. The information systems themselves are a potential source of compromise, as hackers can exploit the Internet connectivity of computer systems.

An often overlooked vulnerability results from the increasing percentage of companies utilizing offshore design work. A tremendous risk of compromise develops if

the information is not tightly controlled. Personnel screening standards may not be as rigid in developing nations or even in other developed nations as they are in the United States. Plans, specifications and requirements, and CAD drawings can be easily sold or transmitted to international terrorist or criminal organizations for monetary gain or ideological reasons. The result is that a project may be compromised even before construction starts.

Information security with 58% influence has the greatest influence on project life-cycle security during the design phase, followed by personnel security, 28% influence, and physical security, 14% influence (Construction Industry Institute 2004a). As in the front-end planning phase, influence is based upon the Security Practice Weightings in Appendix F rather than the number of practices by security element.

8.5.3. Procurement

Approximately 7% of security practice implementation on a project should occur in the procurement phase (Construction Industry Institute 2004a). Table 8.3 summarizes the typical participants, start and finish milestones, and typical activities and products of the procurement phase.

Table 8.3. Procurement Phase Summary

Typical Participants	Owner Personnel
	Design Contractor
	Alliance/Partner
	Vendors/Suppliers
Phase Start	Procurement Plan for Engineered Equipment
Phase Stop	All engineered equipment has been delivered to site
Typical Activities & Products	Supplier Qualification
	Supplier Inquiries
	Bid Analysis
	Purchasing
	Engineered Equipment
	Transportation
	Supplier QA/QC

In the context of industrial projects, the procurement encompasses fabrication and delivery of engineered equipment such as tanks and pressure vessels. For non-engineered equipment, procurement activities are typically included in the construction and startup phases.

Procurement is the first phase in which physical security practices outweigh personnel and information practices. This is indicative of the shift from project planning and design to project execution. The selection of security-related equipment and design and material selection of engineered equipment are key security implementation activities during the procurement phase that will have a direct impact on life-cycle security of the project.

During the procurement phase, physical security, with 41% influence has the greatest influence on project life-cycle security, followed by information security at 33%

influence, and personnel security at 26% influence (Construction Industry Institute 2004a).

8.5.4. Construction

Approximately 14 % of security practice implementation on a project should be in the construction phase (Construction Industry Institute 2004a). Table 8.4 summarizes the typical participants, start and finish milestones, and typical activities and products of the construction phase.

Table 8.4. Construction Phase Summary

Typical Participants	Owner Personnel
	Design Contractor (inspection)
	Construction Contractor and its subcontractors
	Vendors/Suppliers
Phase Start	Beginning of continuous substantial construction activity
Phase Stop	Mechanical Completion
Typical Activities & Products	Setup Trailers
	Site Preparation
	Procurement of Bulks
	Issue Subcontracts
	Construction plan for methods/sequencing
	Build facility & install engineered equipment
	Complete Punchlist
	Demobilize Construction Equipment

While less significant to overall life-cycle security than the front-end planning or design phases, the construction phase is the most complex in terms of security. Construction workers, tools and equipment, deliveries of supplies and material, laydown

and storage areas, and the physical facility being built all create a challenge to implementation of project security. Recognizing the complexity of security during the construction phase and the difficulty of adequately incorporating security into existing CII Best Practices, the Construction Site Security Guidelines in Appendix C were developed to address the implementation of project security during the construction phase. These guidelines are a rather detailed compendium of topics to be addressed when developing a jobsite security plan. They address policies, organization, access control, barriers, lighting, key control, alarms, property control, communications, and emergency planning as well as personnel security issues. The project team should review these guidelines prior to the construction phase and when developing its project security plan.

Security considerations on new construction (greenfield) projects will typically be more contractor-driven. In many cases, greenfield projects may have a lessened likelihood of sabotage and attack than projects in existing facilities, but still have many opportunities for crime.

Some greenfield projects actually have a higher likelihood of sabotage and attack. In areas that have little or no industrial development, opposition from local residents and environmental groups can be significant, resulting in greater security risks. Greenfield projects located in remote geographical areas or developing nations may also incur a greater likelihood of sabotage and attack than a project in an existing facility. For projects in existing facilities (e.g., additions or modernizations), coordination between the manager of the existing facility and the project manager for the current project is necessary in order to implement project security.

An important consideration during the construction phase is the assessment and communication of the effect of change orders. It is critical that the proposed change order be circulated among the project team and corporate security management and risk

management personnel to ensure that it will not violate the assumptions of the selected phase practices and phase risk matrix. If the proposed change order does violate the assumptions of the selected phase practices and phase risk matrix, the project team must conduct a review and adjustment of the practices and phase risk matrix prior to approval of the change order.

As with the procurement phase, in the construction phase physical security has the greatest influence on project life-cycle security with 57% influence. Personnel security, at 33% influence is second, and information security at 10% influence is third (Construction Industry Institute 2004a).

8.5.5. Startup

The startup phase requires approximately 3% of security practice implementation on a project (Construction Industry Institute 2004a). Table 8.5 summarizes the typical participants, start and finish milestones, and typical activities and products of the startup phase.

The startup phase has physical and personnel security risks analogous to that of the construction phase due to the testing, documentation, and training occurring during the phase. The relative physical security influence is greater than that of the construction phase primarily due to a reduction of influence from personnel and information security. It is in the startup phase that the consequences of a security breach increase dramatically. This is due to the introduction of feedstocks and the production of products and byproducts that may be hazardous.

Table 8.5. Startup Phase Summary

Typical Participants	Owner personnel
	Design Contractor
	Construction Contractor
	Training Consultant
	Equipment Suppliers
Phase Start	Mechanical Completion
Phase Stop	Custody transfer to user/operator (steady state operation)
Typical Activities & Products	Testing Systems
	Training Operators
	Documenting Results
	Introduce Feedstocks and obtain first product
	Handover to user/operator
	Operating System
	Functional Facility
	Warranty Work

In the start-up phase, physical security with 77% influence, is the predominant influence on project life-cycle security, followed by personnel security at 16% influence, and information security at 8% influence (Construction Industry Institute 2004a).

Chapter 9. Conclusions

As stated in Chapter 1, this research was a result of the NIST-funded study to determine best practices for project life-cycle security. The study results were used as a basis for developing a methodology of measuring the implementation of security best practices.

This chapter reviews the research objectives and findings. Conclusions from the research and recommendations are presented.

9.1. RESEARCH OBJECTIVES

The research objectives identified in Chapter 1 were:

1. Develop a Security Rating Index (SRI) to measure the implementation of security best practices in the project delivery process.
2. Validate the SRI through expert opinion and data collection
3. Establish the relationship between Threat Level, Consequence Level, and SRI
4. Establish a methodology for assessing the impact of security implementation on project outcomes such as cost and schedule performance
5. Address common security deficiencies based upon data analysis.

The Security Rating Index was developed to quantitatively assess the level of implementation of security practices for a project. The thirty-three identified security best practices were divided into their respective phase and security elements. The Practice Development Team then used the Analytic Hierarchy process to weight each practice through pairwise comparisons.

A scoring algorithm was then created to calculate SRI score based upon responses to a questionnaire utilizing a Likert-type scale. A Web-based data collection tool was used to gather project data for validation.

The SRI was validated through expert opinion and data analysis. The SRI was developed by a team of industry experts using validated construction industry Best Practices. Two gap analyses were conducted during development to ensure the SRI was an appropriate measure of security best practice implementation.

Following its deployment, a series of structured interviews of industry professionals conducted by Smith found that the SRI was easy to use, comprehensive, and beneficial to their level of security awareness (Smith 2004).

Multiple regression was used to examine the relationship between Consequence Level and SRI score. Through use of a correlation matrix, Threat Level was determined not to be related to the SRI score. Statements by Homeland Security Secretary Michael Chertoff regarding the risk-based approach to homeland security highlight the importance of focusing on consequence, rather that threat, in addressing security (Inskeep 2005). The positive correlation between Consequence Level and SRI score was found to be statistically significant. For each incremental consequence level selected, the SRI score is expected to increase by 0.985 holding all other variables constant.

Through extension of the multiple regression model, a methodology was established to assess the impact of security implementation on project outcomes such as cost and schedule performance. Project cost and schedule information is currently gathered by the Web-based data collection tool. Currently, there are not enough projects in the database to assess the relationship with regression. As the database is increasingly populated, it will become possible to determine the impact of security implementation on cost and schedule performance.

Due to the small sample size of the data collected, it was not possible to address common security deficiencies through data analysis. During the structured interviews by Smith, a common finding was that control of information, specifically specifications and design documents, was difficult due to offshoring of design work (Smith 2004).

9.2. CONCLUSIONS

Two conclusions can be drawn from this research:

- The security best practices are comprehensive and have considerable value as a checklist of security practices to be used during project planning and execution.
- The Security Rating Index provides a means for quantifying security best practice implementation and increases security awareness.

9.3. CONTRIBUTIONS

This research provides a framework for implementing security-related practices during the delivery process of industrial projects. It identifies security best practices and provides a checklist of measures to implement during project planning and execution. By focusing on the project delivery process, this research increases the likelihood that cost-effective protective measures will be implemented.

A product of the development of security best practices was the Security Rating Index. The SRI provides a quantitative means for determining the level of use of security-related practices and for assessing their impacts on key project outcomes such as cost and schedule. It is the first tool to quantify risk, consequence, and security best practice implementation. There is no other instrument in use which fully integrates security into the project delivery process.

Finally, a guide to implementing project security practices was written to facilitate the adoption of the security best practices by industry. It advances the security best practices from the realm of research to the field for implementation. The guide offers a framework for integrating security into the project delivery process in the context of likely threats facing the facility and consequences of security breaches.

9.4. RECOMMENDATIONS

While the SRI was validated through expert opinion and data analysis, additional validation could be performed to determine whether implementation of the security best practices is being assessed consistently by the questionnaire. A detailed scenario including project specifications and project team correspondence and meeting minutes could be developed and distributed to multiple project teams. The teams would answer the SRI questionnaire based upon the project scenario and information. The SRI scores for the teams could then be analyzed with ANOVA to determine if there is a difference between the mean SRI scores. If there is no statistically significant difference between the means, the questionnaire would be considered a consistent assessment of the security best practice implementation.

The security best practices that have been developed are specific to industrial sector projects. However, non-industrial sector managers have begun to adapt the practices to their sectors, as evidenced by non-industrial project information populating the CII database. A recommendation would be to develop security practices for other sectors, such as infrastructure and building projects.

While some relationships have been established between SRI score and a few explanatory variables, there has not been enough data to quantify the impact of security best practices on cost, schedule, and safety. The security questionnaire from the Web-based data collection tool should be incorporated into the CII Benchmarking program.

This would leverage the large existing user base as well as signal to the CII membership that project security is an important metric.

As discussed in Section 2.4, Risk can be defined as the product of Threat and Consequence. With a larger data set, the interaction term of (Threat x Consequence) can be regressed against SRI score to determine if there is a statistically significant relationship, i.e., if security best practice implementation increases as risk increases.

Based upon the initial finding of a relationship between respondent type and SRI score, it would be valuable to gather additional data regarding the questionnaire respondents. The questionnaire should be modified to collect information about the team used to answer the questions, such as if the owners and contractors are utilizing security management and risk management personnel when selecting Threat Level and Consequence Level or answering phase questions.

An issue raised during structured interviews of project managers was the release of SRI questionnaire information to third parties (Smith 2004). In many cases, organizational legal counsel recommended against submitting project data due to concerns that the information could be subpoenaed and used against the respondent's organization during litigation in the case of a security incident. This negatively affected the ability to collect data. In most cases, once legal counsel was informed that: (1) the information was confidential and not subject to the Freedom of Information Act, and (2) completing the SRI questionnaire actually demonstrates the intent to implement Security Best Practices, legal counsel approved project data entry. It is important to address this concern in the guide to implementing project security practices as well as on the Web-based data collection tool home page.

Finally, it is recommended that the use of the security best practices be expanded to an audience broader than CII member organizations, with the goal of industry-wide acceptance.

Appendices

APPENDIX A. COMMITTEE MEMBERSHIP

Steering Team

Name	Position	Company
Stretch Dunn	Director of Federal Programs	BE&K, Inc. (Retired)
Charles Poer	Business Unit Manager	Zachry Construction Co.
Jim Porter	Vice President	E. I. DuPont de Nemours & Co., Inc.
David Syphard	Vice President	Jacobs Facilities, Inc.
Bob Chapman	Economist	NIST
Chuck McGinnis	Facilitator	Executive VP/COO, Fru-Con Corp. (Retired); Dir. of Civil Works, US Army Corps of Engineers (Retired); Research Director, CII (Retired)
Steve Thomas	Associate Director	CII

Practice Development Team

Core Team		
Name	**Function**	**Company**
Chuck McGinnis	Facilitator	CII (Retired)
Jay Toadvine	Program Manager	Fluor Corp.
Michael Spight	Corporate Security Manager	Black & Veatch/TRC Companies
John Brady	Corporate Security Manager	ConocoPhillips Co.
Walter Lisiewski	Business Unit Manager	Jacobs Facilities, Inc.
Michael Hewitt	Plant Operation Manager	E. I. DuPont de Nemours & Co., Inc.
Gary Staton	Risk Management Specialist	E. I. DuPont de Nemours & Co., Inc.

