The Role of Organizational Culture in Creating Secure and Resilient Supply Chains

by
Abby Sophia Benson

B.S. Geology and Geophysics
Yale University, 1996

Submitted to the Civil and Environmental Engineering Department and the Engineering Systems Division in Partial Fulfillment of the Requirements for the Degree of

Master of Science in Transportation
and
Master of Engineering in Logistics

at the

Massachusetts Institute of Technology
June 2005

Signature of the Author.....
Civil and Environmental Engineering Department
Engineering Systems Division
May 6, 2005

Certified By.....
James B. Rice, Jr.
Director, MIT Integrated Supply Chain Management Program
Thesis Supervisor

Certified By.....
Yosef Sheffi
Professor, Civil and Environmental Engineering and Engineering Systems
Thesis Supervisor

Accepted By.....
Yosef Sheffi
Professor, Civil and Environmental Engineering and Engineering Systems
Director, Center for Transportation & Logistics

Accepted By.....
Andrew J. Whittle
Professor of Civil and Environmental Engineering
Chairman, Departmental Committee for Graduate Students

The Role of Organizational Culture in Creating Secure and Resilient Supply Chains

by

Abby Sophia Benson

Submitted to the Department of Civil and Environmental Engineering and the Engineering Systems Division on May 6, 2005 in Partial Fulfillment of the Requirements for the Degrees of Master of Science in Transportation and Master of Engineering in Logistics

Abstract

This thesis aims to understand the role that organizational culture plays in creating secure and resilient supply chains. The terrorist attacks of September 11, 2001, and the government's subsequent response, propelled supply chain security and resilience to the forefront of industry's concerns. Public-private partnerships such as the Customs Trade Partnership Against Terrorism (C-TPAT) have capitalized upon these concerns and created incentives for industry to address supply chain security and resilience both internally and with their external partners. The thesis studies how companies manage supply chain security and resilience, and specifically the role that organizational culture plays in instilling their importance into the organization.

Senior security executives at twenty–three companies across a variety of industries were interviewed. Companies were selected based on information previously known about their high performance in the supply chain security and resilience arenas. Interviewees were questioned about their company's security and business continuity programs, and how they relate to the company's overall corporate culture. Schein's organizational culture framework was used to analyze observations on three levels: artifacts, espoused values, and basic underlying assumptions. Each level of culture is summarized, and key success factors for creating a supply chain security culture are proposed. Before implementing these key success factors, it is recommended that companies understand the supply chain security context, specifically the need for supply chain security, the primary drivers behind supply chain security, and the overall corporate culture. The high performance of the companies included in this study suggest that implementation of the proposed key success factors, in alignment with a company's supply chain security objectives and corporate culture, should increase supply chain security and resilience performance throughout the company.

Thesis Supervisor: James Rice
Title: Director, MIT Integrated Supply Chain Management Program

Thesis Supervisor: Yosef Sheffi
Title: Professor of Civil and Environmental Engineering and Engineering Systems
Director, MIT Center for Transportation and Logistics

Acknowledgements

First and foremost, I thank Jim Rice and Yossi Sheffi for their invaluable guidance over the past two years. The hours spent sharing ideas with them across the table were extremely enlightening, and have contributed greatly to my MIT experience.

I have truly valued my tenure on the Supply Chain Response to Terrorism Project. I thank fellow team members Deena Disraelly, David Opolon, and Pablo Torres for their camaraderie. I also thank Phil Spayd for sharing his unique perspective.

I thank Chris Caplice and Joseph Sussman for supporting my desire to complete a dual degree program within the CEE and ESD departments. I also thank both the MST and MLOG classes of 2005 for their friendship and support.

The Center for Transportation and Logistics warmly welcomed me into their family, and for that I am extremely grateful. Thank you in particular to Mary Gibson, Nancy Martin, Karen van Nederpelt, Becky Schneck, Nicole Blizek, and Lisa Emmerich.

This research would not have been possible without the willingness of the interviewees to participate. I sincerely thank all those who took time out of their busy days to share their wisdom, and all those that help make these connections possible.

Thank you to the United States Coast Guard for providing me with this amazing opportunity to expand my horizons. In particular, thank you to CAPT Mary Landry and CDR Tina Burke for their mentorship.

Finally, I would like to thank Chip and Barbara Benson, John Hickey, and Demme Joannou for their love, listening, support, and patience.

Table of Contents

List of Tables

List of Figures

List of Acronyms

AIAG	Automotive Industry Action Group
AGMA	Alliance for Gray Market and Counterfeit Abatement
AP	Assets Protection
CTL	Center for Transportation and Logistics
CBP	United States Bureau of Customs and Border Protection
C-TPAT	Customs Trade Partnership Against Terrorism
CIA	Central Intelligence Agency
CDC	Center for Disease Control and Prevention
CFE	Certified Fraud Examiner
CFO	Chief Financial Officer
COO	Chief Operating Officer
CPP	Certified Protection Professional
CSI	Container Security Initiative
DHS	United States of Department of Homeland Security
FBI	Federal Bureau of Investigation
FDA	United States Food and Drug Administration
FAA	Federal Aviation Administration
HR	Human Resources
ISO	International Organization for Standardization
ISMA	International Security Management Association
ISPS	International Ship and Port Facility Security Code
IT	Information Technology
MIT	Massachusetts Institute of Technology
MTSA	Maritime Transportation Security Act of 2002
OSAC	Overseas Security Advisory Council
OSHA	Occupational Safety and Health Administration
POPI	Protection of Proprietary Information
QA	Quality Assurance
RFID	Radio Frequency Identification
RILA	Retail Industry Leader's Association
ROI	Return on Investment
SCRT	Supply Chain Response to Terrorism
SEC	United States Security and Exchange Commission
SOX	Sarbanes-Oxley Act of 2002
SST	Smart and Secure Tradelane Initiative
TAPA	Technology Asset Protection Association
TQM	Total Quality Management
USCG	United States Coast Guard
USDA	United States Department of Agriculture
VACIS	Vehicle and Cargo Inspection System
VP	Vice President

1 Introduction

The terrorist attacks of September 11, 2001 and the government's subsequent response propelled supply chain security to the forefront of industry's concerns. These attacks alerted industry and governments to the potential for disruptions from high impact/low probability events such as terrorism. Since September 11, 2001, public-private partnerships such as the Customs Trade Partnership Against Terrorism (C-TPAT) and the Container Security Initiative (CSI) have capitalized upon this concern and created incentives for industry to address supply chain security both internally and with their external partners (see Appendix A for brief descriptions of these programs). These initiatives have also encouraged companies to broaden the scope of supply chain security beyond its historical focus on theft avoidance to include disruptions such as natural disasters, sabotage, and terrorism. Companies today are challenged with the dual task of securing their supply chains to prevent a variety of potential disruptions, and improving resiliency to respond to them if and when they do occur.

For the purposes of this study, security is defined as protecting the integrity of product, processes, and information from internal and external threats. The use of the term "security program" throughout this study implies a program that assumes responsibility for supply chain security. Resilience describes the ability of an organization to react to an unexpected disruption and restore normal operations. The use of the term "business continuity planning (BCP) program" throughout this study refers to a program charged with maintaining business operations, which in turn emphasizes the need for resilience.

This study is just one initiative of the Supply Chain Response to Terrorism (SCRT) project at the Massachusetts Institute of Technology (MIT) Center for Transportation and Logistics (CTL). The purpose of the SCRT project is to study the impact of high-impact/low-probability disruptions, such as global terrorism, on supply chains. This particular study aims to identify how companies manage their security and resilience programs, and specifically the role that organizational culture plays in instilling their importance into the organizations.

Senior security officials at twenty-three companies across a variety of industries were interviewed for this study. Companies were selected based on information previously known

about their high performance in the security and resilience arenas. Interviewees were questioned about their company's security and business continuity programs, and how they relate to the company's overall corporate culture. Schein's organizational culture framework was used to analyze the observations on three levels: artifacts, espoused values, and basic underlying assumptions. Each level of culture is summarized, and key success factors for creating a supply chain security culture are proposed.

1.1 Thesis Overview

Chapter One introduces the thesis and provides an overview of its organization. Chapter Two includes a survey of the literature that covers three specific areas: supply chain security, organizational culture theory, and anecdotal examples of corporate culture used to further develop the chosen framework. Chapter Three provides a detailed overview of the methodology used in this study and introduces the results.