Practice Development Team

Ex Officio		
Name	**Function**	**Company**
Steve Thomas	Principal Investigator	CII
Bob Chapman	Sponsor	NIST
MAJ Jonathan Sylvie	Graduate Research Assistant	US Army
Sang-Hoon Lee	Analyst	CII
1LT Benjamin Matthews	Graduate Research Assistant	US Air Force
Roger Snyder	CII Education Committee	US Department of Energy

Subject Matter Experts		
Name	**Function**	**Company**
Edd Gibson	Pre-Project Planning & Alignment	University of Texas
Richard Tucker	Design Effectiveness	University of Texas
James O'Connor	Constructability & Planning for Startup	University of Texas
Lansford Bell	Materials Management	Clemson University

APPENDIX B. RESULTS OF PRACTICE MAPPING

	Security Element		
	Physical	**Personnel**	**Information**
Front-end Planning	Security Stakeholders on P3 Team (AI #1)[2]		
		Social Issues (B8)[1]	
			CADD/Model Requirements (M1)[1]
	Operating Philosophy (A3)[1]		
		Training Requirements for Operational Facility (P6)[1]	
			Document Control Systems (M3)[1]
	Reliability Philosophy (A1)[1]		
	Affordability/Feasibility (B4)[1]		
	Affordability/Feasibility (7-3)[5]		
	Future Expansion Considerations (B6)[1]		
	Technology (C1)[1]		
	Processes (C2)[1]		
	Project Objectives Statement (D1)[1]		
	Objectives with Security Delineated (AI #8)[2]		
	Effective Communication (AI #4)[2]		
	Clear Priorities (AI #3)[2]		
	Project Design Criteria (D2)[1]		
	Project Design Criteria (7-3)[5]		
	Site Characteristics (D3)[1]		
	Lead/Discipline Scope of Work (D5)[1]		
	Process Simplification (E1)[1]		
	Design/Material Alternates Considered (E2)[1]		
	Design/Material Alternates Considered (7-3)[5]		

	Security Element		
	Physical	**Personnel**	**Information**
Front-end Planning	Site Location (7-3) [5] Permit Requirements (F4)[1] Fire Protection & Safety Considerations (F6)[1] Plot Plan (G8)[1] Plot Plan (7-3) [5] Equipment Status (H1)[1] Civil/Structural Requirements (I1)[1] Architectural Requirements (I2)[1] Water Treatment Requirements (J1)[1] Loading/Unloading/Storage Facilities Requirements (J2)[1] Substation Requirements Power Sources Ident. (K4)[1] Instrument & Electrical Specifications (K6)[1] Procurement Procedures and Plans (L2)[1] Engineering/Construction Plan & Approach (P2)[1] Engineering/Construction Plan & Approach (7-3)[5] Pre-Commissioning. Turnover Sequence Requirements (P4)[1] Startup Requirements (P5)[1] PEP incorporates security (I-1) [4] PEP incorporates security (7-3)[5] Security input into planning (I-2) [4]	Design Effectiveness Criteria (RS8-1)[3]	
	Procurement/Logistics Procedures and Plans/Strategies (7-3)[5]	Procurement/Logistics Procedures and Plans/Strategies (7-3)[5]	Procurement/Logistics Procedures and Plans/Strategies (7-3)[5]

	Security Element		
	Physical	Personnel	Information
Front-end Planning	Security input into planning (7-3)[5] Estimate Startup Security Costs (2-B)[7] Identify Startup Security Objectives (3-A)[7] Assign Startup Security Stakeholders (3-C)[7] Reconcile Startup Logic with Security Plan (3-D)[7] Acquire O&M Input for Security Systems (3-E)[7] Identify Startup Security Risks (3-F)[7] Identify Startup Security Procurement Requirements (3-H)[7] Refine Startup Security Costs (3-I)[7] Develop Startup Security Plan (3-X)[7] Develop Construction Site Security Plan (CSS)[6]	Security input into planning (7-3)[5] Estimate Startup Security Costs (2-B)[7] Identify Startup Security Objectives (3-A)[7] Assign Startup Security Stakeholders (3-C)[7] Reconcile Startup Logic with Security Plan (3-D)[7] Acquire O&M Input for Security Systems (3-E)[7] Identify Startup Security Risks (3-F)[7] Identify Startup Security Procurement Requirements (3-H)[7] Refine Startup Security Costs (3-I)[7] Develop Startup Security Plan (3-X)[7] Develop Construction Site Security Plan (CSS)[6]	Security input into planning (7-3)[5] Estimate Startup Security Costs (2-B)[7] Identify Startup Security Objectives (3-A)[7] Assign Startup Security Stakeholders (3-C)[7] Reconcile Startup Logic with Security Plan (3-D)[7] Acquire O&M Input for Security Systems (3-E)[7] Identify Startup Security Risks (3-F)[7] Identify Startup Security Procurement Requirements (3-H)[7] Refine Startup Security Costs (3-I)[7] Develop Startup Security Plan (3-X)[7] Develop Construction Site Security Plan (CSS)[6]

	Security Element		
	Physical	**Personnel**	**Information**
Design	Design approaches and/or alternatives consider security (I-5); (II-2); (II-5)[4] Site layout considers security (I-6) [4] Consider security aspects of construction accessibility for retrofit (II-6)[4] Update Startup Security Risks (4-I)[7] Ensure Security Addressed in O&M Training Plan (4-J)[7] Refine Startup Security Costs (4-N)[7] Update Startup Security Plan (4-X)[7] Refine Construction Site Security Plan (CSS)[6]	Update Startup Security Risks (4-I)[7] Ensure Security Addressed in O&M Training Plan (4-J)[7] Refine Startup Security Costs (4-N)[7] Update Startup Security Plan (4-X)[7] Refine Construction Site Security Plan (CSS)[6]	Update Startup Security Risks (4-I)[7] Ensure Security Addressed in O&M Training Plan (4-J)[7] Refine Startup Security Costs (4-N)[7] Update Startup Security Plan (4-X)[7] Refine Construction Site Security Plan (CSS)[6]
Procurement		Materials Management Personnel Security Procedures Training (7-3)[5] Background Investigations/Personnel Screening for Site Personnel (7-3)[5]	
Construction	Assess & Communicate Startup Security Effects from Changes (4-B)[7] Finalize Startup Security Risks (6-F) [7] Finalize Startup Security Plan (6-X)[7] Implement Construction Site Security Plan (7-3)[5] Implement Construction Site Security Plan (CSS)[6]	Assess & Communicate Startup Security Effects from Changes (4-B)[7] Finalize Startup Security Risks (6-F) [7] Finalize Startup Security Plan (6-X)[7] Implement Construction Site Security Plan (7-3)[5] Implement Construction Site Security Plan (CSS)[6]	Assess & Communicate Startup Security Effects from Changes (4-B)[7] Finalize Startup Security Risks (6-F)[7] Finalize Startup Security Plan (6-X)[7] Implement Construction Site Security Plan (7-3)[5] Implement Construction Site Security Plan (CSS)[6]

	Security Element		
	Physical	**Personnel**	**Information**
Startup	Implement Startup Security Plan (7-A)[7] Implement Construction Site Security Plan (CSS)[6]	Implement Startup Security Plan (7-A)[7] Implement Construction Site Security Plan (CSS)[6]	Implement Startup Security Plan (7-A)[7] Implement Construction Site Security Plan (CSS)[6]

Phase and Source Key
[1] PDRI, IR 113-2
[2] Alignment, IR 113-3
[3] Design Effectiveness, RS 8-1
[4] Constructability, Pub 34-1
[5] Materials Management, IR 7-3
[6] Construction Site Security Plan
[7] Planning for Startup, IR 121-2

APPENDIX C. CONSTRUCTION SITE SECURITY GUIDELINES

The owner is ultimately responsible for determining the measures that need to be implemented; this is especially true in renovation or addition projects, where the project occurs in or adjacent to an active facility.

Security considerations on "greenfield" projects will typically be more contractor-driven. "Greenfield" projects may have a lessened likelihood of sabotage and attack than projects in existing facilities, but still have many opportunities for crime

The success of construction site security will be strongly contingent on the role management takes in the project (Broder 2000).

I. Policy and Program
   a. Has a security policy been established?
   b. Has the policy been published?
      i. A crucial aspect of construction site security is establishing a written security policy. The security policy defines objectives and priorities, ensuring alignment between owner and contractor.
   b. Has the policy been agreed to between the owner and contractor?
      i. While the project owner must approve the security policy, the contractor must concur with all elements, since he will be responsible for much of the daily oversight and enforcement while the construction site is active.
      ii. Any exceptions to the policy must be resolved between the owner and contractor. This is crucial in cases where the construction site security plan will result in schedule or budget impact.
   c. Is the contractor's security supervisor accessible to the owner's security manager?
      i. These individuals will be responsible for ensuring compliance with their employers' objectives. They should have regular contact during the course of the construction project.
   d. What are the consequences of non-compliance?
      i. If the owner's security manager determines that the construction security plan is being violated, there should be clearly identified consequences.
         1. Disciplinary procedures should be specified in writing, preferably in the construction contract.
         2. Enforcement measures can range from written notices for minor infractions to monetary penalties for repeated offenses.
         3. Non-compliance with the construction security plan is at least as serious as non-compliance with material specifications or other contract specifications.

II. Organization
   a. Has the contractor appointed a full-time security supervisor?
      i. It is crucial to have a security supervisor on site at all times. If the contractor does not have an employee on site whose sole responsibility is security, he should appoint a person who will be on site for the majority of the project as security supervisor. An example would be the construction superintendent or a foreman.
      ii. What is the security chain of command?
         1. The designated security supervisor must have access to owner's security manager, regardless of who he reports to for non-security related issues.
   b. Are there security shifts?
      i. When the construction site is not operational, who assumes security responsibilities? Security is a full-time responsibility.
         1. On renovation/addition projects, the owner's full-time security personnel may assume responsibility after hours. If this is the case, have written procedures for handoff of security responsibilities.
         2. On Greenfield projects, this may not be possible. Have a written contract for professional security personnel or have other trained contractor personnel secure the site.
   c. Have security personnel received security training?
      i. Security training and certification is available from organizations such as the American Society for Industrial Security (ASIS) - http://www.asisonline.org/, which sponsors classes and conferences, as well as on-line coursework
   d. Are written reports made for incidents?
   e. Has there been a background investigation performed for security personnel?
   f. Are there periodic inspections of the construction site security by owner personnel?
   g. Does the security supervisor maintain contact with local law enforcement agencies to keep abreast of criminal activities and potential disorder in the community (Broder 2000)?

III. Access Control
   a. Is 100% identification required of all persons entering the construction site?
      i. Are identification badges issued?
         1. Photo identification badges are preferred. They can also incorporate the following security measures:
            a. Proximity Card
            b. Magnetic Strip
            c. Radio Frequency Identification Tag (RFID)
            d. Smart Card

            e. Biometric information
        ii. Wearing enforcement?
        iii. A written issue/return process is necessary
            1. Badge recipients must sign an acknowledgment that they will report any lost badges
b. Is the personnel and vehicle search policy clearly posted at all entrances?
c. Who is responsible for controlling access to the site?
d. What is the visitor registration procedure?
    i. Are visitors escorted at all times while on the construction site?
e. How is access between the construction site and the operational facility controlled?
f. How are vehicles admitted to construction site?
    i. There should be a written policy stating vehicle access procedures and who is the approving authority
        1. An approved vehicle access roster should be kept by the gate guard(s)
            a. Approved vehicles that need to access the site for more than a day should be registered and provided a tag
        2. Worker vehicles should have a designated parking area outside the construction site.
        3. Policies and procedures should include
            a. Employees
            b. Visitors
            c. Deliveries
            d. Material and equipment removal

IV. Barriers
a. Is there a continuous fence around the entire construction site?
    i. Permanent vs. non-permanent
    ii. Eight feet high, two-inch square mesh, 11-guage or heavier wire (Broder 2000)
b. Gates (Broder 2000)
    i. In good repair
    ii. Gates same height and construction as fence?
    iii. Open only when required for operations?
    iv. Locked other times?
    v. Equipped with alarm (how many?)
    vi. Guarded when open?
    vii. Under surveillance when open? How?
    viii. Alternate access gates should be installed, but are not required to be active at all times
        1. For emergency egress
        2. Organized labor considerations, i.e., if main gate is blocked by striking workers or protestors

V. Lighting
   a. Is the entire perimeter of the construction site lighted?
      i. Both sides of the fence must be lighted so that an intruder may be detected at 100 meters (Broder 2000)
      ii. Any access gates must be illuminated
   b. Lights must be checked daily, prior to darkness, so that deficiencies may be corrected prior to their use.
   c. The power supply for perimeter lighting must be inaccessible or tamper-proof. For example, if using light tower/generator set trailers, they must be secured in place and the control doors locked.
   d. Switches and controls (Broder 2000)
      i. Protected?
      ii. Weatherproof and tamper resistant?
      iii. Accessible to security personnel?
      iv. Inaccessible from outside the perimeter barrier?
   e. Materials and equipment in receiving, shipping, and storage areas adequately lighted (Broder 2000)?
      i. If laydown areas are geographically separate from the construction site, they must have the same security measures as the construction site.

VI. Locks and Keys
   a. Is the contractor security supervisor responsible for control of locks and keys?
      i. The contractor security supervisor should have overall authority for the issue and replacement of all locks and keys for the construction site.
         1. If the construction site is within an existing facility, the contractor should control the site, even though he may not be able to access it without passing through the owner's security.
         2. Owner personnel should not be allowed to access the construction site without contractor security supervisor approval.
   b. The lock and key control procedures should be in writing
      i. All key recipients should sign a key control register
         1. Non-employees should not be allowed to sign for keys
         2. Key recipients must sign an acknowledgment that they will report any lost keys and that they may not duplicate any keys
      ii. Master keys should not be identifiable as such (Broder 2000)
      iii. Spare locks and keys should be double locked (i.e. in a locked container in a locked room)

c. Padlocks should be locked to a hasp or staple when door or gate is open to prevent substitution (Broder 2000).
d. Locks on inactive doors or gates should be checked regularly for evidence of tampering (Broder 2000).

VII. Alarms
a. Intrustion Detection
    i. What assets should be protected?
        1. Three general classes (POA Publishing 2003)
            a. Perimeter or point of entry
            b. General Area
            c. Object
b. Fire
    i. Does it comply with National Fire Protection Association (NFPA) Code 72, National Fire Alarm Code
    ii. What sensor type(s) are appropriate for the construction site?
        1. Detecting a fire at an early stage is critical. Certain construction materials or locations may necessitate different sensors because of the nature of potential fires.
        2. Sensors (POA Publishing 2003)
            a. Thermal (heat)
            b. Smoke (photoelectric)
            c. Flame (ultraviolet)
            d. combination
            e. Fusable link
            f. Water flow indicator
c. How will the alarms be monitored?
    i. Central monitoring
        1. What is the primary method of transmission?
            a. Some alternatives available include: wire, RF, microwave, laser, cellular telephone, satellite(POA Publishing 2003).
            b. Is there an alternate method of communication if the primary method is disabled or inoperative?
    ii. Local monitoring
        1. A consideration of local monitoring is that someone must be on-site 24/7. If the site is remote or located in a high-crime area, remote monitoring is recommended, even if the site is guarded.

VIII. Communications
a. Are there separate communications for security and emergency use (Broder 2000)?
    i. Telephone
        1. Are telephones Caller ID capable?

ii. Radio
    1. If the radio is shared with other users, security should be able to override them in emergency situations
    2. Some manufacturers offer handheld radios equipped with a button that sends an emergency duress signal, including unit identification, to a central monitoring station (Garcia 2001)
iii. Cellular

b. Is there a means of contacting guard on patrol immediately? How? (Broder 2000)
c. What is the procedure for contacting local police and fire departments
    i. Verify if 911 service or similar service is available in the location of the construction site
    ii. Contact the local police and fire departments to determine if there a direct number to contact emergency dispatchers
        1. Do emergency service responders have another preferred method of contact?
d. How will employees on site be alerted to an emergency?
    i. Ensure that there are both visual and audible signals
        1. Visual – strobe light, flashing lights on site
        2. Audible – intercom/public address announcement, klaxon, siren

IX. Property Control

a. Has a property control policy been established?
    i. Is it published?
b. Who approves the issue of property?
    i. Issue of equipment, material, and tools should require a signed authorization from a designated authority.
    ii. When the designated authority is the intended recipient, a higher level authority must approve the issue.
    iii. Property transactions should be audited by a third party, other than security (Broder 2000)
c. How is access controlled to the construction site?
    i. All gates should be guarded as per Section III – Access Control
    ii. Workers' personal vehicles should not be allowed to access the construction site – a separate parking location should be designated
d. Vehicles departing the construction site should undergo inspection
        1. Determine an frequency of inspection that balances security with job performance
        2. Authorization for vehicles to depart with property (including salvage material) must be delivered to gate guards prior to vehicles arriving at gate

a. It is important that the designated property control authority approve each item departing the construction site

e. Tools and equipment
    i. Employees must sign for tools and equipment issued
        1. Issuing authority must specify the period of issue
            a. Must not be open-ended, i.e., when "job is complete"
            b. Follow up on items signed out past due-date
    ii. Tools and pilferable items must be secured in locked cages or rooms
    iii. Inventories must be conducted regularly and losses reported
f. Loss Reporting
    i. All losses must be reported
    ii. Property issuing authority must conduct an investigation and provide findings to management

X. Emergency Planning

a. Has an emergency response plan been developed?
    i. Is it published?
        1. Responses to:
            a. Weather, i.e. flood, tornado, hurricane
            b. Fire
            c. Explosion
            d. Chemical release
            e. Bomb threat
            f. Terrorist acts
        2. Responsible individuals designated (Broder 2000)
        3. Responsibilities delineated
b. Are emergency response drills rehearsed?
    i. Drills must me conducted for key leaders as well as all personnel on the construction site
        1. Leader rehearsals can consist of walkthroughs or "what-if" scenarios
        2. 100% personnel drills should involve a scenario and response, including evacuation of the construction site
c. Have critical features of plant and equipment been identified? (Broder 2000)
    i. Are they protected by barriers, access control, and lighting?
d. Has the emergency response plan been coordinated with:
    i. Local emergency responders
        1. Police
        2. Fire
        3. Medical

ii. Disaster Responders
1. FEMA

e. Has a disaster recovery plan been developed?
i. What resources are required?

XI. Personnel

a. Employment Application
i. All prospective employees should fill out a written application and sign it to certify that the information is correct
ii. Candidates for a position should be interviewed prior to receiving an employment offer

b. Background Investigation
i. Does prospective employee have a criminal record?
ii. Verify previous employment
1. Employer
2. Dates of employment
3. Title and responsibilities
4. Characterization of employment
5. Reason for resignation/termination
iii. Verify education and training
iv. Examine medical record
1. Does prospective employee have a history of drug abuse?
2. Does applicant have previous work injuries or occupational illnesses?
v. Additional screening for positions of increased responsibility
1. Supervisory
2. Purchasing
3. Inventory Control
4. Cleaning/Housekeeping Personnel
a. They have access to most areas of the construction site

c. Are supervisors trained to look for indicators of abuse?
i. The indicators fall into three categories: performance, behavior, and general (Fay 2002).
1. Performance
a. Frequent no-shows and lateness
b. Unexplained absences from construction site (15-30 minutes every 4-5 hours)
c. Frequent and long visits to the restroom
2. Behavior
a. Unexplained change in disposition in a short period
i. A mood swing may be due to drug use. A change from a “down” mood to an “up”

mood may be because the employee took a drug. A change in the opposite direction may be because the drug is wearing off.

b. Weight loss and/or loss of appetite
c. Nervousness
    i. Nervousness may manifest itself in a non-smoking employee starting to smoke or a smoker increasing the amount of smoking
d. Reluctance to show the arms or legs.
    i. Most, if not all, employees on a construction site will be wearing long sleeves and long pants for protective purposes. In this case, blood spots on pants legs and sleeves may indicate drug usage.
e. Withdrawal symptoms
    i. Common symptoms of a drug wearing off are runny nose, sniffling, bloodshot eyes, trembling, unsteady gait, and a general tiredness
f. Active symptoms
    i. The employee is under the influence of a drug on the construction site. Symptoms will differ for depressants and stimulants.
        1. Stimulants. Hyperactive, jumpy, energetic, fast moving, and talking in a rapid, nonstop manner.
        2. Depressants. Slow-moving, distracted, and talking in a slurred manner.

3. General
    a. Admission of drug use to seek help or to explain poor performance.
    b. Possession of drugs without a valid prescription or medical reason.
        i. Prescription drugs or illegally manufactured drugs can be abused by an employee.
        ii. Common forms of drugs include pills, tablets, capsules, powders, pastes, leafy materials, gum like substances, and liquids.

APPENDIX D. SECURITY QUESTIONNAIRE

#	Security was a consideration in:	Phase					Security Element		
		FEP	D	P	CON	SU	Phy	Per	Info
1	Establishing project objectives (e.g., reliability and operating philosophy, affordability and feasibility, constructability, future expansion, etc.)	X					X		
2	Preparation of the specifications and requirements (e.g., civil/structural, architectural, water treatment, loading/unloading/storage facilities, substation/power sources, instrument & electrical, etc.)	X	X				X		X
3	Developing and evaluating design criteria (based on vulnerability assessment)	X	X				X		
4	Developing project scope	X					X		
5	Design and material selection		X	X			X		
6	Developing the engineering/construction plan & approach	X	X	X	X		X		
7	Developing the procurement/materials management procedures and plans (e.g., warehousing, inventory control, key & lock control, hazardous materials)	X	X	X			X	X	X
8	Prequalification/selection of suppliers	X	X	X				X	
9	Developing the pre-comm/turnover sequence/startup requirements/objectives	X	X				X	X	X
10	Technology and process selection	X	X				X		
11	Determining required site characteristics and location	X					X		
12	Preparing the permitting plan	X					X	X	
13	Developing the plot plan (i.e., layout, accessibility, gate configuration, etc.) - retrofit & greenfield	X	X				X	X	X
14	Evaluation of various personnel issues (e.g., education/training, safety and health considerations)	X					X		
15	Development of a distribution matrix for document control (e.g., drawings, project correspondence, CAD, as-built documents)	X	X					X	
16	The project team was in alignment concerning the importance of security issues identified in the project objectives.	X	X		X	X	X	X	X
17	Security-related equipment was defined and purchased with appropriate input (e.g., O&M, Security Manager, etc.)		X	X			X	X	X
18	Identifying stakeholders for the project team (based on vulnerability assessment)	X					X	X	X

#	Security was a consideration in:	Phase					Security Element		
		FEP	D	P	CON	SU	Phy	Per	Info
19	Establishing priorities between cost, schedule, and required project features (based on vulnerability assessment)	X	X				X	X	X
20	Identifying and resourcing startup requirements (e.g., procurement, personnel, training)	X					X	X	X
21	Screening of the project team for appropriate level of clearance	X						X	
22	Screening of contractor/subcontractor employees/delivery personnel for appropriate level of clearance	X	X	X	X	X		X	
23	Identifying startup risks	X	X	X	X		X	X	X
24	Developing/implementing startup security plan	X	X	X	X		X	X	X
25	Developing system startup plan (reconciled with security plan)	X	X				X	X	X
26	Developing training plans (e.g., job site, O&M, startup)	X	X	X	X	X	X	X	X
27	Assessing & communicating effects from change orders				X	X	X	X	X
28	Developing/implementing construction site security plan (e.g., fire protection and safety considerations, egress, emergency responder access, process shutdown)				X	X	X	X	X
29	The project had a designated site security coordinator				X	X	X	X	X
30	Developing business partnerships/alliances	X	X	X	X	X	X	X	X
31	Project information systems security plan (e.g., firewalls, wireless security, passwords, access controls)		X	X	X	X			X
32	Security breaches/incidents were routinely investigated				X	X			
33	Developing emergency response plan in coordination with local authorities				X	X			

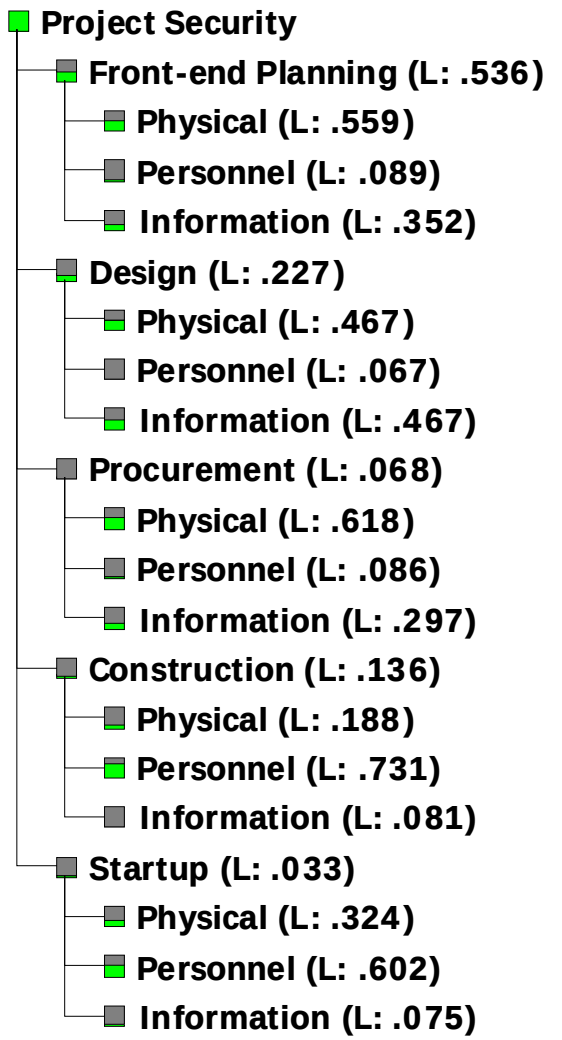
APPENDIX E. CONSOLIDATED RISK PROFILES

	New Construction, Green Field, Grassroot Risk Item	Renovation, Retrofit, Add-on, Modernization Risk Item
Front-end Planning	1. Premature Information Disclosure/Compromise 2. Document Theft 3. Cyber Attack 4. Activist and/or Local Opposition/Disruptions	1. Activist and/or Local Opposition/Disruptions 2. Attack on facility 3. Sabotage of facility 4. Cyber attack 5. Premature Information Disclosure/Compromise
Design	1. Information Disclosure/Compromise (incl. theft and sabotage) 2. Competitor Sabotage (e.g. hiring away employees, bribery, disloyal employees) 3. Cyber Attack	1. Information Disclosure/Compromise (incl. theft and sabotage) 2. Competitor Sabotage (e.g. hiring away employees, bribery, disloyal employees) 3. Cyber Attack 4. Activist and/or Local Opposition/Disruptions
Procurement	1. Material Pilferage/theft (onsite or during transportation) 2. Material Destruction (onsite or during transportation) 3. Activist and/or Local Opposition/Disruptions 4. Information Disclosure/Compromise 5. Competitor Sabotage (e.g. by talking to your vendors) 6. Cyber Attack 7. Employee disloyalty	1. Material Pilferage/theft (onsite or during transportation) 2. Material Destruction (onsite or during transportation) 3. Information Disclosure/Compromise 4. Competitor Sabotage (e.g. by talking to your vendors) 5. Cyber Attack 6. Employee disloyalty 7. Activist and/or Local Opposition/Disruptions
Construction	1. Pilferage/theft 2. Sabotage (incl. terminated employees) 3. Activist and/or Local Opposition/Disruptions 4. Terrorist attack 5. Information Disclosure/Compromise 6. Cyber Attack	1. Pilferage/theft 2. Sabotage (incl. terminated employees) 3. Activist and/or Local Opposition/Disruptions 4. Terrorist attack 5. Information Disclosure/Compromise 6. Cyber attack 7. Change in operational facility security to limit of retrofit area is difficult to maintain

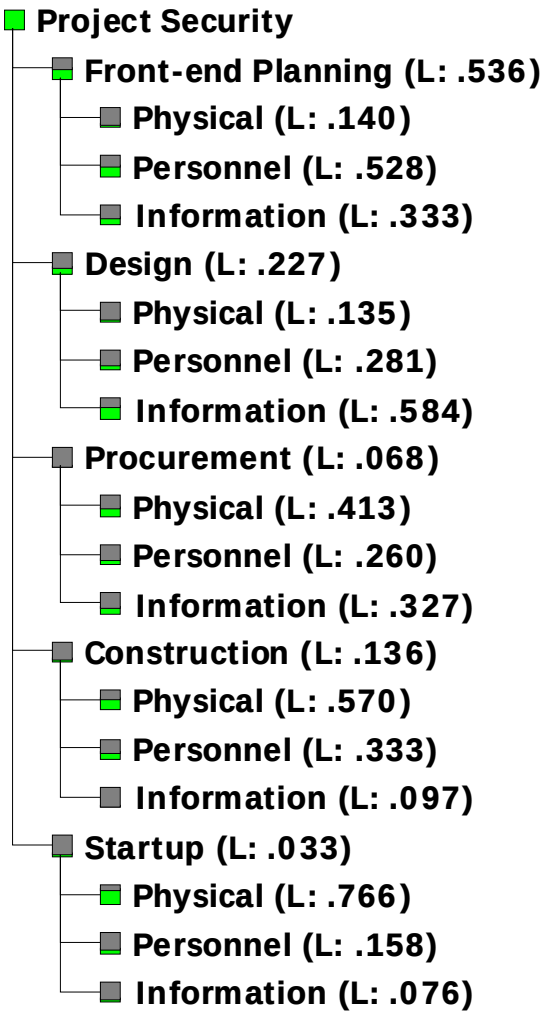
	New Construction, Green Field, Grassroot Risk Item	Renovation, Retrofit, Add-on, Modernization Risk Item
Startup	1. Pilferage/theft 2. Sabotage (incl. terminated employees) 3. Activist and/or Local Opposition/Disruptions 4. Terrorist attack 5. Change in project and security teams creates opportunity to exploit security 6. Information Disclosure/Compromise	1. Pilferage/theft 2. Sabotage (incl. terminated employees) 3. Activist and/or Local Opposition/Disruptions 4. Terrorist attack 5. Change in project and security teams creates opportunity to exploit security 6. Information Disclosure/Compromise

APPENDIX F. INITIAL AND FINAL PHASE AND SECURITY ELEMENT WEIGHTS

Initial Weights (09/04/03)