Chapters Four and Five discuss observations in the context of the chosen framework outlined in Chapter Three. Chapter Four discusses supply chain security artifacts, while Chapter Five discusses supply chain security espoused values. Chapter Six builds on the results in Chapters Four and Five to suggest three basic underlying assumptions that appear to support adoption of a supply chain security culture. Chapter Seven suggests key success factors useful in creating a supply chain security culture. Chapter Eight describes methods to understand the company-specific context surrounding creation of this supply chain security culture. Chapter Nine summarizes conclusions of the study, and describes areas for potential further research.

2 Literature Review

The literature review consisted of three parts. The first part involved surveying the literature for research on the role of organizational culture in improving supply chain security and resilience. The second part involved surveying the literature on corporate culture theory, and choosing a framework with which to conduct my analysis. The final part involved further developing that framework through a review of anecdotal literature on corporate culture.

2.1 Supply Chain Security Culture

Sheffi (2001) wrote one of the first articles to directly address supply chains' response to terrorism. The article focuses on new ways of managing supply chains in the wake of the September 11, 2001 terrorist attacks. Sheffi recommends several business practices including improving supplier relationships, revisiting inventory management, entering into public-private partnerships, and increasing shipment visibility and collaboration. He also addresses the issue of culture directly, stating "no Chief Security Officer or Security Organization will be successful unless the culture of the enterprise adds security consciousness to its daily life."

Martha and Subbakrishna (2002) compare the effects of terrorist incidents to those from other low probability, high impact events such as natural disasters. The authors recommend increasing insurance levels, arranging for alternate sourcing and transportation, influencing customer demand to match inventory, and revisiting minimum inventory levels. The article provides comparisons of well-prepared and under-prepared companies in the wake of events such as natural disasters, public health crises, and terrorist incidents.

Rice and Caniato (2003) conducted a survey of several companies with global operations to determine the effectiveness of implementing both security and resilience measures in the supply chain. The measures implemented by companies include improving redundancy, flexibility, and focusing on business continuity planning. The authors categorized companies' responses as basic, reactive, proactive, and advanced. One important group of

responses dealt specifically with organizational capabilities, such as "socializing" security, increasing visibility of security leadership, and providing extensive training to employees.

Lee and Wolfe (2003) argue that Total Quality Management (TQM) principles can effectively assist in creating secure and resilient supply chains. Some of these principles include prevention, designing security into the supply chain, keeping control of security processes, and focusing on the process versus the final product. Lee and Whang (2003) draw again from the quality movement, stating that the overriding theme of the quality movement "that higher quality can be attained at lower cost by proper management and operational design" can be applied to security as well. The authors provide a simple quantitative model showing the cost benefits of participating in the Smart and Secure Tradelane Initiative (SST), a public-private partnership (see Appendix A for a brief description of this program).

Finally, Coutu (2002) looks at the more human aspect of resilience, making the connection between personality traits that foster resilience in individuals and how organizations that embody these same traits can also be resilient. She concludes that resilient people and organizations are those that face reality, search for meaning in all situations, and ritualize ingenuity.

2.2 Corporate Culture Theory

Corporate culture first gained attention in the early 1970s as an elusive driving force behind many organizations' success. The concept has grown in acceptance over the past thirty years, and much research has been conducted regarding how to define, measure, and link corporate culture to a company's success. Although difficult to quantify, corporate culture acts as a behavioral mechanism that affects beliefs and norms used to make decisions in the organizational context. At the most basic level, corporate culture can be expressed as simply "how we do things around here." Members of an organization, in fact, may struggle to understand or express their corporate culture. Although some companies have built their success on specific cultures, such as 3M's focus on innovation and IBM's focus on customer service, culture remains for many a strong, yet elusive, influence on their effectiveness.

The term culture finds its origins in social anthropology's studies of late nineteenth and early twentieth century "primitive societies," such as Eskimo, African, and Native

American peoples (Kotter & Heskett, 1992). Although the word culture brings to mind studies of countries and their people, the terms can be equally applied to any defined group of people with common affiliations or goals. The term "corporate culture" has been used to describe the culture of people within a firm. This concept came to the forefront of business literature in the early 1980s, when American businesses were in crisis compared to their successful Japanese counterparts who were using different management techniques (Hofstede, 1986). Although no universally accepted definition of corporate culture exists, the literature suggests a wide variety of definitions that share common themes but differ in details.

In the early days of culture popularity, Schwarz and Davis (1981) described methods to match corporate culture with business strategy. They relate anthropologist Clyde Kulckhohn's definition of culture as "the set of habitual and traditional ways of thinking, feeling and reacting that are characteristic of the ways a particular society meets its problems at a particular point in time," with the idea that corporate culture "is reflected in the attitudes and values, the management style, and the problem-solving behavior of its people." They further define culture as "a pattern of beliefs and expectations shared by the organization's members...that produce norms that powerfully shape the behavior of individuals and groups."

Schwarz and Davis argue that leaders are often selected based on their embodiment of these cultural norms, and then face a significant challenge when they are forced to violate these norms in order to influence change in the organization. They state that culture overlaps with structure, systems, and people of an organization, and that any attempt to influence change through these three elements should be compatible with the existing culture.

Deal and Kennedy (1982) conducted a study of approximately eighty companies in an attempt to understand their cultures. They determined that the main elements of culture are business environment, values, heroes, rites and rituals, and the cultural network. They further assert that "a strong culture is a system of informal rules that spell out how people are to behave most of the time" and "a strong culture enables people to feel better about what they do, so they are more likely to work harder."

Hampden-Turner (1990) asserts that cultures are simply responses to corporate dilemmas, and therefore describes the culture of an organization as one that "defines appropriate behavior, bonds, and motivates individuals, and asserts solutions where there is ambiguity." According to this model, every corporation faces daily dilemmas, such as

managing competing priorities, and the culture of the organization should be used to reconcile these dilemmas.

Denison's research studies (1990) present a framework to study the close relationship between the culture of an organization, its management practices, and its future performance and effectiveness. In this study, he refers to culture as "the underlying values, beliefs, and principles that serve as a foundation for an organization's management system as well as the set of management practices and behaviors that both exemplify and reinforce those basic principles."

In Managing People and Organizations, Lorsch (1991) examines the how managers use organizational design to influence subordinates to work toward a firm's goals. In this study, he argues that organization-design changes have more impact if they are consistent with an existing culture. He defines culture in this context as "shared implicit and explicit assumptions that members make about what is legitimate behavior in an organization...The culture includes not only such norms about how people should behave but also the values they are expected to hold."

Kotter and Heskett (1992) conducted numerous research studies in an attempt to tie corporate culture to long term economic performance. As a result of their studies, they describe organizational culture as having two levels. The first, shared values, occurs at a deep level and is difficult to understand, and therefore change. These shared values comprise "important concerns and goals that are shared by most of the people in a group, that tend to shape group behavior, and that often persist over time even with changes in group membership."

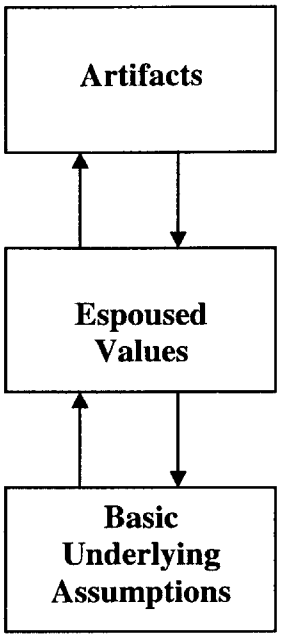
The second level, group behavior norms, are more visible and therefore easier to change. This level comprises "common or pervasive ways of acting that are found in a group that persist because group members tend to behave in ways that teach these practices (as well as their shared values) to new members, rewarding those who fit in and sanctioning those who do not." The authors also indicate that an organization may have many cultures, especially those that are large and geographically dispersed, but the term corporate culture usually applies to "values and practices that are shared across all groups in a firm, at least within senior management."

As evidenced above, many definitions for culture exist. The difficult nature of attempting to define culture is addressed by Hofstede, Neuijen, Ohayv and Sanders (1990). In the introduction to their work on measuring organizational cultures, they admit that "there is no consensus on a definition for culture, but most authors will probably agree on the following characteristics of the organizational/corporate culture construct: it is 1) holistic, 2) historically determined, 3) related to anthropological concepts, 4) socially constructed, 5) soft, and 6) difficult to change."