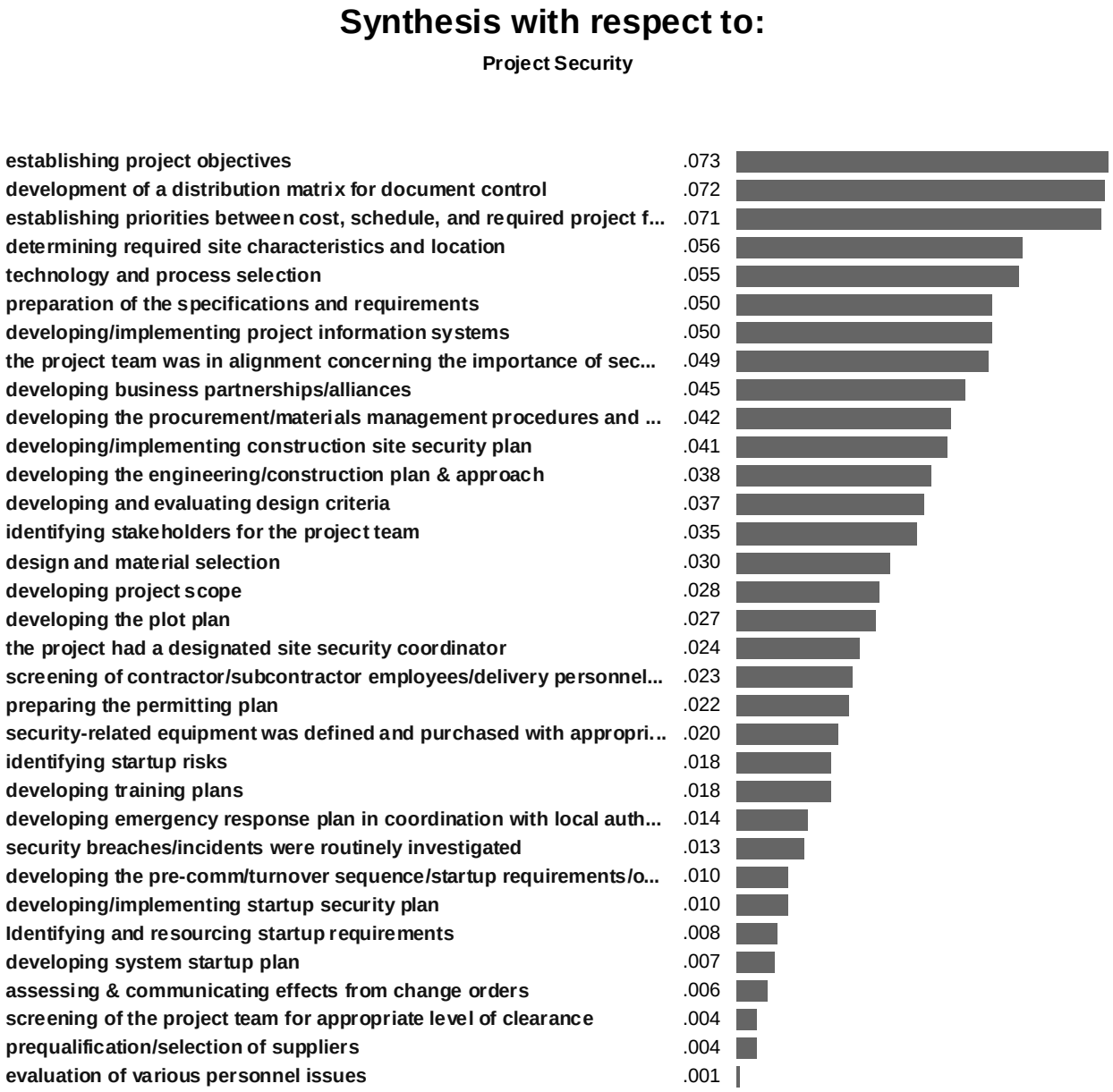


Final Weights (09/28/03)

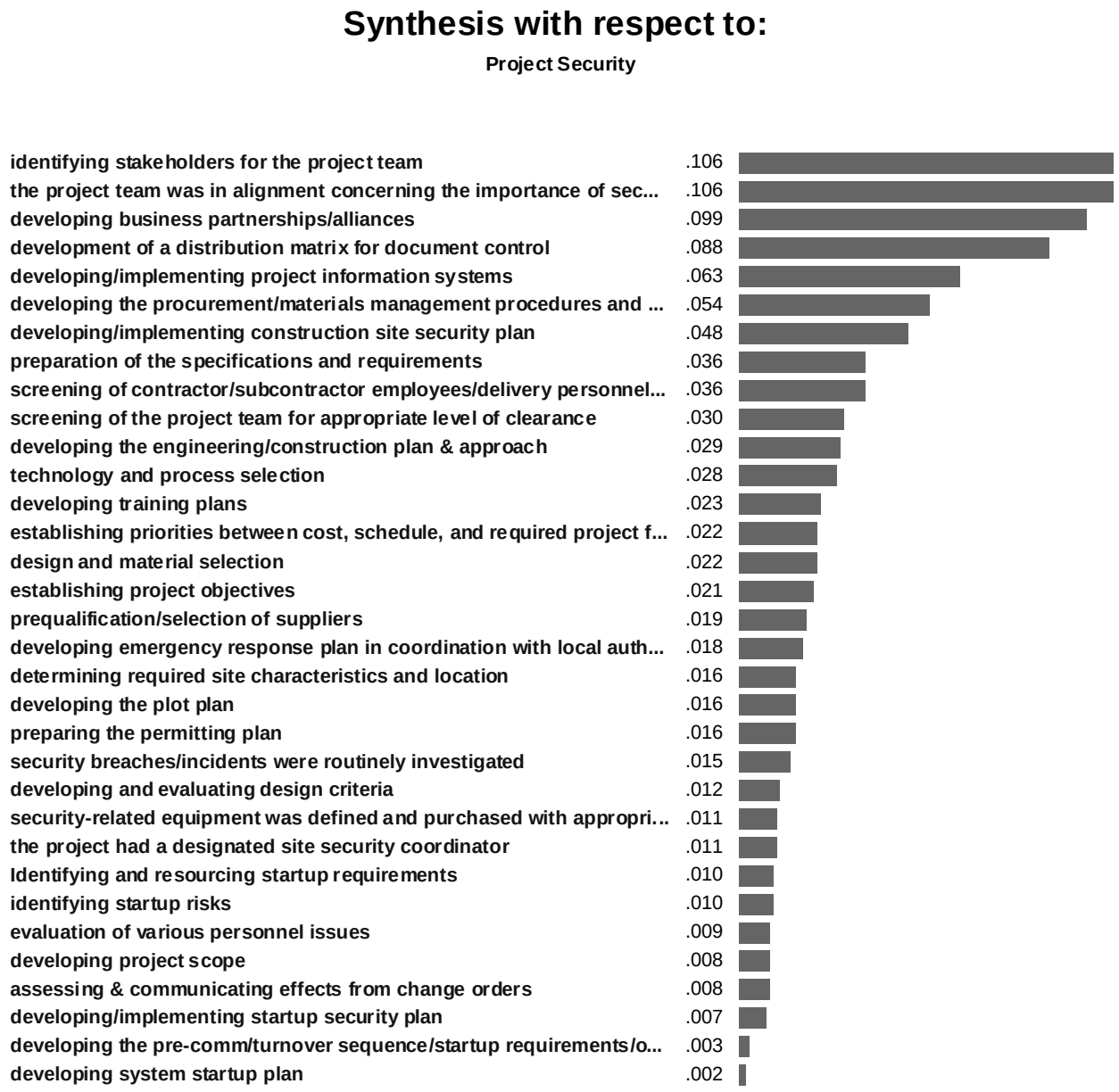


APPENDIX G. INITIAL AND FINAL AHP OUTPUT

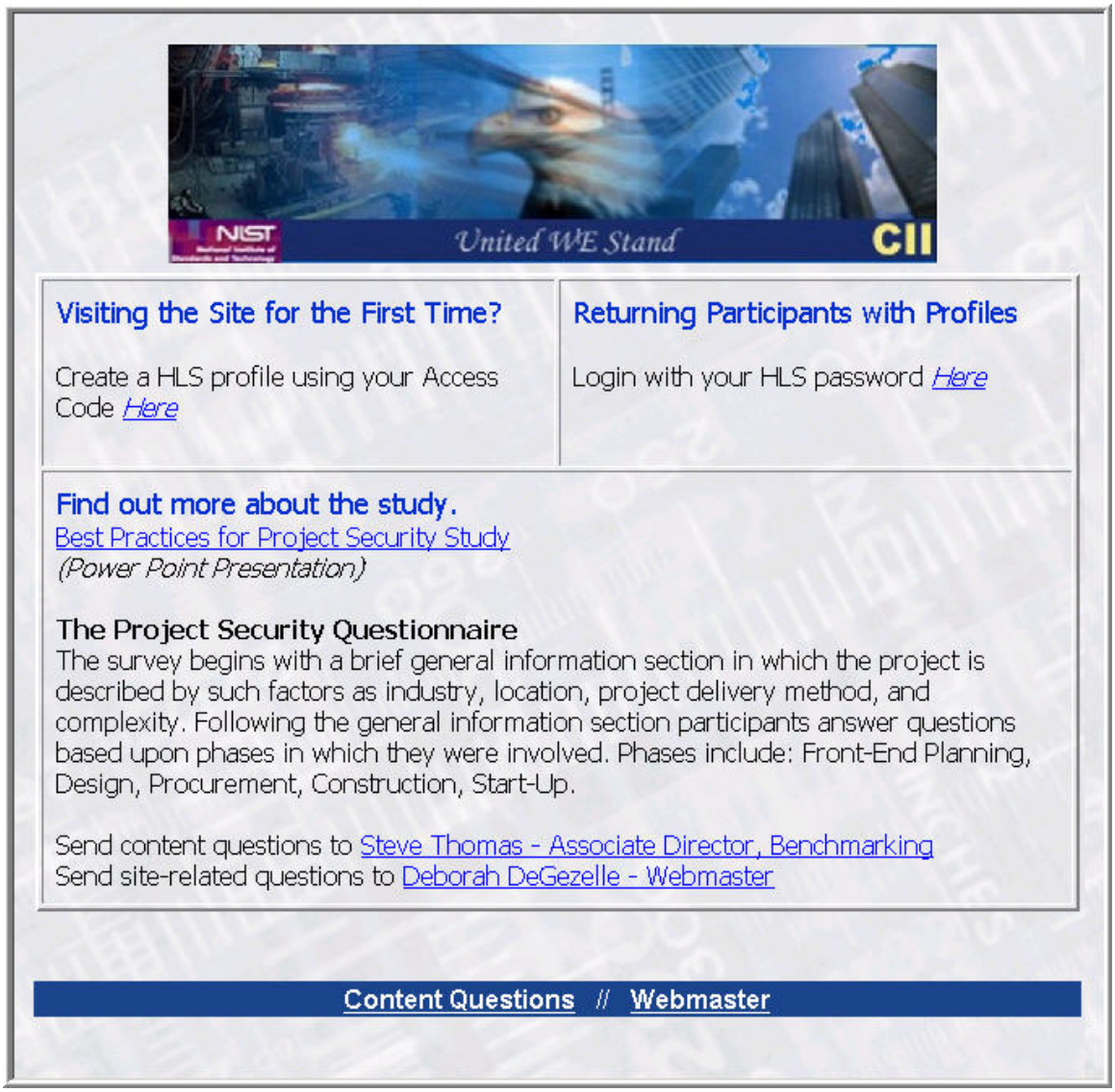
Initial AHP Output



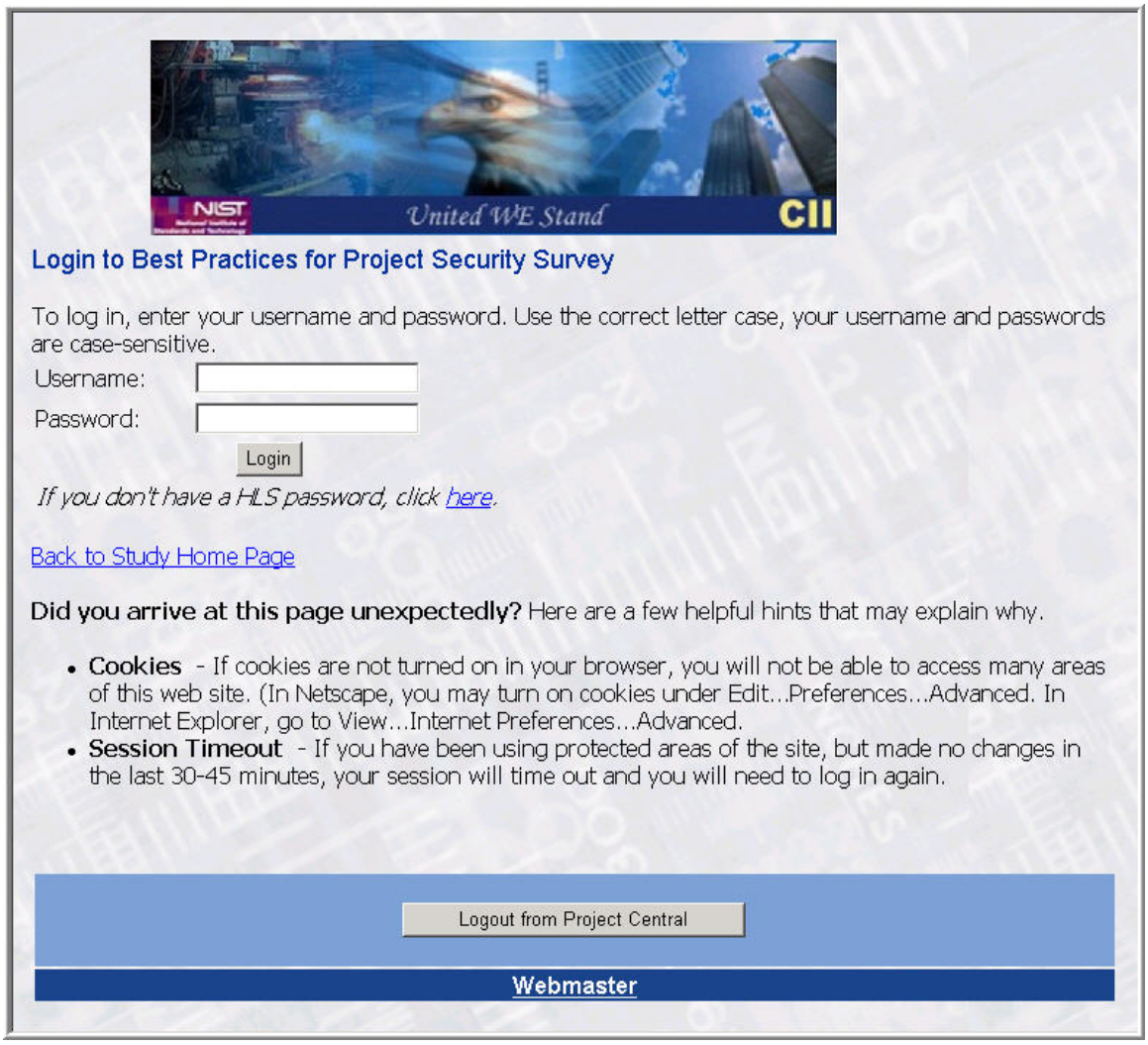
Final AHP Output



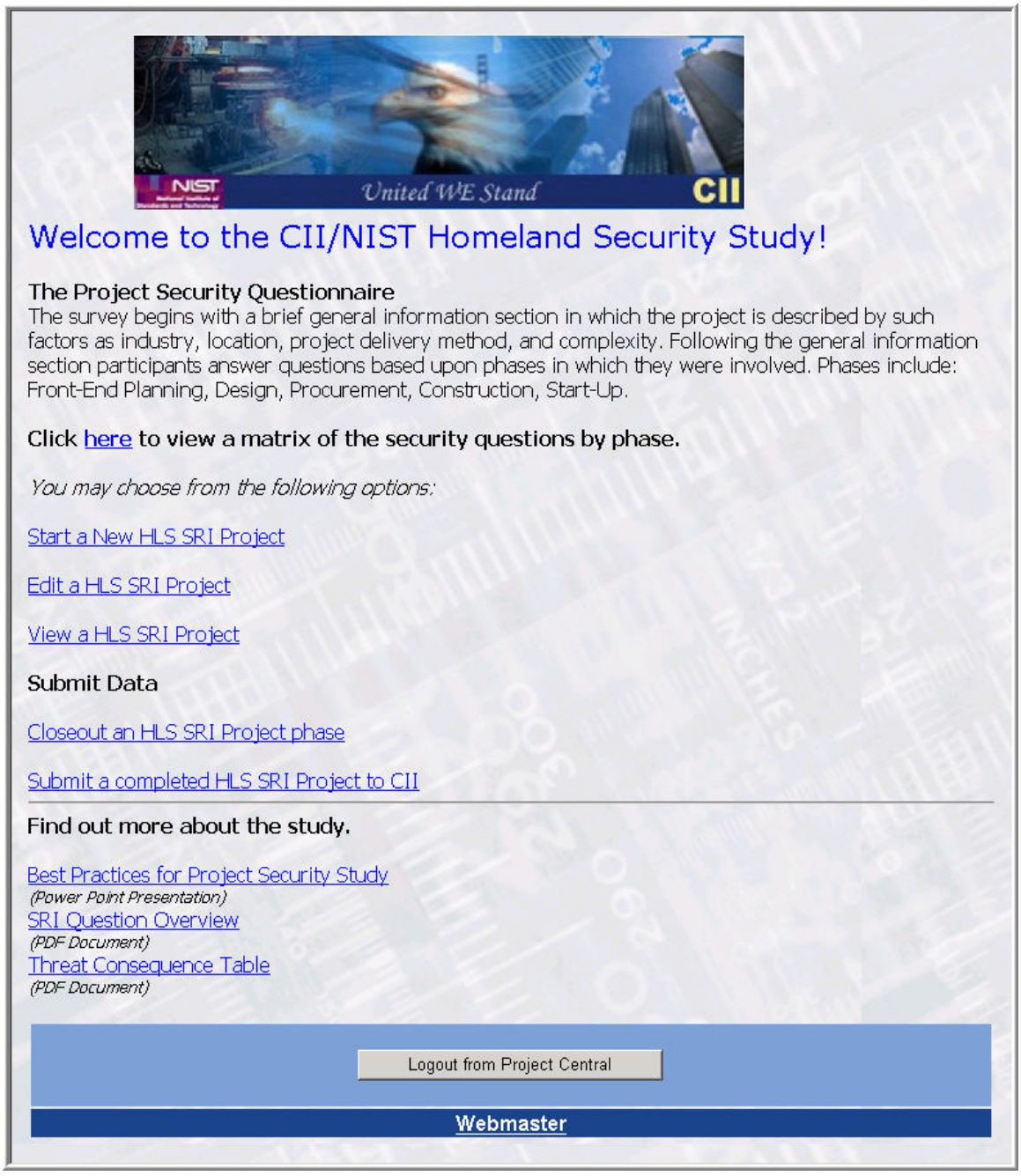
APPENDIX H. WEB-BASED DATA COLLECTION TOOL SCREENSHOTS



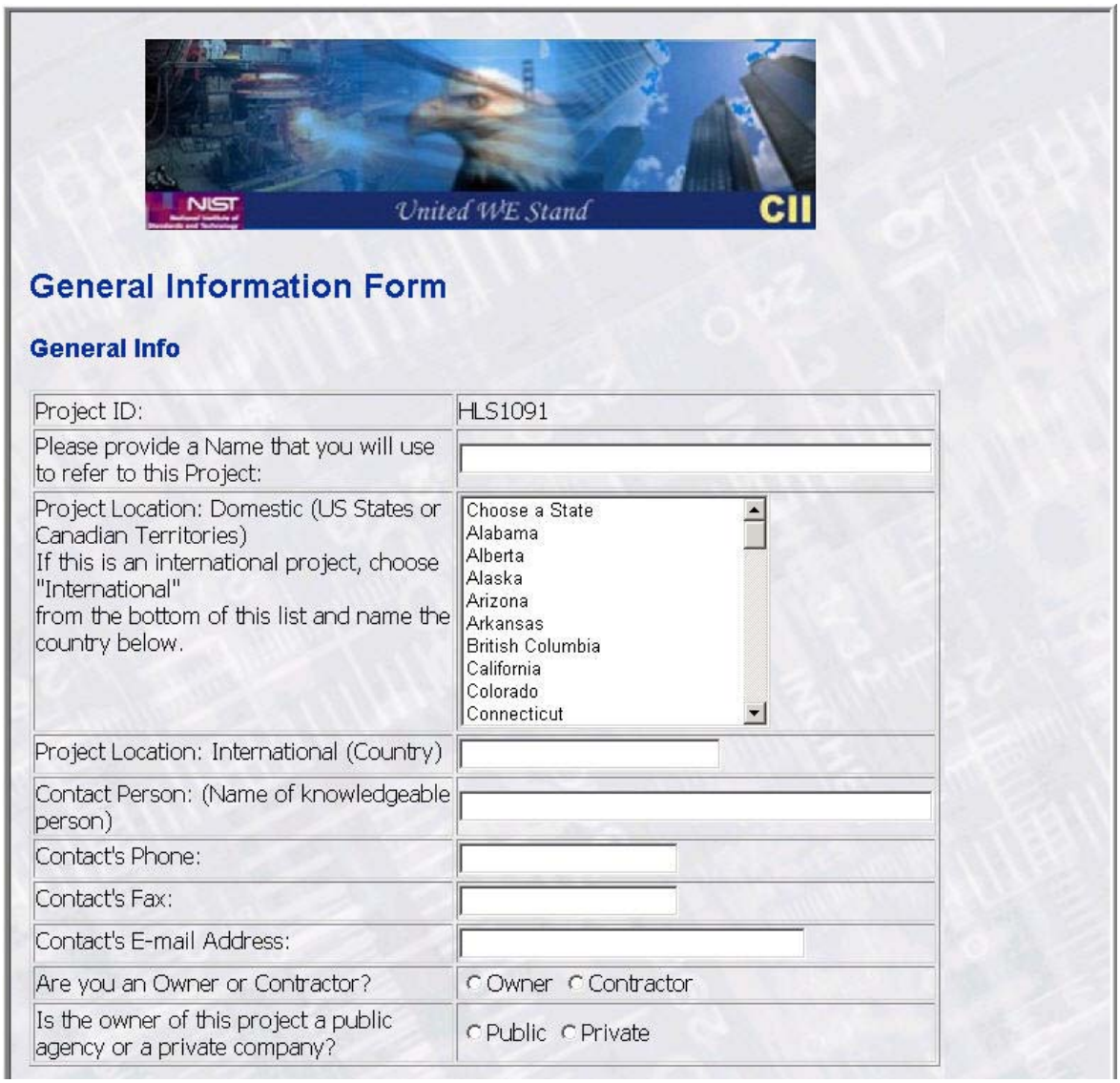
Home Page


United WE Stand
CII
Login to Best Practices for Project Security Survey
To log in, enter your username and password. Use the correct letter case, your username and passwords are case-sensitive.
Username:
Password:
Login
If you don't have a HLS password, click here.
Back to Study Home Page
Did you arrive at this page unexpectedly? Here are a few helpful hints that may explain why.
Cookies - If cookies are not turned on in your browser, you will not be able to access many areas of this web site. (In Netscape, you may turn on cookies under Edit...Preferences...Advanced. In Internet Explorer, go to View...Internet Preferences...Advanced.
Session Timeout - If you have been using protected areas of the site, but made no changes in the last 30-45 minutes, your session will time out and you will need to log in again.
Logout from Project Central
Webmaster

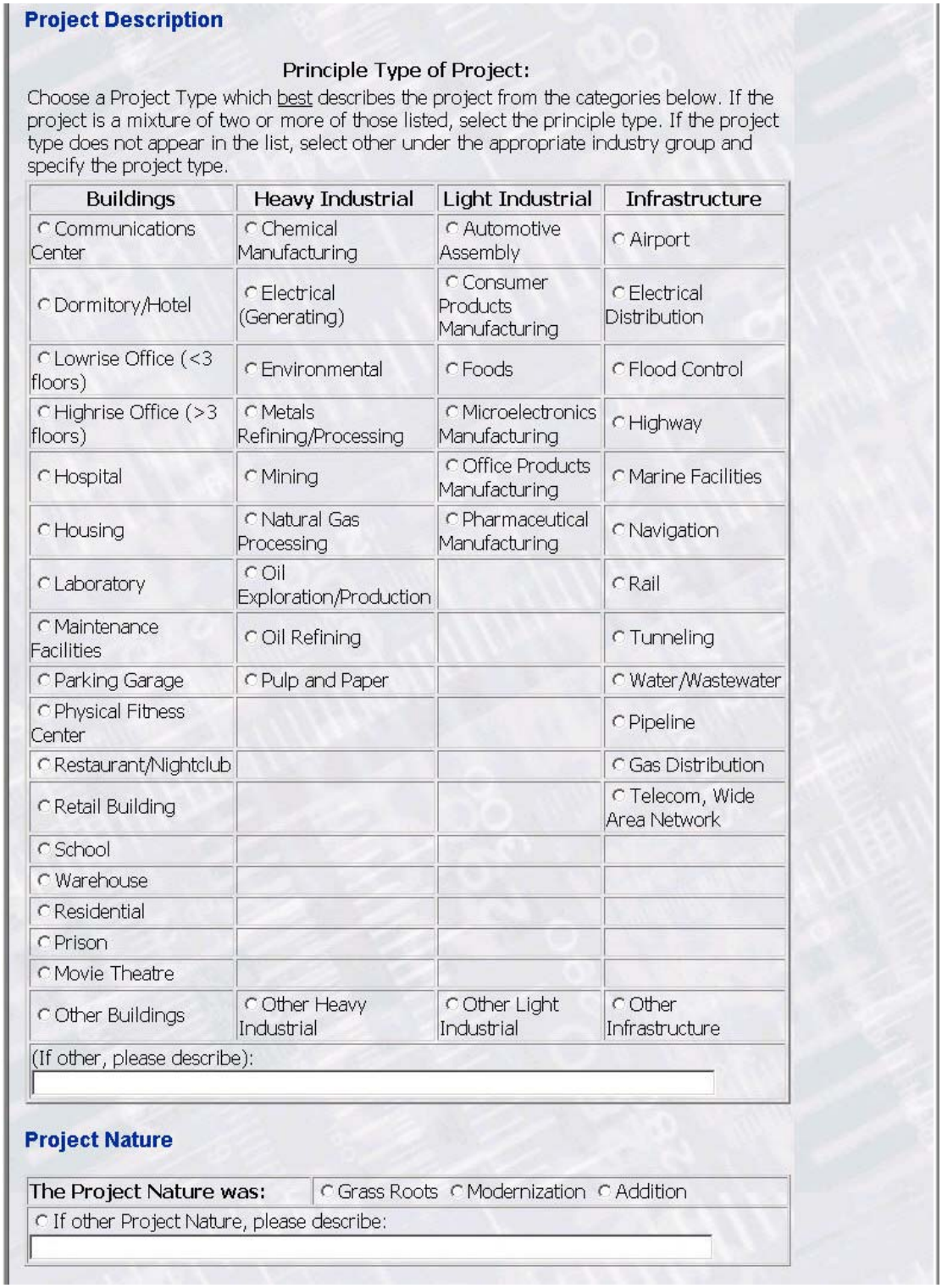
Login Page



Project Central



Project Information Entry



Project Description

Principle Type of Project:

Choose a Project Type which best describes the project from the categories below. If the project is a mixture of two or more of those listed, select the principle type. If the project type does not appear in the list, select other under the appropriate industry group and specify the project type.

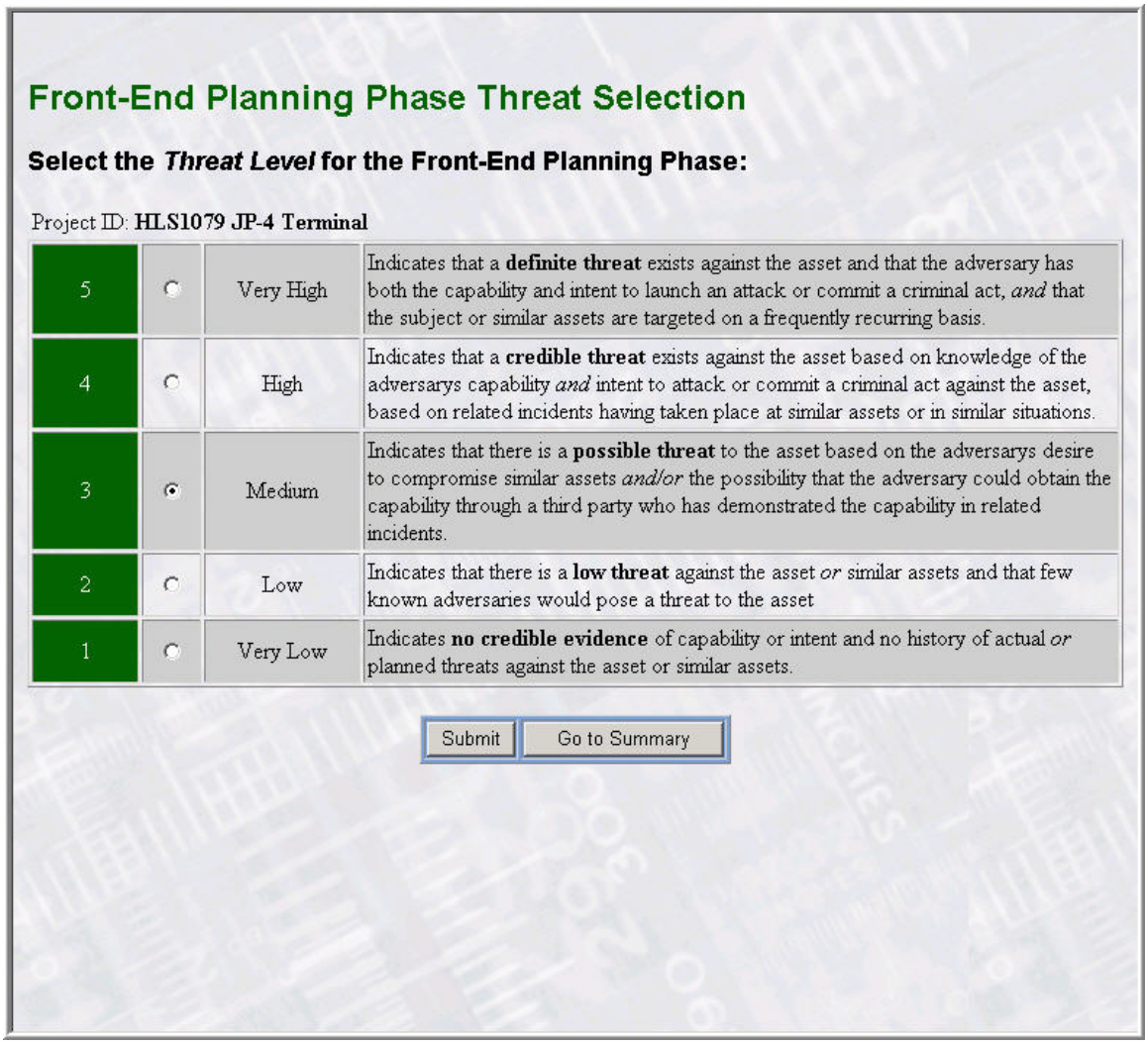
Buildings	Heavy Industrial	Light Industrial	Infrastructure
○ Communications Center	○ Chemical Manufacturing	○ Automotive Assembly	○ Airport
○ Dormitory/Hotel	○ Electrical (Generating)	○ Consumer Products Manufacturing	○ Electrical Distribution
○ Lowrise Office (<3 floors)	○ Environmental	○ Foods	○ Flood Control
○ Highrise Office (>3 floors)	○ Metals Refining/Processing	○ Microelectronics Manufacturing	○ Highway
○ Hospital	○ Mining	○ Office Products Manufacturing	○ Marine Facilities
○ Housing	○ Natural Gas Processing	○ Pharmaceutical Manufacturing	○ Navigation
○ Laboratory	○ Oil Exploration/Production		○ Rail
○ Maintenance Facilities	○ Oil Refining		○ Tunneling
○ Parking Garage	○ Pulp and Paper		○ Water/Wastewater
○ Physical Fitness Center			○ Pipeline
○ Restaurant/Nightclub			○ Gas Distribution
○ Retail Building			○ Telecom, Wide Area Network
○ School			
○ Warehouse			
○ Residential			
○ Prison			
○ Movie Theatre			
○ Other Buildings	○ Other Heavy Industrial	○ Other Light Industrial	○ Other Infrastructure