One definition, put forth by Edgar Schein (1992), appeared pervasive throughout the literature. Schein defines organizational culture as "a pattern of shared basic assumptions that the group learned as it solved its problems of external adaptation and internal integration that has worked well enough to be considered valid and, therefore, to be taught to new members as the correct way to perceive, think, and feel in relation to those problems." Schein further proposes that culture can be defined using the following three levels (Figure 2-1), where the term level refers to "the degree to which the cultural phenomenon is visible to the observer."

- Artifacts: Visible organizational structures and processes (easy to observe, hard to decipher)
- Espoused Values: Strategies, goals, philosophies (espoused justifications)
- Basic Underlying Assumptions: Unconscious, taken for granted beliefs, perceptions, thoughts and feelings (ultimate source of values and action)

Figure 2-1 Levels of Culture (Schein, 1992)



Visible Organizational Structures and processes (hard to decipher)

Strategies, goals, philosophies (espoused justifications)

Unconscious, taken-for granted beliefs, perceptions, thoughts, and feelings (ultimate source of values and action)

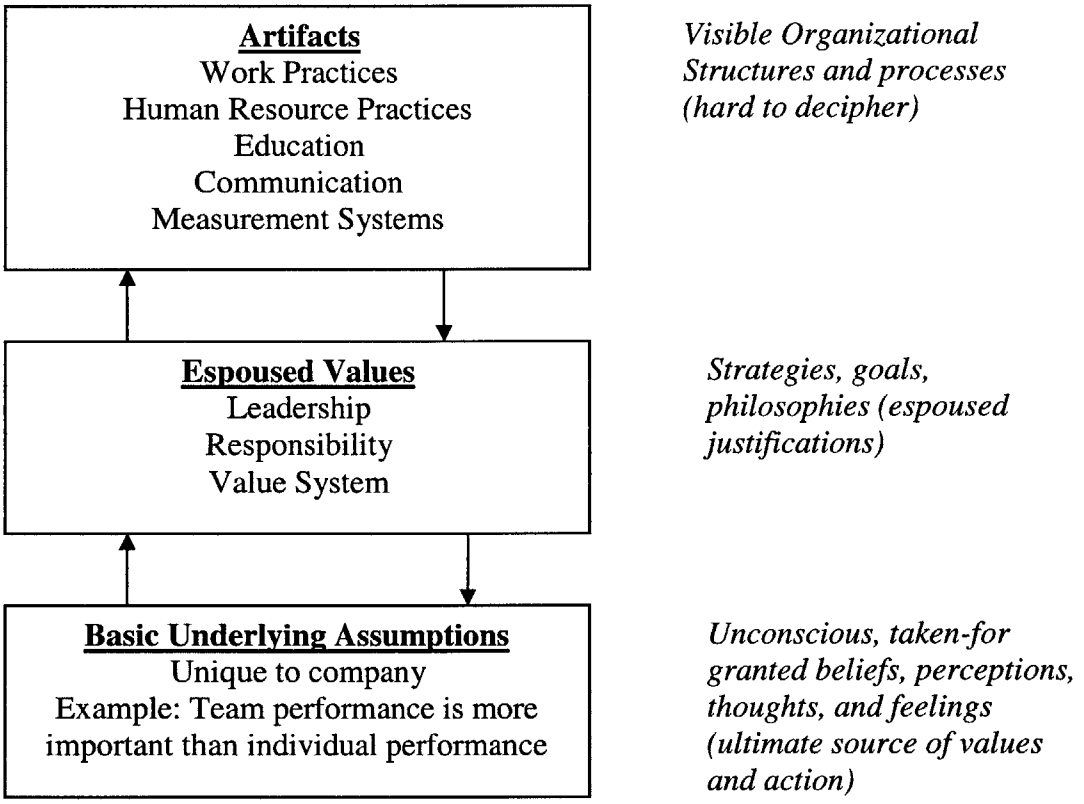
According to Schein, many people mistake artifacts and espoused values alone for corporate culture, ignoring the basic underlying assumptions beneath them. He states, however, that the basic underlying assumptions are the "essence" of culture. Artifacts are items that are easily observed at the surface when someone encounters a new group with an unfamiliar culture. Artifacts are easily observed, but their meaning is often hard to decipher. Espoused values often begin as the reflection of someone's original values, for example the leader of an organization. It is not until these espoused values are acted upon and tested by members of the organization that they become shared values or beliefs. These shared values and beliefs then may be transformed into the third level of culture, basic underlying assumptions. Basic underlying assumptions are so strong that members in a group find behavior that doesn't align with them inconceivable.

2.3 Schein's Modified Framework

In order to further develop Schein's framework, anecdotal examples of artifacts and espoused values were gleaned from the literature to identify items that contribute to corporate

culture, and grouped according to Schein's top two levels, artifacts and espoused values (see Figure 2-2). Common artifacts include work practices and infrastructure, human resource practices, education, communication, and measurement systems. Common espoused values include leadership, responsibility, and value systems, as these three items dictate, explicitly or through example, how members of the organization should behave.

Figure 2-2 Levels of Culture (modified from Schein, 1992)



Note that basic underlying assumptions are unique to each organization, and are therefore difficult to categorize. These assumptions provide members with insight into the basis for the organization's objectives and priorities. Some examples of basic underlying assumptions are that team performance is more important than individual performance, or that designing a company to operate at a financial loss in a capitalist environment is inconceivable (Schein, 1992). Because of their unique nature, it is impossible to generalize basic underlying assumptions of an organization through reading one article about a company, or interviewing one member of a company.

2.3.1 Artifacts

The following section describes groups of artifacts including work practices and infrastructure, human resource practices, education, measurement systems, and communication, with examples drawn from the literature where appropriate.

2.3.1.1 Work Practices

This category covers the broad range of systems and policies put in place by an organization in order to facilitate achievement of their objectives. From the bare bones outline of a job description to an innovative formalized teamwork structure, these practices can provide a sense of organizational culture, priorities, and individual responsibilities. These processes are put in place to help employees make routine decisions in response to predictable events, and may therefore provide the basis for decision-making in unpredictable situations.

Some organizations rely on a corporate program to facilitate their overarching cultural objectives, such as Total Quality Management (quality), Safety Management Systems (safety), or the Toyota Production System (quality, lean). Others will create systems geared toward the organization's goals. At Norm Thompson Outfitters, a clothing catalogue company dedicated to sustainability, they created a Sustainability Action Plan which identified prevention of global warming, toxics, habitat destruction, and waste as the company's top priorities and incorporated them into the their business goals (Smith, 2003). At Toyota, employees are grouped into small teams that are cross-trained to compensate in areas where one employee may be lacking. In addition, managers' span of control is reduced to allow for further involvement in the managers' areas of responsibility (Krafik, 1998). In the Federal Aviation Administration (FAA) Air Traffic Control community, controllers are assigned in teams of two to ensure redundancy in decision-making, a necessary factor in an organization described as having a "high reliability" culture (Roberts, 1990).

Another important aspect of work practices that is conducted formally and informally is experimentation and exercising of cultural values. The experimentation practice happens informally in environments where employees are allowed to try new ideas without fear of retribution. At a General Electric Plant in Massachusetts, for example, one key aspect of a change in the safety procedures of the plant involved allowing employees to present safety-

conscious ideas and act on them without inhibiting oversight from plant mangers (Simon, 1999).

Formal exercises are often carried out in military organizations, in an attempt to follow standard operating procedures to determine if they will be successful in the face of a particular scenario. The U.S. Army in particular conducts intense two-week long training sessions where an organizational unit of 3000-4000 people competes with a like-sized competitor to complete a realistic simulation of conflict. After the exercise, they conduct After Action Reports where members attempt to understand what went wrong, why, and how to prevent it in the future (Pascale, 1997). According to a recent SCRT interview with an automotive manufacturer, their organization conducts war-gaming drills for potential disruption of their supply chains to improve training, knowledge management, and knowledge capture.