(If other, please describe):

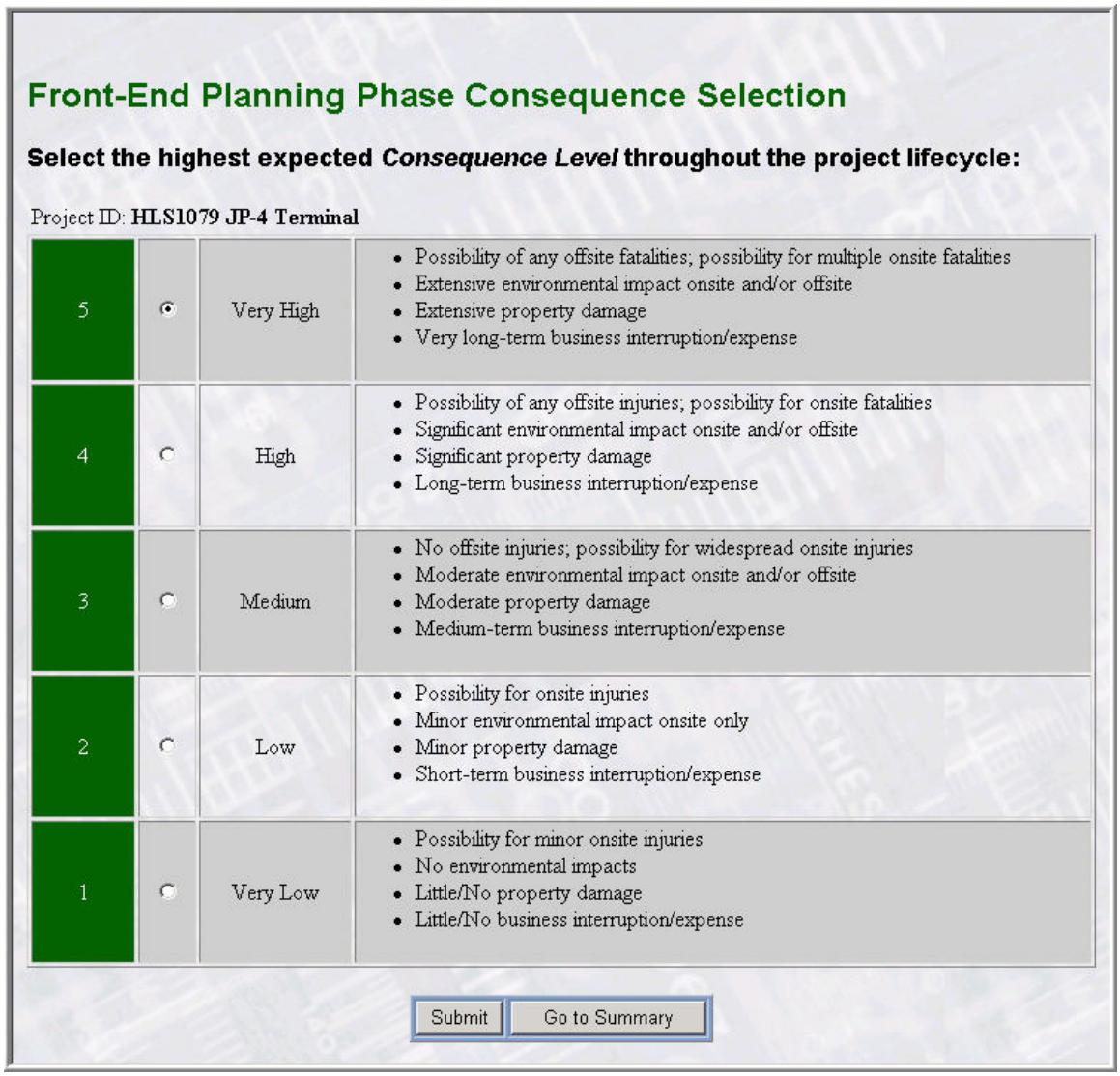
Project Nature

The Project Nature was:	○ Grass Roots ○ Modernization ○ Addition
○ If other Project Nature, please describe:	

Project Description Entry



Threat Selection



Front-End Planning Phase Consequence Selection

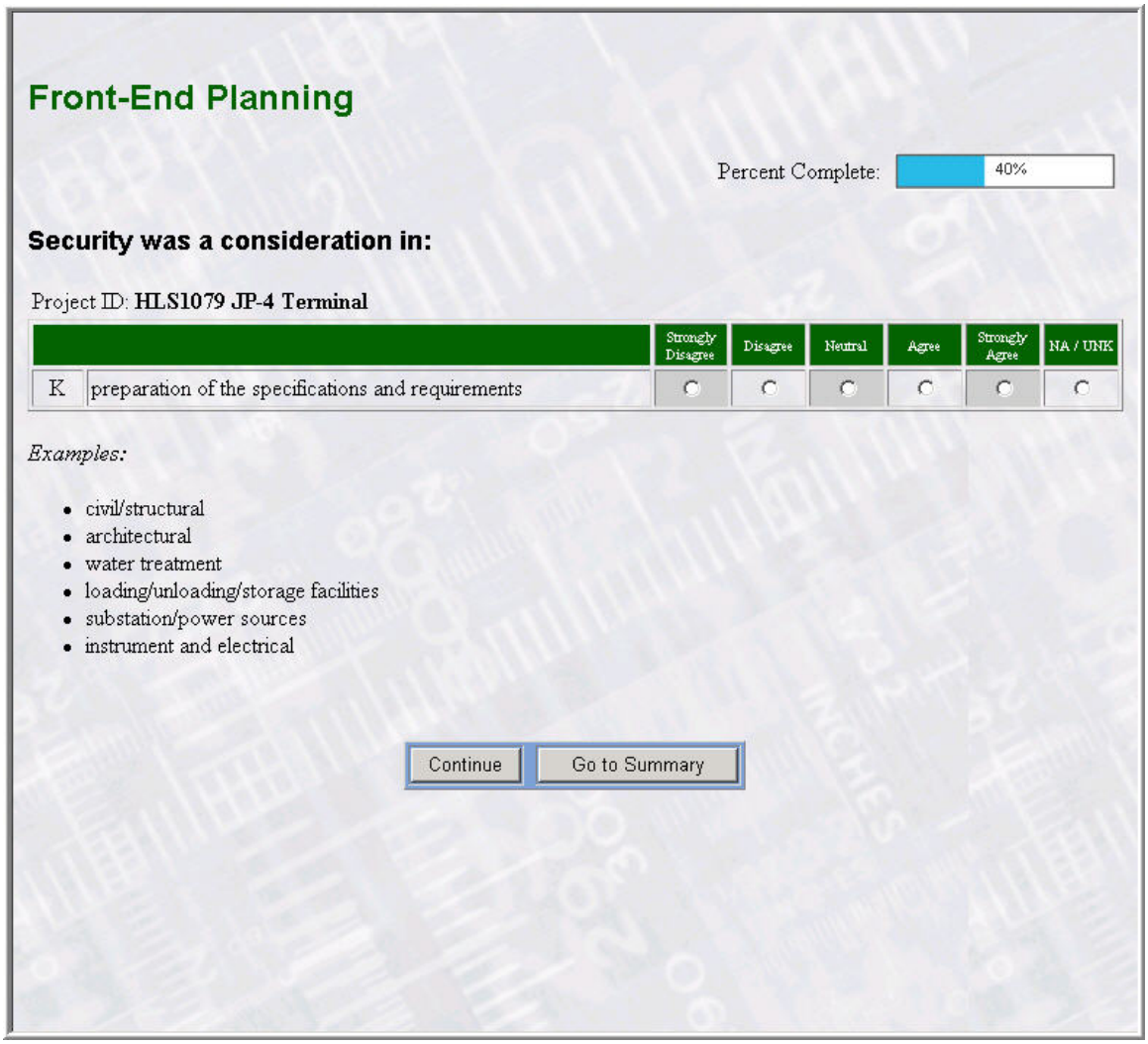
Select the highest expected *Consequence Level* throughout the project lifecycle:

Project ID: **HLS1079 JP-4 Terminal**

5	◉	Very High	• Possibility of any offsite fatalities; possibility for multiple onsite fatalities • Extensive environmental impact onsite and/or offsite • Extensive property damage • Very long-term business interruption/expense
4	○	High	• Possibility of any offsite injuries; possibility for onsite fatalities • Significant environmental impact onsite and/or offsite • Significant property damage • Long-term business interruption/expense
3	○	Medium	• No offsite injuries; possibility for widespread onsite injuries • Moderate environmental impact onsite and/or offsite • Moderate property damage • Medium-term business interruption/expense
2	○	Low	• Possibility for onsite injuries • Minor environmental impact onsite only • Minor property damage • Short-term business interruption/expense
1	○	Very Low	• Possibility for minor onsite injuries • No environmental impacts • Little/No property damage • Little/No business interruption/expense

Submit | Go to Summary

Consequence Selection



Question Page

Front-End Planning Summary

Phase SRI Score: 7.08

To change an answer, click on the corresponding letter of that question.

		Very Low	Low	Medium	High	Very High
A	Threat			X		
B	Consequence					X

Security was a consideration in:

		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	NA / UNK
A	establishing project objectives				X		
B	developing business partnerships/alliances			X			
C	identifying stakeholders for the project team				X		
D	technology and process selection					X	
E	establishing priorities between cost, schedule, and required project features (based upon vulnerability assessment)						X
F	screening of the project team for appropriate level of clearance			X			
G	the project team was in alignment concerning the importance of security issues identified in the project objectives				X		
H	developing project scope		X				
I	developing and evaluating design criteria (based upon vulnerability assessment)					X	
J	determining required site characteristics and location				X		
K	preparation of the specifications and requirements		X				
L	developing the engineering/construction plan and approach					X	
M	developing the plot plan				X		
N	developing the procurement/materials management procedures and plans			X			
O	developing the pre-commissioning/turnover sequence and startup requirements/objectives			X			
P	identifying and resourcing startup requirements					X	
Q	identifying startup risks					X	
R	developing/implementing startup security plan					X	
S	developing the system startup plan (reconciled with the security plan)				X		
T	screening of contractor/subcontractor employees and delivery personnel for appropriate level of clearance				X		
U	preparing the permitting plan				X		
V	evaluation of various personnel issues				X		
W	development of a distribution matrix for document control					X	
X	developing training plans				X		
Y	developing/implementing project information systems security plan				X		

Enter Another Project Phase//Back to HLS Central

Summary Page

APPENDIX I. CORRELATION MATRIX

	PhaseSRI	Threat	Conseq	Heavy	FEP	DES	PRO
Threat	0.337						
	0.003						
Conseq	0.479	0.596					
	0.000	0.000					
Heavy	0.171	0.076	-0.076				
	0.144	0.523	0.518				
FEP	-0.062	0.069	0.006	0.079			
	0.602	0.559	0.961	0.503			
DES	-0.086	-0.073	-0.011	0.004	-0.296		
	0.467	0.537	0.928	0.972	0.010		
PRO	-0.084	-0.039	-0.091	-0.017	-0.284	-0.244	
	0.476	0.743	0.440	0.887	0.014	0.037	
CON	0.065	0.003	0.010	-0.017	-0.284	-0.244	-0.233
	0.581	0.977	0.932	0.887	0.014	0.037	0.045
SU	0.187	0.035	0.091	-0.062	-0.259	-0.222	-0.213
	0.111	0.766	0.440	0.597	0.026	0.058	0.069
Grass	0.192	0.267	0.228	0.422	0.055	0.010	-0.040
	0.101	0.021	0.051	0.000	0.639	0.935	0.736
Add	-0.370	-0.115	-0.434	-0.209	-0.027	-0.005	0.020
	0.001	0.330	0.000	0.074	0.817	0.968	0.868
Mod	0.179	-0.150	0.208	-0.209	-0.027	-0.005	0.020
	0.127	0.203	0.075	0.074	0.817	0.968	0.868
Owner	-0.465	-0.130	-0.180	-0.113	0.027	0.005	-0.020
	0.000	0.270	0.124	0.338	0.817	0.968	0.868
US	-0.382	-0.049	-0.363	-0.164	0.035	0.002	-0.007
	0.001	0.678	0.001	0.163	0.767	0.988	0.950
DB	0.318	0.096	0.130	0.320	0.067	-0.020	-0.002
	0.006	0.418	0.269	0.006	0.570	0.867	0.985
DBB	-0.051	0.193	0.136	-0.177	-0.098	-0.008	0.034
	0.664	0.100	0.248	0.132	0.404	0.944	0.771
MDB	-0.145	-0.281	-0.164	-0.442	-0.035	-0.002	0.007
	0.217	0.015	0.164	0.000	0.767	0.988	0.950
PP	0.182	0.037	0.143	0.125	0.193	0.067	-0.099
	0.122	0.752	0.224	0.288	0.100	0.572	0.400
CM	-0.419	-0.281	-0.427	0.164	-0.035	-0.002	0.007
	0.000	0.015	0.000	0.163	0.767	0.988	0.950

	CON	SU	Grass	Add	Mod	Owner	US
SU	-0.213						
	0.069						
Grass	-0.040	0.008					
	0.736	0.943					
Add	0.020	-0.004	-0.495				
	0.868	0.972	0.000				
Mod	0.020	-0.004	-0.495	-0.510			
	0.868	0.972	0.000	0.000			
Owner	-0.020	0.004	0.129	0.510	-0.638		
	0.868	0.972	0.275	0.000	0.000		
US	-0.007	-0.028	-0.389	0.192	0.192	-0.192	
	0.950	0.815	0.001	0.101	0.101	0.101	
DB	-0.002	-0.053	0.407	-0.375	-0.028	-0.249	-0.513
	0.985	0.654	0.000	0.001	0.812	0.032	0.000
DBB	0.034	0.053	-0.213	-0.070	0.281	-0.047	0.335
	0.771	0.655	0.069	0.551	0.015	0.693	0.003
MDB	0.007	0.028	-0.187	0.377	-0.192	0.192	0.072
	0.950	0.815	0.112	0.001	0.101	0.101	0.540
PP	-0.099	-0.090	0.150	-0.002	-0.147	0.147	0.055
	0.400	0.444	0.201	0.987	0.212	0.212	0.640
CM	0.007	0.028	-0.187	0.377	-0.192	0.192	0.072
	0.950	0.815	0.112	0.001	0.101	0.101	0.540