2.3.1.2 Human Resources Practices

One way of perpetuating organizational culture is to seek out potential employees that are either inherently aligned with the organizational cultural values, or show a strong propensity to eventually conform to these values. Human resources personnel should clearly define those cultural attributes that the organization values, and look for their manifestation in potential applicants. For example, Toyota tends to seek out young, educated minds that have little experience elsewhere but show the appropriate attitude and potential to learn (Vaghefi, 2000). At Procter and Gamble, the company does not try to oversell themselves to potential candidates, but rather aims to provide their applicants with an understanding of the company and encourage them to voluntary deselect themselves if they do not think they will "fit in." (Pascale, 1985) U.S. Navy Admiral (ADM) Rickover, credited as the father of the navy nuclear power program, bypassed all standard naval recruiting procedures and hand picked sailors he felt would best succeed in the program (Bierly, 1995).

After hiring, some organizations choose to present an employee with a code of conduct that specifically lies within the "value system" of the organization (See Section 2.3.2.3). This code of conduct, along with relevant job requirements, should be used when evaluating an employee's performance for incentives, promotion, termination, etc. If an employee does not demonstrate alignment with the organizational cultural values, action should be taken according to human resource policy (termination, punishment, additional

training, etc). For example at IBM, if an employee commits an act that goes against the corporate culture, they are sent to the "penalty box." This means that they are generally rotated to a less desirable position in order to have time to ponder their actions, and to allow organizational memory to fade so they can be placed someplace more effective for their next assignment (Pascale, 1985).

2.3.1.3 Education

Both new and current employees require regular education not only to understand their job descriptions, but also to remain up to date with an organization's cultural values. This education may be conducted through formal training or more informal socialization. Formal training on the organization's values is often given to new employees upon hiring. At IBM for example, all new Master of Business Administration (MBA) employees and seasoned professionals undergo the same training process at the beginning of their IBM tenure (Pascale, 1985). At Marriott, all employees must go through a weeklong training that deals specifically with the company values. During this training, employees are required to role-play in difficult scenarios that make them apply the company value system to their decision-making process (Pascale, 1985).

In the U.S. military, intense training is conducted in the form of basic training ("boot camp") for enlisted ranks and through Officer Candidate School or military academy training for officers. These training sessions not only focus on the nuts and bolts of military duties, but also on less tangible factors such as leadership, morals and ethics. All recruits in the U.S. Marine Corps specifically must struggle through a 54-hour field exercise called The Crucible. This exercise presents recruits with a series of grueling challenges with little sleep or food, with the intent of instilling pride, teamwork, high energy and most importantly, loyalty to the organization (Katzenbach, 1999).

In those organizations that pride themselves on creating a culture defined by an overarching value, such as safety, quality, or leanness, formal training in these particular areas may accompany job training. This training serves to educate employees on the importance of these values, and how to incorporate them into everyday behaviors within the company. At Norm Thompson Outfitters, for example, they realized that their employees and suppliers didn't really know what the principles of sustainability were. To remedy the situation they

partnered with a non-profit organization to educate every level of employee on the guiding principles of sustainability (Smith, 2003).

Another aspect of education comes in the form of socialization. While the training programs mentioned above have a formal structure, an underlying aim is to socialize employees into the organization's culture. This can also be done informally as well. For example at Toyota, employees are indirectly required to attend many outside social events with their colleagues, a practice in line with Japanese culture (O'Reilly, 1989). At Bain and Company, all junior associates are subjected to what is deemed "meeting overload." Associates are forced to attend many types of meetings-company, office, case team, recruiting, team, social-in an attempt to build cohesiveness within and identification with the firm (Pascale, 1985).

Another important aspect of socialization is the use of folklore in demonstrating an organization's values. In the former Bell system, employees used to share stories about severe conditions that employees had overcome to keep phones working, demonstrating the level of employee commitment in reaching the company's goals. This folklore was so pervasive that in times of natural disaster it empowered Bell employees to cut corners and achieve the extraordinary without being confined by existing corporate bureaucracy (Pascale, 1985). Another example of the power of tradition can be found at Kentucky Fried Chicken (KFC), where new recruits are introduced to the Walk of Leaders, a hall in the Corporate Headquarters that is full of memorabilia commemorating great moments in the company's history (Katzenbach, 1999).

2.3.1.4 Measurement Systems

Once work processes and cultural values have been communicated to current and future employees, a cogent method must exist to measure their success. Without a solid measurement system, employees may feel lost in the performance of their duties. This may also send the message that management does not place emphasis on job performance or alignment with cultural values. Measurement systems may come in the form of adherence to standards or regulations, such as the International Organization for Standardization (ISO) 9000 or Occupational Safety and Health Administration (OSHA) Guidelines. It may also come through measurement systems embedded in programs such as Total Quality Management. At Chrysler, for example, the concept of "quality gates" dictates that if quality

guidelines are not met at certain stages of a project, the project will not move forward (Vasilash, 2003). At Norm Thompson Outfitters, buyers are provided with a sustainability toolkit and scorecard designed to educate them about sustainable principles and provide them with a method of measuring success in their decisions (Smith, 2003).

Another method of measuring success in adherence to cultural values is through the use of audits or assessments. These audits involve looking at such things as statistical performance, employee reviews, and perception questionnaires. Several consultants offer cultural assessment models that utilize these methods, such as The Simon Open System Culture Change Model (Simon, 1999) and the K.L. Strategic Change Consulting Group's Corporate Change Model (K.L. Strategic Change Consulting website, 2005).

2.3.1.5 Communication

Communication on two levels, internal and external, plays an important role in an organization's culture. Internally, employees need to know what should be communicated, in what time frame, and how to do so. For example, Sears holds town hall meetings in an attempt to communicate in a straightforward manner to all members of the company (Pascale, 1997). The standard presentation format at IBM is through the use of flip charts, where common practice is for the audience to probe the presenter with questions (Pascale 1985). Air traffic controllers use a very specialized language to pass information along in a timely and accurate fashion.

Another aspect of internal communication involves feedback to employees on their performance. At Intel, the "constructive confrontation" method encourages employees to deal with disagreements in an immediate and direct manner. At Shell, the company uses "valentines," a concept borrowed from Ford, to facilitate communication and conduct conflict resolution. Valentines are regular gatherings of salaried and hourly employees where they are encouraged to air grievances and work together to propose solutions. A similar process of "creative conflict" is utilized at Johnson & Johnson (O'Reilly, 1989). The After Action Reviews conducted by the U.S. Army and described above, provide an open environment for identifying what went wrong during an exercise and how to address shortcomings (Pascale, 1997). These accepted methods of communication provide a comfortable forum for effective communication within the organization.

External communication can also be extremely important when dealing with supply chain issues. If a company holds particular cultural values above others, they must inform their suppliers and incorporate these values into their decisions making processes. An SCRT interview with one technology company described their feeling that personal relationships and reciprocal knowledge builds reliable relationships, obviating the need for flexibility agreements in contracts. At Norm Thompson Outfitters, their buyers educate and partner with their supply chain partners to make sustainability based decisions and potentially change the way products are manufactured or selected for inclusion in their catalogues (Smith, 2003). Effective external communication is a key tool in ensuring that cultural values are supported throughout the supply chain.

Internal and external communication can also play an important role in the resilience of an organization in a crisis situation, as evidenced by the supplier fire that severely threatened the performance of mobile phone handset producers Nokia and Ericsson. A fire in March of 2000 at a Philips plant in Albuquerque New Mexico destroyed the manufacturer's inventory and many items in production. Philips notified both Nokia and Ericsson, their primary customers, within three days; however word traveled very differently within the companies. Nokia's culture encouraged bad news to travel fast, and the situation was briefed up the chain of the command almost immediately despite the initial report that the plant would soon be back up and running. This rapid communication allowed Nokia to work closely with Philips and other suppliers to come up with a solution to their shortages. At Ericsson, the news traveled much slower, and the head of their mobile phone decision didn't hear about the problem until early April. At this point it was too late to overcome the severe shortage of chips, and Ericsson withdrew entirely from the mobile phone handset production business shortly thereafter. In this example, the encouraged method of communication at Nokia, aimed at uncovering problems as soon as they arise, led to the ultimate success of Nokia over Ericsson in the industry (Latour, 2001).

2.3.2 Espoused Values

The following section discusses leadership, responsibility and value systems. These items are grouped under espoused values since they project an understanding of how an organization's members should act, either explicitly or by example.

2.3.2.1 Leadership

Leadership style plays a large role in any cultural endeavor. Leadership may manifest itself in the form of general leadership principles within an organization, or a specific person or organizational unit designated to carry out the application of cultural ideals to the depths of an organization. An example of the former would be organization-specific leadership principles that get passed on through educational programs. An example of the latter would be a Chief Executive Officer (CEO), a department head, or a person charged with implementing a functional culture, such as a safety or quality officer. While not every organization can be blessed with an omnipresent or powerful leader, the most important aspect of leadership when inculcating cultural values is demonstrated commitment to those values. Those in leadership positions must not only communicate an organization's cultural values, but they must demonstrate them continually through their decision making process. A leader who declares cultural intentions but does not back them up will most likely not gain the trust and support of those he is trying to influence.

For example, at one General Electric plant, a decline in safety performance was adversely affecting employee morale and productivity. A series of safety officers attempted to instill new safety leadership and programs, but it wasn't until a cultural audit was conducted that they realized that managers and labor force had conflicting ideas about the safety at the plant. While they both knew that the safety record was lacking, the managers had a more positive outlook than the laborers in areas such as incentives and rewards. Once these differences were identified, a productive process changed the safety culture of the plan dramatically (Simon, 1999).

A strong leader can make an enormous difference in an organization's culture and its success. An extreme example of the power of one specific leader comes in the form of Rick Rescorla, the Vice President of Corporate Security at Morgan Stanley. A decorated Vietnam Veteran, Mr. Rescorla not only predicted the 1993 World Trade Center bombing, but created an evacuation plan for the company that was exercised, often begrudgingly, many times by its employees. Mr. Rescorla used this expertise and authority on September 11, 2001 to help 2700 well-trained Morgan Stanley employees evacuate the towers. As a result, only six Morgan Stanley employees perished that day. Unfortunately, Mr. Rescorla was one of them (Grunwald, 2001).

Another example of extreme leadership can be found in Admiral (ADM) Rickover of the United States Navy. ADM Rickover is called the "father of the nuclear navy" and is credited with spearheading creation of the first nuclear submarine and the nuclear navy as a whole. He was obsessive about the quality of his employees and the standards of the nuclear program, going above and beyond normal navy hiring regulations and hand screening every officer applicant into the program. ADM Rickover continued to exert his powerful influence over the ships, technology and personnel of the nuclear navy for three decades (Bierly, 1995).

A final example of strong leadership can be found within Lucent Technology's recent shift. Mr. Jose Mejia, President of Lucent Supply Chain Networks, initiated a dramatic shift in that company's supply chain management practices by focusing on the company's culture. He introduced a "burning" platform that focused on the dire state of the company and used its proud history to inspire people to change the way they did business. He focused on alignment through the use of the phrase "kill snakes." A "snake" was anything that was not in alignment with the organization's cultural values, and his attitude was that snakes needed to be put on the table immediately, and dealt with, i.e. "killed." Finally, Mr. Meija consistently emphasized honest, open communication between employees at all levels and stages of product management, as well as between Lucent employees and their suppliers (Scholtz, 2004).

2.3.2.2 Responsibility

Another important aspect of organizational culture is responsibility. In order for cultural values to penetrate the organization, all members must feel responsible for upholding these values. If an employee does not feel that upholding the cultural values affects their employment, promotion, or status, then they may not feel obliged to do anything. In high reliability organizations, such as the nuclear community of the U.S. Navy and the FAA air traffic control system, extremely high levels of responsibility are required at the operator level so that each operator understands the consequences of their actions (Bierly, 1995).

The level of responsibility must also be clearly tied to incentives (or disincentives) for certain behavior. For example, At 3M, the "15% Rule" allows employees to spend 15% of their time engaged in researching their own ideas that they feel may eventually be useful to the company. This rule, along with money provided through "Seed Capital" and "Genesis Grants", help stimulate an environment of innovation (Studt, 2003).

Another important aspect of responsibility ties into the leadership principles discussed above. In many cases, it is important to have a single person or group that is charged with ensuring that cultural values are demonstrated at all levels of the organization. The placement within the organization affects the way that it is viewed throughout the organization, for example a security department that falls within the compliance group may be treated differently than a security department that falls under operations. These differing perspectives often depend on the cultural values of an organization.

2.3.2.3 Value System

Many organizations have an explicitly stated value system in the form of a company mission statement, code of conduct, core values, or motto. These values generally offer a clear and concise manifestation of the company's values that may be used to provide motivation or aid in the decision making process. Some better known mottos include Hewlett Packard's "The HP Way," Ford's "Quality is Job 1," and the "Delta Family Feeling." Each military service embeds their cultural values within their "core values." For example the U.S. Navy and Marine Corps' "honor, courage, and commitment" and the U.S. Coast Guard's "honor, respect and devotion to duty" are used at all levels of training to inculcate cultural values in their new recruits' mindset. In addition to these succinct and often catchy value systems, many organizations will draft a more comprehensive mission or value statement that covers multiple specific topics and is well-publicized throughout the organization.

3 Methodology

This chapter discusses different methods of studying culture, and provides a detailed summary of the methodology used during this study. The chapter also summarizes the observations of the study, which are discussed in further detail in following chapters.

3.1 Studying Culture

According to Schein, culture may be studied three ways (Schein,1992a). The first, the survey research approach, approaches culture through identification of "deep" conceptual definitions of culture such as "mental models" or "basic assumptions," but then attempts to quantify culture through individual questionnaires. This, Schein states, forces data into certain dimensions and addresses culture only on a superficial level.

A second method of studying culture, the ethnographic approach, originates in anthropology and sociology. Use of this method assumes that culture reaches into such depths of an organization, that they must be extensively observed and interviewed. The result of this is a "thick description" of culture, but according to Schein, it ignores the conceptual and definitional problems of the concept of culture.

The third method of studying culture, and the one used in this study, is called the analytical descriptive approach. Using this approach, one breaks culture down into specific components that are easier to measure and describe. While this approach is practical for research purposes, Schein argues that this focus on the manifestations of a culture's "deeper" phenomena do not address the core concepts of an organization's culture. This argument supports the focus of this study on observed artifacts and espoused values, with suggestions of basic assumptions that should be present for a supply chain security culture.

3.2 Methodology

While none of the three methods described above provides a perfect method of studying culture, the analytical descriptive approach fit well with the research goals of this study. The research for this thesis was conducted in two phases. Phase one entailed a comprehensive literature review of supply chain security and organizational culture, as presented in Chapter Two. This literature review included work conducted to date as part of the Massachusetts Institute of Technology (MIT) Supply Chain Response to Terrorism (SCRT) Project. The literature on organizational culture theory was then used to develop a framework with which to analyze data to be collected in phase two.

During phase two, a questionnaire was created based on this framework and used to conduct interviews with senior security executives at twenty-one manufacturers, distributors, and transportation providers. Two additional security and risk consultants were interviewed about their general experiences in the field. In order to protect the confidentiality of interviewees, their titles have been generalized, and companies are referred to throughout this study as Company A through Company U. Table 3-1 provides fundamentals of each company, including industry, generalized title of interviewee, approximate range of annual sales, and approximate range of employees. The companies interviewed varied in size, industry, and nationality, but they all maintain a major presence in the United States.

Companies were chosen based on information previously known about their high security or resilience performance, and on their anticipated ability to contribute to the study. Most companies either had a prior relationship with MIT's Center for Transportation and Logistics (CTL), or expressed desire to participate in the study based on information provided on the CTL website. This thesis does not claim to be a statistically significant study of several companies, or a random selection of companies representing all industries, rather a hand-picked groups of companies chosen based on the above-mentioned criteria.

Interviewees were senior executives charged with security responsibilities. Although most of the interviewees were charged with security and not business continuity planning responsibilities, they were all questioned about both programs. This was done to gauge security executives' awareness and involvement in business continuity planning efforts.

The questionnaire, provided as Appendix B, included twenty-four questions addressing supply chain security practices, business continuity practices, and corporate

culture. The interviews were semi-structured in that the response to each question dictated the follow-up question. Not ask all questions were asked of all interviewees, nor were the questions included on the questionnaire the only ones asked. If a specific item warranted further discussion, additional question were asked. Additional questions and answers were recorded in brackets in the transcribed interview reports.