	DB	DBB	MDB	PP
DBB	-0.654			
	0.000			
MDB	-0.141	-0.335		
	0.230	0.003		
PP	-0.108	-0.256	-0.055	
	0.360	0.028	0.640	
CM	-0.141	-0.335	-0.072	-0.055
	0.230	0.003	0.540	0.640

Cell Contents: Pearson correlation
P-Value

APPENDIX J. REGRESSION OUTPUT

Regression Analysis: PhaseSRI versus Conseq

The regression equation is
PhaseSRI = 2.33 + 1.15 Conseq

Predictor	Coef	SE Coef	T	P
Constant	2.3305	0.7017	3.32	0.001
Conseq	1.1550	0.2494	4.63	0.000

S = 2.19393 R-Sq = 23.0% R-Sq(adj) = 21.9%

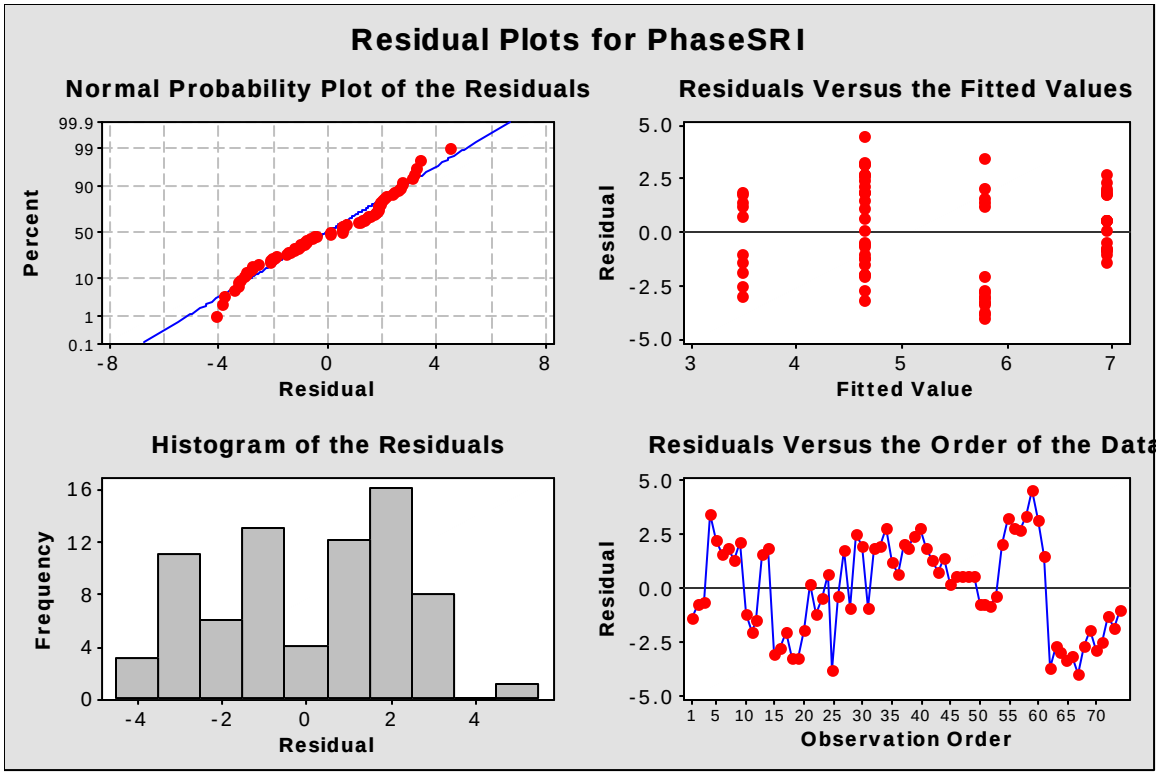
Analysis of Variance

Source	DF	SS	MS	F	P
Regression	1	103.26	103.26	21.45	0.000
Residual Error	72	346.56	4.81		
Total	73	449.82			

Unusual Observations

Obs	Conseq	PhaseSRI	Fit	SE Fit	Residual	St Resid
59	2.00	9.158	4.640	0.298	4.517	2.08R

R denotes an observation with a large standardized residual.


Residual Plots for PhaseSRI
Normal Probability Plot of the Residuals
Percent
99.9
99
90
50
10
1
0.1
-8
-4
0
4
8
Residual
Residuals Versus the Fitted Values
Residual
5.0
2.5
0.0
-2.5
-5.0
3
4
5
6
7
Fitted Value
Histogram of the Residuals
Frequency
16
12
8
4
0
-4
-2
0
2
4
Residual
Residuals Versus the Order of the Data
Residual
5.0
2.5
0.0
-2.5
-5.0
1 5 10 15 20 25 30 35 40 45 50 55 60 65 70
Observation Order

Regression Analysis: PhaseSRI versus Conseq, Owner

The regression equation is
PhaseSRI = 4.13 + 0.985 Conseq - 2.04 Owner

Predictor	Coef	SE Coef	T	P
Constant	4.1265	0.7711	5.35	0.000
Conseq	0.9849	0.2295	4.29	0.000
Owner	-2.0388	0.4962	-4.11	0.000

S = 1.98584   R-Sq = 37.8%   R-Sq(adj) = 36.0%

Analysis of Variance

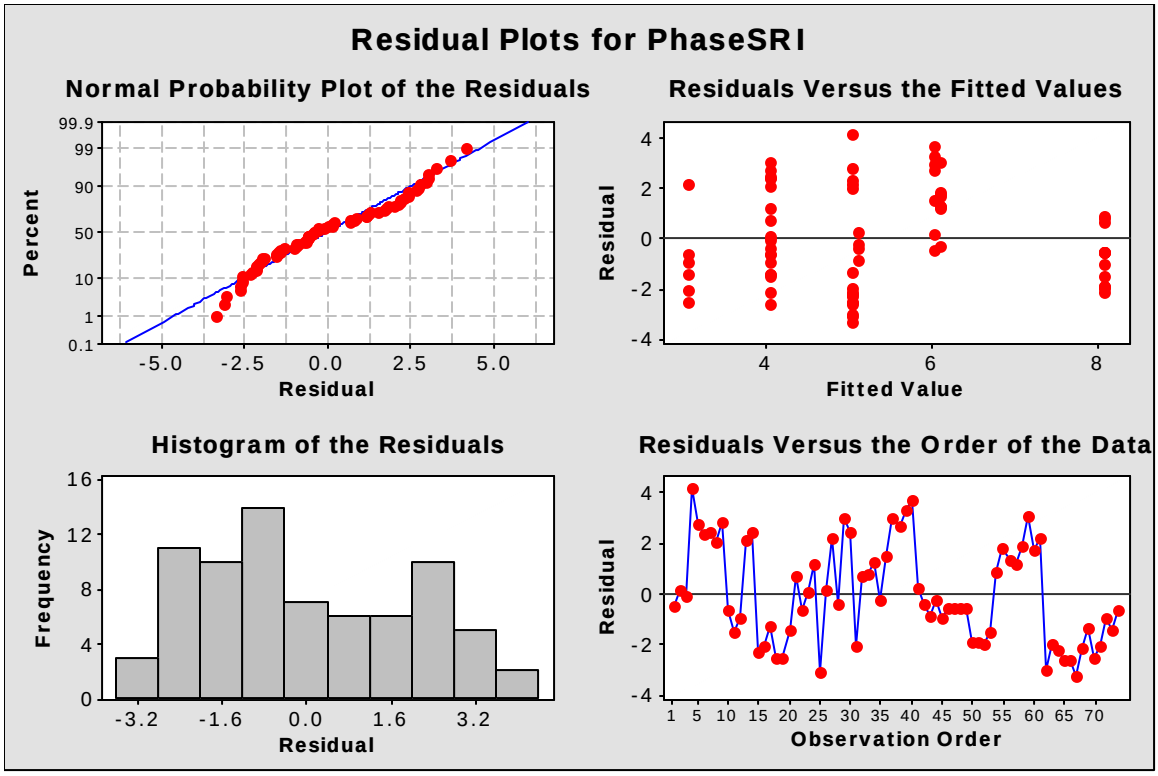
Source	DF	SS	MS	F	P
Regression	2	169.825	84.913	21.53	0.000
Residual Error	71	279.992	3.944		
Total	73	449.817			

Source	DF	Seq SS
Conseq	1	103.258
Owner	1	66.567

Unusual Observations

Obs	Conseq	PhaseSRI	Fit	SE Fit	Residual	St Resid
4	3.00	9.239	5.042	0.307	4.196	2.14R

R denotes an observation with a large standardized residual.


Residual Plots for PhaseSRI
Normal Probability Plot of the Residuals
Percent
99.9
99
90
50
10
1
0.1
-5.0
-2.5
0.0
2.5
5.0
Residual
Residuals Versus the Fitted Values
Residual
4
2
0
-2
-4
4
6
8
Fitted Value
Histogram of the Residuals
Frequency
16
12
8
4
0
-3.2
-1.6
0.0
1.6
3.2
Residual
Residuals Versus the Order of the Data
Residual
4
2
0
-2
-4
1 5 10 15 20 25 30 35 40 45 50 55 60 65 70
Observation Order

List of Acronyms

A/E – Architectural/Engineering

ASIS – American Society of Industrial Security

CAD – Computer-aided Design

CII – Construction Industry Institute

CON – Construction Phase

DES (or D) – Design Phase

FEMA – Federal Emergency Management Agency

FEP – Front-end Planning Phase

HLS – Homeland Security

NFPA – National Fire Protection Association

NIST – National Institute of Standards and Technology

O&M – Operations and Maintenance

PDT – Practice Development Teams

PRO (or P) – Procurement Phase

RFID – Radio Frequency Identification Tag

ST – Steering Team

SRI – Security Rating Index

SU – Startup Phase

SVA – Security Vulnerability Assessment

Glossary

Consequence: the amount of loss or damage that can be expected, or may be expected from a successful attack against an asset

Critical Infrastructure: the assets, systems, and functions vital to national security, governance, public health and safety, economy, and national morale

Domestic Terrorism: criminal acts dangerous to human life that appear intended to intimidate or coerce the civilian population or the government

Front-end planning: the process of developing sufficient strategic information with which owners can address risk and make decisions to commit resources in order to maximize the potential for a successful project

Homeland Security: a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur

Information security: practices and procedures for protection of documents, networks, computer facilities and verbal communication. Firewalls, passwords, and a document control matrix are some examples of information security measures

Materials management: an integrated process for planning and controlling all necessary efforts to make certain that the quality and quantity of materials and equipment

are appropriately specified in a timely manner, are obtained at a reasonable cost, and are available when needed

Personnel security: practices and procedures for hiring, terminations, and workplace issues and response

Physical security: involves equipment, building and grounds design and security practices designed to prevent physical attacks against facilities, people, property or information. Examples include fencing, doors, gates, walls, turnstiles, locks, motion detectors, vehicle barriers, and hardened glass

Security: includes all measures taken to guard against malevolent, intentional acts, both internal and external (e.g., sabotage, crime, and attack), that result in adverse impacts such as project cost growth, schedule extension, operability degradation, safety concerns, transportation delays, emergency response, and offsite effects (consequence)

Security Vulnerability Assessment (SVA): the process of determining the likelihood of an adversary successfully exploiting vulnerability, and the resulting degree of damage or impact

Startup: the transitional phase between plant construction completion and commercial operations, including all of the activities that bridge these two phases

Terrorism: premeditated, politically motivated violence perpetrated against noncombatant targets by sub national groups or clandestine agents, usually intended to influence an audience

Threat: any indication, circumstance, or event with the potential to cause loss of, or damage, to an asset. It is also the intention and capability of an adversary to undertake actions that would be detrimental to valued assets

References

Albright, S. Christian, Wayne L. Winston, and Christopher Zappe. *Data Analysis and Decision Making with Microsoft® Excel*. Second Edition ed. Pacific Grove, CA: Thomson Learning, Inc., 2003.

Alinea Group. *Intensity Questions and the Likert Scale*, 2003 [cited February 17, 2005]. Available from http://www.alineagroup.com/pdfs/Intensity%20Questions%20and%20the%20Likert%20Scale.pdf.

Allen, Richard K. "Legal Implications of Security Awareness in Design and Construction Practice." *Journal of Professional Issues in Engineering Education and Practice* 130, no. 3 (2004): 208-09.

American Academy of Actuaries. *Terrorism Insurance Coverage in the Aftermath of September 11th*. Washington, DC, 2002.

American Chemistry Council. "Site Security Guidelines for the U.S. Chemical Industry." Hallcrest Systems, Inc., 2001.

American Institute of Chemical Engineers. Center for Chemical Process Safety. *Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites*, *Ccps Guidelines Series*. New York, NY: Center for Chemical Process Safety of the American Institute of Chemical Engineers, 2003.

American Petroleum Institute. *Security Guidelines for the Petroleum Industry*, 2003. Available from http://api-ec.api.org/filelibrary/Security_Guidance2003.pdf.

American Petroleum Institute, and National Petrochemical & Refiners Association. *Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries, Second Edition*. Washington, D.C.: API Publishing Services, 2004.

Ansell, Jake, and Frank Wharton, eds. *Risk: Analysis, Assessment and Management*. Chichester, West Sussex, England: John Wiley & Sons Ltd, 1992.

ASIS International. "General Security Risk Assessment Guideline." Alexandria, VA, 2003.

ASTM International. " Standard Practice for Applying Analytical Hierarchy Process (AHP) to Multiattribute Decision Analysis of Investments Related to Buildings and Building Systems." E1765-02. West Conshohocken, PA, 2002.

Bardenaro, Michael. "Calculating Security's Cost." In *ENR: Engineering News-Record*, 29: McGraw-Hill Companies, Inc., 2003.

Berry, W.D., and S. Feldman. "Multiple Regression in Practice." In *Sage University Paper Series on Quantitative Applications in the Social Sciences*. Series No. 07-050. Newbury Park, CA: Sage Publications, Inc., 1985.

Blakeslee, Sandra. "Nuclear Lab's Missing Disks May Not Exist." *The New York Times*, August 12 2004, A17.

Bradley, David. *Construction Sites Vulnerable to Theft* March 5, 2005 [cited March 9, 2005]. Available from http://www.timesdispatch.com/servlet/Satellite?pagename=RTD%2FMGArticle%2FRTD_BasicArticle&c=MGArticle&cid=1031781368236&path=!flair&s=1045855936229.

Broder, James F. *Risk Analysis and the Security Survey*. 2nd ed. Boston, MA: Butterworth Heinemann, 2000.