Table 3-1 Company Fundamentals

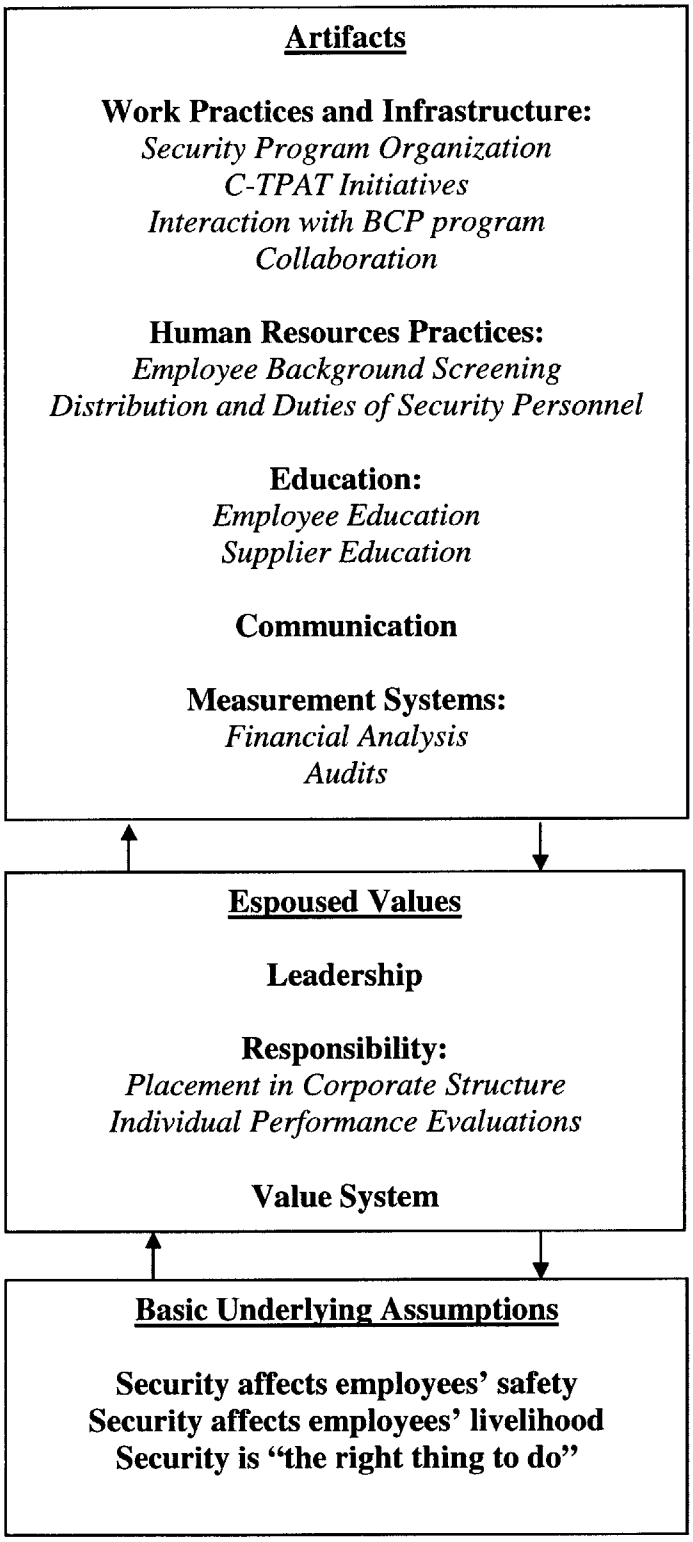
Company Name	Industry	Range of Annual Sales (billions of $)	Interviewee Title	Range of Employees (thousands)
Company A	Grocery	10-50	VP of Asset Protection	200-250
Company B	Marine Shipping	1-10	VP of Security and VP of Customer Service	NA
Company C	Railroad	1-10	Assistant VP for Customer Service	10-50
Company D	Electronics	1-10	Security Manager	10-50
Company E	Automotive	150-200	Security Administrator	300-350
Company F	Consumer Products Manufacturer	10-50	VP of Corporate Security	10-50
Company G	Toys	1-10	Director of Corporate Security	10-50
Company H	Automotive	0.1-0.5	Risk Assessment Leader	NA
Company I	Computer Hardware	50-100	Security Manager	150-200
Company J	Computer Services	50-100	Director of Security	350-400
Company K	Electronics	10-50	Director of Security	50-100
Company L	Food	10-50	Senior Director of Security	100-150
Company M	Apparel	1-10	Senior Vice President	100-150
Company N	Footwear	10-50	Senior Business Continuity Analyst	10-50
Company O	Marine Shipping	10-50	Security Officer	1-10
Company P	Marine Shipping	1-10	Director of Governmental Policy	NA
Company Q	Pharmaceutical	50-100	Director of Security	100-150
Company R	Footwear	10-50	Director of Import Operations	1-10
Company S	Computer Hardware	1-10	Director of Supply Chain Security	10-50
Company T	Retail	10-50	Manager of Operations and Investigations	300-350
Company U	Transportation Services	10-50	Director of Security	350-400

1) Source: Hoover's, Inc.
2) Some titles and Industries have been generalized
3) NA = Not Available

3.3 Summarized Observations

Upon completion of the interviews, observations were distilled into artifacts and espoused values that contribute to creating a supply chain security culture, and grouped according to the modified Schein framework presented in Section 2.3 (3-1). Chapter Four describes select observations categorized as artifacts, while Chapter Five describes select observations categorized as espoused values. Chapter Six then suggests three basic underlying assumptions that support a supply chain security culture. Appendix C provides a detailed matrix summarizing observations from these interviews.

Figure 3-1 Supply Chain Culture Artifacts, Espoused Values, and Basic Underlying Assumptions (modified from Schein, 1992)



4 Artifacts

Schein describes artifacts as visible organizational structures and processes. These are items that are easily identifiable, especially by a person who is unfamiliar with the organization. As a result, artifacts are often used to describe an organization's culture. Although artifacts are easily observed, their true meaning is often difficult to decipher. The framework depicted in Figure 3-1 categorizes artifacts into five major groups. Four of these groups also contain sub-groups that are specific to supply chain security. This chapter describes supply chain security artifacts, organized under the following groups and sub-groups.

- Work Infrastructure and Practices
    - Security Program Organization
    - Customs Trade Partnership Against Terrorism Initiatives
    - Interaction with Business Continuity Planning Programs
    - Collaboration
- Human Resource Practices
    - Employee Background Screening
    - Distribution and Duties of Security Personnel
- Education
    - Employee Education
    - Supplier Education
- Communication
- Measurement Systems
    - Auditing
    - Financial Analysis

4.1 Work Infrastructure and Practices

Work practices encompass the broad range of systems and policies put in place by an organization in order to facilitate achievement of their objectives, which for the purposes of this study is supply chain security. The initial framework includes items such as teamwork, systems design, and experimentation. Phase two of this research, however, focused on the infrastructure that these work practices took place in. This section summarizes work

infrastructure and practices common to many companies that had the most effect on supply chain security programs. This section also includes supporting observations where appropriate.

4.1.1 Security Program Organization

Every company who participated in the study has an established security program, although not necessarily one dedicated to supply chain security. These programs are generally administered at corporate headquarters, and are often divided them into segments including physical security, personnel security, supply chain security, information technology security, and investigations. The corporate security staff ranges from one person to many, and they are usually charged with creation and dissemination of security standards, educating employees, conducting oversight, and conducting investigations into security incidents. Some companies also operate 24-hour security centers where they keep track of world events and intelligence that may help them predict or respond to incidents that occur.

Although corporate staff maintains oversight of these programs, most companies delegate responsibility for implementation of the programs down to the field level. At this level, the senior business manager at each location is held responsible for ensuring the security program is being followed. This manager may report to a regional or country security manager, depending on the size and global distribution of the company. The local business manager may also be assisted by full- or part-time security personnel who are either employed by the company or a third party firm specializing in security. The distribution of security personnel is discussed further in Section 4.2.2.

With this common structure, the corporate staff often acts as a consultant to their field personnel. At Company J, for example, security is the responsibility of the process owner, not the security group, as demonstrated by their Director of Security who refers to himself as a security consultant. He provides security support for those organizations that deal with product development and all of their research efforts, and tries to keep senior executive management in those lines of business current on the kind of threats and exposures that they face as a business.