Brown, Jeffrey R., and National Bureau of Economic Research. *An Empirical Analysis of the Economic Impact of Federal Terrorism Reinsurance* National Bureau of Economic Research, 2004. Available from http://papers.nber.org/papers/W10388.

Bush, George W. *National Strategy for the Physical Protection of Critical Infrastructures and Key Assests*. Washington, D.C.: The White House, 2003.

Center for Chemical Process Safety of the American Institute of Chemical Engineers. *Guidelines for Analyzing and Managing the Security Vulnerabiliites of Fixed Chemical Sites*. New York, NY, 2002.

Construction Industry Institute. "Evaluation of Design Effectiveness." Research Summary 8-1. Austin, TX, 1986.

Construction Industry Institute. "Input Variables Impacting Design Effectiveness." Research Summary 8-2. Austin, TX, 1987.

———. "Constructability." Implementation Guide 34-1. Austin, TX, 1993.

———. "Pre-Project Planning Handbook." Special Publication 39-2. Austin, TX, 1995.

———. "Project Definition Rating Index (PDRI), Industrial Projects." Implementation Resource 113-2. Austin, TX, 1996.

———. "Alignment During Pre-Project Planning—a Key to Project Success." Implementation Resource 113-3. Austin, TX, 1997.

———. "Planning for Startup." Implementation Resource 121-2. Austin, TX, 1998.

———. "Procurement and Materials Management: A Guide to Effective Project Execution." Implementation Resource 7-3. Austin, TX, 1999.

———. "A Guide to the CII Implementation Model and Knowledge Structure." Implementation Resource 166-2. Austin, TX, 2001.

———. "CII Best Practices for Improving Project Performance." Implementation Resource 166-3. Austin, TX, 2002.

———. "Project Objective Setting." Research Summary 12-1. Austin, TX, 2003.

———. *SRI Questionnaire*, 2003 [cited February 22, 2005]. Available from http://www.construction-institute.org/sri.

———. "Best Practices for Project Security." BMM2004-10. authored by Stephen R. Thomas, Jonathan R. Sylvie, and Candace L. Macken. Austin, TX, 2004.

———. *Construction Industry Institute*, 2004 [cited March 5, 2005]. Available from http://www.construction-institute.org.

———. *Mission*, 2004 [cited February 10, 2005]. Available from http://www.construction-institute.org/mission.cfm.

Davis-Blake, Allison, Joeseph P. Broschak, Fernando J. Rodriquez, G. Edward Gibson, Jr., and Todd A. Graham. "Owner/Contractor Organizational Changes, Phase II Report." Report No. 2. Austin, TX, 1999.

Dearborn Financial Institute. *Terrorism Coverage for Commercial Lines*, *Dearborn Career Development*. [Chicago]: Dearborn Financial Institute, 2003.
Design-Build Institute of America. *An Introduction to Design-Build*, 1994 [cited March 7, 2005]. Available from http://www.dbia.org/pubs/pd_intro.pdf.
Dixon, Lloyd S., and Rachel Kaganoff Stern. *Compensation for Losses from the 9/11 Attacks*. Santa Monica, CA: RAND, 2004.
Einstein, Josh. "The Hidden Fortress." *Access Control & Security Systems*, January 1, 2005, 18.
Expert Choice Inc. *Expert Choice 2000 for Groups*. 2nd ed. Arlington, VA: Expert Choice, Inc., 2003.
Fay, John. *Contemporary Security Management*. Boston: Butterworth-Heinemann, 2002.
Fickes, Michael. "Will 2005 Be the Year for Chemical Security Regulations?" *Access Control & Security Systems*, January 1, 2005, 16.
Garcia, Mary Lynn. *The Design and Evaluation of Physical Protection Systems*. Boston: Butterworth-Heinemann, 2001.
Gibson, G. Edward, Jr. , Allison Davis-Blake, Joeseph P. Broschak, and Fernando J. Rodriguez. "Owner/Contractor Organizational Changes, Phase I." Report No. 1. Austin, TX, 1998.
Gips, Michael A. "Tough Track for Railroads." *Security Management* 49, no. 1 (2005): 56.
Green, Samuel B. "How Many Subjects Does It Take to Do a Regression Analysis." In *Multivariate Behavioral Research*, 499: Lawrence Erlbaum Associates, 1991.
Guthrie, Vernon H., David A. Walker, Charles M. Mitchell, and James J. Rooney. *Modeling Security Risk*, 2005 [cited April 28, 2005]. Available from http://www.inmm.org/topics/contents/pdfs/Risk.pdf.
Hitchcock, April, and Karen Porter. *The Likert Scale*, 2005 [cited February 17, 2005]. Available from http://www.arches.uga.edu/~porterk/likertscale.html.
Holland, Jennifer. "S. Carolinians Recount Events after Chlorine Cloud Moved In." *Austin American-Statesman*, January 8 2005, A10.
Houghton Mifflin Company. *The American Heritage Dictionary of the English Language*. 4th ed. Boston: Houghton Mifflin, 2000.
Inskeep, Steve. *Chertoff Details Risk-Analysis Approach to Security* (Morning Edition) National Public Radio, March 16, 2005. Available from http://www.npr.org/templates/story/story.php?storyId=4537007.
Jolly, Adam, ed. *Managing Business Risk*. London, UK: Kogan Page Ltd, 2003.
Krimgold, Frederick, David Hattis, William I. Whiddon, and United States. Federal Emergency Management Agency. *Insurance, Finance, and Regulation Primer for Terrorism Risk Management in Buildings : Providing Protection to People and Buildings*. [Washington, D.C.]: U.S. Dept. of Homeland Security, FEMA, 2003.
Kunreuther, Howard, Erwann Michel-Kerjan, and National Bureau of Economic Research. *Policy Watch Challenges for Terrorism Risk Insurance in the United States* National Bureau of Economic Research, 2004. Available from http://papers.nber.org/papers/W10870.
Matthews, Benjamin E. "Addressing Security Concerns in the Early Stages of the Project Lifecycle." The University of Texas at Austin, 2003.

Merriam-Webster Inc. *Webster's New Collegiate Dictionary*. Springfield, Mass.: G. & C. Merriam Co., 1980.
MINITAB Inc. *Minitab StatGuide*, 2003 [cited February 20, 2005].
Mogey, Nora. *Likert Scale Information Page*, 1999 [cited February 17, 2005]. Available from http://www.icbl.hw.ac.uk/ltdi/cookbook/info_likert_scale/.
National Equipment Register. *The Problem of Heavy Equipment Theft*, 2004 [cited August 12, 2004]. Available from http://www.nerusa.com/theft_problem.asp.
National Institute of Standards and Technology. *NIST Mission, Vision, Values, and Practices*, 2000 [cited 2005 January 28,]. Available from http://www.nist.gov/public_affairs/nist_mission.htm.
National Institute of Standards and Technology. "Best Practices for Project Security." NIST GCR 04-865. authored by Stephen R. Thomas, Jonathan R. Sylvie, and Candace L. Macken. Gaithersburg, MD, 2004.
———. *General Information*, 2004 [cited February 10, 2005]. Available from http://www.nist.gov/public_affairs/general2.htm.
———. *Technologies for Public Safety and Security:*
Activities at the National Institute of Standards and Technology, 2004 [cited March 5, 2005]. Available from http://www.nist.gov/public_affairs/factsheet/homeland.htm.
———. *BFRL: Advanced Construction Technology*, 2004 [cited March 6, 2005]. Available from http://www.bfrl.nist.gov/goals_programs/HS_goal.htm.
National Research Council (U.S.). Committee on Science and Technology for Countering Terrorism. *Making the Nation Safer : The Role of Science and Technology in Countering Terrorism*. Washington, D.C.: National Academy Press, 2002.
New York (State). Legislature. Assembly. Standing Committee on Insurance. *Impact of the Federal Terrorism Risk Insurance Act of 2002 : Public Hearing*. [Mineola]: EN-DE Reporting Services, 2003.
O'Hanlon, Michael E. *Protecting the American Homeland : One Year On*. [Updated] with a new preface. ed. Washington, D.C.: Brookings Institution Press, 2003.
Office of Homeland Security. *National Strategy for Homeland Security*. Washington, D.C.: Office of Homeland Security, 2002.
Osborne, Jason W., and Elaine Waters. *Multiple Regression Assumptions*, 2002 [cited February 20, 2005]. Available from http://www.ericdigests.org/2003-3/multiple.htm.
POA Publishing. *Asset Protection and Security Management Handbook*. Boca Raton, FL: Auerbach Publications, 2003.
Princeton University. *DSS - Interpreting Regression Output*, 2004 [cited February 20, 2005]. Available from http://dss.princeton.edu/online_help/analysis/interpreting_regression.htm.
Redmill, Felix. *Risk Analysis - a Subjective Process*, 2002 [cited March 6, 2005]. Available from http://www.system-safety.org/eJSS_Editions/Edition1/techarticle.html.
Robinson, Linda G., and International Risk Management Institute. *Terrorism Insurance : What Risk and Insurance Professionals Must Know*. Dallas, TX: International Risk Management Institute, 2003.

Saaty, Thomas L. *The Analytic Hierarchy Process*. New York, NY: McGraw-Hill, Inc., 1980.
———. *The Analytic Hierarchy Process : Planning, Priority Setting, Resource Allocation*. 2nd ed. Pittsburgh, PA: RWS Publications, 1990.
Sakamoto, Arthur Jr., March 4, 2005. Personal communication.
Selltiz, Claire, and Louise Kidder. *Selltiz, Wrightsman and Cook's Research Methods in Social Relations*. Edited by Louise Kidder. 4th ed. New York, NY: Holt, Rinehart, and Winston, 1981.
Smetters, Kent A., and National Bureau of Economic Research. *Insuring against Terrorism the Policy Challenge* National Bureau of Economic Research, 2005. Available from http://papers.nber.org/papers/W11038.
Smith, Ryan. "Validation of the Security Rating Index." The University of Texas at Austin, 2004.
Taleb, Nassim N. "Learning to Expect the Unexpected." *The New York Times*, April 8 2004, A29.
The Construction Specialist. *Security Check* Reed Business Information, 2005 [cited March 4, 2005]. Available from http://www.manufacturing.net/ind/index.asp?layout=tcsArticle&articleID=CA499309.
Thomas, Stephen R. "An Assessment Tool for Improving Project Team Communications." The University of Texas at Austin, 1996.
Trochim, M.K. *Statistical Power*, 2002 [cited February 20, 2005]. Available from http://www.socialresearchmethods.net/kb/power.htm.
Union Carbide Corp. *Bhopal - the Incident, Response, and Settlement*, 2004 [cited March 7, 2005]. Available from http://www.bhopal.com/irs.htm.
United States. Congress. House. Committee on Financial Services. Subcommittee on Capital Markets Insurance and Government Sponsored Enterprises., and United States. Congress. House. Committee on Financial Services. Subcommittee on Oversight and Investigations. *A Review of Tria and Its Effect on the Economy : Helping America Move Forward : Hearing before the Subcommittee on Capital Markets, Insurance and Government Sponsored Enterprises and the Subcommittee on Oversight and Investigations of the Committee on Financial Services, U.S. House of Representatives, One Hundred Eighth Congress, Second Session, April 28, 2004*. Washington: U.S. G.P.O. : For sale by the Supt. of Docs., U.S. G.P.O., 2004.
United States. Congress. House. Committee on Financial Services. Subcommittee on Oversight and Investigations. *How Much Are Americans at Risk until Congress Passes Terrorism Insurance Protection? : Hearing before the Subcommittee on Oversight and Investigations of the Committee on Financial Services, U.S. House of Representatives, One Hundred Seventh Congress, Second Session, February 27, 2002*. Washington: U.S. G.P.O. : For sale by the Supt. of Docs., U.S. G.P.O. [Congressional Sales Office], 2002.

United States. Congress. House. Committee on the Judiciary. *Homeland Security Act of 2002 : Hearing before the Committee on the Judiciary, House of Representatives, One Hundred Seventh Congress, Second Session, on H.R. 5005, June 26, 2002*. Washington: U.S. G.P.O. : For sale by the Supt. of Docs., U.S. G.P.O. [Congressional Sales Office], 2002.

United States. Congress. Senate. Committee on Banking Housing and Urban Affairs. *Terrorist Risk Insurance : Hearing before the Committee on Banking, Housing, and Urban Affairs, United States Senate, One Hundred Seventh Congress, First Session on How the Insurance Industry Should Respond to Risks Posed by Potential Terrorist Attacks and the Extent to Which the Government Should Play a Role Alongside the Industry to Address These Risks, in Light with the September 11, 2001, and How These Decisions Will Effect Insurance Coverage and Premiums on Property and Casualty Reinsurance Contracts as They Come up for Renewal, October 24 and 25, 2001*. Washington: U.S. G.P.O. : For sale by the Supt. of Docs., U.S. G.P.O., [Congressional Sales Office], 2002.

United States. Dept. of Homeland Security. "Securing Our Homeland U.S. Department of Homeland Security Strategic Plan." Department of Homeland Security. Securing our homeland: vision, mission, core values & guiding principles U.S. Department of Homeland Security strategic plan Cover title. Shipping list no.: 2004-0270-M. Washington, D.C.: U.S. Dept. of Homeland Security, 2004.

United States. General Accounting Office., and United States. Congress. House. Committee on Financial Services. *Terrorism Insurance : Implementation of the Terrorism Risk Insurance Act of 2002*. Washington, D.C.: GAO, 2004.

Wait, Patience. "Info Sharing Can Be Perilous—Just Ask Energy and DHS." *Government Computer News*, February 7, 2005 2005.

Weiss, Eric M., and Spencer S. Hsu. "90-Day Hazmat Ban Is Passed." *The Washington Post* 2005, B01.

Yu, Alex. *Regression Assumptions -- SAS Tips*, 1998 [cited February 20, 2005]. Available from http://seamonkey.ed.asu.edu/~alex/computer/sas/regression_assumption.html.

Vita

Jonathan Reed Sylvie was born in New York City, New York on September 9, 1970, the son of Arthur Joseph Sylvie and Gloria Rose Sylvie. After completing his high school education at the Bronx High School of Science, New York City, New York in 1988, he entered Carnegie Mellon University in Pittsburgh, Pennsylvania. He received the degree of Bachelor of Science in Industrial Management with an additional major in Information and Decision Systems from Carnegie Mellon University in May, 1992, at which time he was commissioned as a Second Lieutenant in the United States Army. During the following years he served in positions of increasing responsibility as an officer in the Medical Service Corps. While assigned to Fort Sam Houston, Texas in 1996, he entered the University of Texas at San Antonio. He received the degree of Master of Business Administration in Business Finance in May, 1998. In 1999, he was assigned to Schofield Barracks, Hawaii for three and one-half years where he served as Project Manager for medical construction projects in Hawaii, Japan, Kenya, Kuwait, Nepal, the Republic of Korea, the Republic of the Marshall Islands, and Thailand. In July, 2002, he entered the Graduate School at the University of Texas at Austin to pursue his doctorate in Civil Engineering. He was promoted to the rank of Major in February, 2003.

Permanent address: 6604 Nusser Lane, Austin, Texas 78739

This dissertation was typed by the author.