At Company F, security is considered a corporate function, and the corporate staff members are also viewed as in house consultants. Each Company F operating entity is responsible for security, which, according to their VP for Corporate Security, is both good and

bad. Their principle manufacturing sites have full time security managers, but they are the exception to the rule. According to this VP, "in the rest of our manufacturing sites and in just about every one of our value chain locations, [security] is a collateral duty. So we have to then not only oversee this function, but also train and support the man or woman that is wearing the security hat for 10-15% of their time."

The Investigations Manger for Company D views their security program as consisting of two completely separate organizations, one in their operations division that includes production, logistics, and research, and another in their headquarters, that includes sales, finance, and information technology. The operations side of the program is very formalized, while the headquarters program is much more informal. The Investigations Manager on the headquarters side works often with their area and country security managers, traveling internationally at their request to assist with specific problems.

4.1.1.1 Influence of Safety Program

Many security programs are modeled after existing safety and environmental health programs, and therefore share the same structure. Safety programs are also generally administered at the corporate level, with field personnel in place to implement and monitor the program's effectiveness. The field personnel may be charged with safety duties full time, but are often responsible for safety on a part-time basis along with other duties, including security. Accountability for adherence to the safety program is relegated to the general manager at a facility, along with other programs such as security or quality. Safety programs also usually include an audit process that may be conducted in conjunction with the security program (see Section 4.4.2). Finally, safety programs usually have a strong regulatory component, often based on standards set forth by the Federal Occupational Health and Safety Administration (OSHA) or other local governing bodies. Although technically a voluntary program, Customs Trade Partnership Against Terrorism (C-TPAT) plays a similar role as OSHA in providing very broad security standards.

Company O, for example, established an International Standardization Organization (ISO) 9000-based program in the late 1980's to monitor the safety of their vessels. They have since expanded this program twice, first to include environmental aspects, and a second time to include security challenges. This process allowed them to utilize existing policy and procedures to address their security objectives in a timely and familiar fashion. Company P

has used their existing safety, health and environment committee to provide a conduit for security reporting.

The presence of an established safety program often assists in encouraging employees to embrace of a security program, since they often share common characteristics such as providing a workplace free of internal and external threats. While safety programs generally focus on preventing accidents from within, security programs spend more time trying to prevent external disruptions to their facilities.

At Company E, safety and security work hand in hand, as safety is one of the company's overriding values. The safety and security programs utilize the same communication methods, and often stand on committees together to evaluate new projects. Company E views safety as a means to protect their assets, primary their people. According to their Security Administrator, "[Company E] employees know that corporate is going to protect you, provide you with a safe work environment. It's really drummed into you. I think people feel that security is part of that."

The respondent from Company I feels that safety and security overlap in many areas. An example of using this overlap to mitigate safety and security risk came at a time when Company I's employees and customers were concerned about potentially hazardous materials coming in to the workplace through the mail. Company I's safety personnel combined their technical know-how of hazardous materials with the security personnel's knowledge of threat assessment, to design a screening process for all packages coming into Company I facilities.

As a railroad, Company C has a deep historical safety culture. This culture pervades both the field and office-based activities, where personnel conduct safety briefings before each meeting or job begins. Company C relies on their safety program when handling hazardous materials and equipment, but they also rely on their security program to understand the origins and detailed information about handling shipments. According to their Assistant VP for Customer Service, "security is becoming a higher priority because people are starting to realize that security is an integral part of safety as a broader concept."

Safety concerns may also be used to help justify security investments. At Company D, for example, the Investigations Manager uses safety concerns to implement security measures at the field level. According to him, "safety is a huge thing at this company and if I can show that there is a safety need in the company, [the security measure] has a much better chance of getting through."

Although the presence of a safety program often helps facilitate security, some companies view the distinction as blurred. The VP of Security at Company B views the line between safety and security as very thin at the field level, since "some of the conventions for security were some of the same conventions that were in place before for safety reasons." At Company G, the safety program is viewed as having an advantage over security, since the safety program is backed by regulations while the security program, and C-TPAT, are still viewed as voluntary. As a result of this difference, the company relies on a company mandate to abide by security regulations, rather than employees' inherent knowledge that the mandate is backed by regulations.

Although safety and security overlap in many instances, some firms prefer to keep the two disciplines separate. Company F, for example, maintains a strong safety culture, presumably as a result of their strong manufacturing background. The success of this program is reflected in their low injury rates and numerous OSHA awards. Despite the success of this program, the company keeps the two disciplines separate except in areas where they are forced to overlap, such as building evacuation. From their VP for Corporate Security's perspective, "I'm in no hurry to go down that road [combining safety and security] because we're not staffed up for it and there is a whole knowledge basis there. I think we're large enough that we can keep it discrete."

Company Q also maintains a strong safety culture, as is common in the highly regulated pharmaceutical industry. While they recognize that safety and security overlap at the site level, they feel that at the corporate level there is less overlap than in other industries. According to their Director of Security, "I think this is the changing nature of security...I think security should be a full time job in many places, and not part of the safety effort, they're different. For a smaller company it might make sense to combine the two, but for a larger company it does not."

4.1.1.2 Influence of Quality Program

Quality programs also integrate with security programs at the field level, although to a lesser extent than with safety. The majority of overlap between the two programs comes in two areas, auditing and incident analysis. Many companies have quality auditing teams that visit their facilities on a regular basis. In some cases, these teams have been charged with additional security requirements, in order to avoid expending resources on additional teams

(See Section 4.4.2). Another area where security programs have adopted quality methods is the approach and analysis of security issues (See Section 4.4.1).

At one company, security has switched from partnering with safety to partnering with quality. Company L's main focus is protection of their product, so they felt that the quality group was the most responsible for the quality of their product. As a result, the security program partners with the quality group to develop security standards in their framework. According to their Senior Director of Security, "[quality] has been ingrained since day one at [Company L], so it was a natural thing to hitch our wagons to quality, then its an already accepted practice, we don't have to reinvent the wheel...we live and die by quality."

4.1.2 Customs Trade Partnership Against Terrorism (C-TPAT) Initiatives

Every company we interviewed, with the exception of one, identified the Customs Trade Partnership Against Terrorism (C-TPAT) initiative as a core part of their security program. The United States Customs and Border Protection Department (U.S. CBP, formerly known as U.S. Customs) instituted the Customs-Trade Partnership Against Terrorism (C-TPAT) program in November 2001, and updated it in March 2005. This public-private partnership was born out of CBP's recognition that close cooperation with industry would be paramount to providing the highest level of supply chain security in the wake of the September 11, 2001 terrorist attacks. C-TPAT aims to engage the private sector in securing the global supply chain in exchange for streamlined inspection processes.

In order to become C-TPAT validated, applicants must submit a self-assessment of their supply chain security practices to CBP, addressing such areas as physical security, personnel security, education and training, access controls, manifest procedures, and conveyance security. In addition to this worksheet, importers are told to "develop and implement a sound plan to enhance security procedures throughout your supply chain. Where an importer does not control a facility, conveyance, or process subject to these recommendations, the importer agrees to make every reasonable effort to secure compliance by the responsible party" (U.S. CBP website, 2005). This significant aspect of C-TPAT ensures that members do not focus solely on their own facilities or those in the U.S., but that they address their entire global supply chain. The majority of companies view the cost of not

complying with C-TPAT, in terms of effect on speed-to-market, as the main driver for participation in the program.

In general, the larger companies with established global security programs view C-TPAT as a means to document procedures already in place, educate suppliers through contractual requirements, improve relations with CBP, and gain competitive advantage by being subject to fewer inspections. The respondent from Company D, for example, feels that they have benefited from C-TPAT through being forced to document security procedures that were already in place. According to their Investigations Manager, "in most cases we're doing what we need to do from safety and security standpoint, but what we're doing has not been properly documented. C-TPAT has forced us to document what we're currently doing." When Company K applied for C-TPAT certification, CBP conducted an on-site validation process and accepted their security program as is. According to their Director of Security, CBP commented that they had "evolved security to a science, and that [Company K] had the best program they had seen to date."

Smaller companies with fewer resources, or companies with a lesser concern for security, have used C-TPAT as a guideline to create or strengthen their existing programs. Company G, for example, views themselves as a low-risk importer with high volumes of low-value product that don't justify extensive security investments. They realize, however, that if they do not comply with C-TPAT, they will no longer be considered a low-risk importer and will potentially be subject to additional inspections. From the security standpoint, this threat from C-TPAT has allowed the company to institute security initiatives that may not have been accepted otherwise.

Company R has relied heavily on C-TPAT to shape their current security program. Company R does not own any manufacturing facilities, so their security concerns lie heavily on their U.S retail stores and distribution channels. According to their Director of Import Operations, C-TPAT was a starting point for conducting risk analysis and putting controls in place to mitigate that risk. This process was put in place, despite limited resources. This Director states, "it seems that when C-TPAT occurred there was a cottage industry of people coming in saying they were security professionals and we didn't have much of a budget so we tried to socialize it more to use our existing resources."

Most companies indicate that C-TPAT has at the very least raised awareness throughout the company about the need for security. Company B's VP of Security, for

example, stated that C-TPAT has "raised awareness and provided guidelines for people in terms of evaluating their people, process and technology for security....[Executives] all now understand C-TPAT, so when we talk about our business, they have C-TPAT in the back of their mind."

At Company S, C-TPAT has also helped with awareness and the treatment of security as a priority. According to their Director for Supply Chain Security, "What [C-TPAT] has done is solidified the need for a dedicated supply chain security group within the global security organizations. That didn't exist prior...When I needed people, I would have to compete for time with their manager...and now I have my own people. I think C-TPAT helped that."

4.1.3 Collaboration

Collaboration also plays an important role in creating effective security programs. Observed formal collaboration efforts fall into three broad categories: internal collaboration between a company's organizational units, external collaboration within the industry, and external collaboration with government.

Most internal collaboration with security comes in the form of leadership councils at the senior executive level. These councils include senior security managers and other members of the company's departments (i.e. Finance, Legal, Operations, Human Resources, etc.), and provide a forum to give input into company decisions involving security. For example, Company J formed a Global Trade Council to address supply chain security, and C-TPAT implementation in particular. This Council comprises the VP for Import Compliance, the Director of Security, and the VP for Government programs. According to their Director of Security, "a big part of my job is working with executive management in the various lines of business to convince them that they need to be implementing appropriate security measures in their areas." At Company F, security has collaborated internally with the Legal, Audit, Value Chain, Risk Management, and Business Continuity Planning departments to form a Loss Control Committee that tracks supply chain related losses.

Company L also created a North American Security Council, whose purpose is to " bring everyone from legal to procurement to quality to distribution, manufacturing and transportation together to discuss and make sure people have security on their radar screen." This model has worked well in North America, specifically dealing with C-TPAT issues, and

they are in the process of developing similar councils in countries throughout their global supply chain.

This internal collaboration often leads to improved training and awareness. Company M has charged a wholly owned-subsidiary charged with supply chain compliance across a variety of areas including security. This subsidiary collaborates with security, sourcing, and transportation, and develops training and development guides for their field personnel with support from their supply chain partners. When they decided to conduct security training for personnel charged with loading containers, for example, they asked their distributors to identify best practices and suggestions, and adopted some of these for their own programs.

Another area where some progressive security groups collaborate internally is with sourcing. At Company Q, for example, Security created a reputation for collaboration through assisting the Legal Department, their parent division, with items such as investigations. As a result of these collaborative successes, security has been asked to conduct other functions, such as providing input into choosing service providers. This opportunity to provide input on potential suppliers has allowed security to become part of the strategic process. According to their Director of Security, "a large part of our success at [Company Q] relates to the quality of our security staff and how integrated we are with other business units."

Company S also collaborates internally on logistics decisions. According to Company S's Director of Supply Chain Security, "I view logistics as my customer. 100% of my time is devoted to supply chain security, so I have an intensive amount of interaction with them." This manifests itself in several ways. Company S's security personnel get involved in the request for quote (RFQ) process, and no decisions are made regarding selection of a provider without security's input. Company S will also not consider entering a just in time (JIT) hub, unless the location has been screened and accepted by their security program. Company T also provides input to their transportation department regarding sourcing decisions. According to their Manager of Operations and Investigations, "we now are able to support our transportation partners by saying you know a certain merchant, it's not a good idea going there because of a security point of view."

The second level of collaboration involves industry-wide initiatives. Security officers often collaborate with their counterparts across different industries through security-specific associations such as the International Security Management Association (ISMA) or the Overseas Security Advisory Council (OSAC). Many companies have also entered into

collaborative partnerships with their direct competitors to identify problems, solutions, and best practices regarding security issues facing their industry.

Company E, for example, collaborates with other automotive manufacturers and suppliers through the Automotive Industry Action Group (AIAG), a group that has been in existence since 1982 to discuss quality issues. Company U, along with other small parcel carriers, participates in the Postal and Shipping Coordination Council. This group has helped to open doors for communication in the event of a security related incident.

Both Company M and Company N address security issues through an industry group called Retail Industry Leaders Association (RILA). RILA's goal is to "bring the key executives from the most innovative and successful retail and product manufacturer companies in the industry together in unique forums to learn from each other and industry experts, advocate for the best course of action in public policy for the industry, and work to advance the reputation of the retail industry as a whole" (RILA website, 2005). Company O works closely with the World Shipping Council to discuss security issues. The World Shipping Council is an association representing the liner shipping industry whose member lines operate more than 90% of the industry's vessel tonnage serving America's foreign commerce (World Shipping Council Website, 2005).

Company K is a member of the Technology Asset Protection Association (TAPA), an association of security professionals and related business partners from high technology companies who have organized for the purpose of addressing the emerging security threats that are common to the technology industry (TAPA website, 2005). Company I has also worked with TAPA and the Alliance for Gray Market and Counterfeit Abatement (AGMA) to combine data from several companies to conduct statistical analyses of losses.

Despite these collaborative efforts, companies differ in their view of security as a competitive advantage. Company O, for example, will eagerly share information if they feel that sharing will serve a useful purpose for them. When the 24-Hour Rule was initiated (see Appendix A for a brief description of this program), they openly shared the process they created to manage the immense documentation issues. They shared information because the new rule posed such a threat to the industry, that they recognized that helping other companies deal with it effectively would positively affect their business. Company E collaborates with other automotive companies on security issues; however, they treat their security best practices as a competitive advantage and therefore do not share them.

Finally, companies collaborate at different levels with government authorities. Company C, for example, has its own, fully deputized law enforcement force that often partners with state and federal authorities to ensure secure operations during rail incidents or special events. Company E works closely with the U.S. Coast Guard and the State Police at their corporate headquarters to share security related information. Company E has also allowed law enforcement agencies to put antennas on the roof of their highest buildings, they make a point to meet with local police departments regularly, and they use their 24-hour crisis information center to produce a global daily intelligence bulletin that goes to all of their executives as well as law enforcement partners.

At Company A, one of their directors in the Asset Protection group has formed a relationship with officials at the U.S. Food and Drug Administration (FDA) and various government agencies charged with protection of America's food supply. These officials contact him often to discuss new threats and regulatory issues. According to their VP for Asset Protection, "the Chairman understands how important it is to our business to have someone plugged into D.C. with the credibility and respect and they know if they call him, they will get the truth."

Not all companies, however, find collaboration with government beneficial. Marine carriers, in particular, expressed concern about the government's influence on their operations. Company B, for example, struggles with whether or not to collaborate with the government, due to their experience with government's erratic responses to security incidents in the past. Company O also expressed frustration at the inability to predict the government's response to potential threats. One example of an incident that caused concern is the 2004 "Lemongate" incident that took place outside the Port of New York and New Jersey. In this incident, an email sent to the U.S. Department of Agriculture indicated that a shipment of lemons on a ship bound for the U.S. could be contaminated with a biological agent. As a result of this email threat, the ship containing the lemons was forced to sit outside the port for seven days while various government agencies determined the best course of action.

In addition to these concerns, two companies indicated concerns about reporting information to the government. Company B has received multiple government contacts that they are required to notify to report an incident or intelligence-related information. This has reduced their confidence that intelligence information is being well managed behind the scenes. Company O indicated that their personnel will often provide U.S. Customs with

suspicious information, but that they rarely received feedback notifying them of how a particular issue was resolved. This lack of consistency has reduced these companies' confidence that incident reporting is being effectively managed by the U.S. government.

4.1.4 Business Continuity Planning Integration Initiatives

Most companies we spoke with have a Business Continuity Planning (BCP) program. BCP programs have historically focused on information technology, but are more recently expanding beyond these boundaries. BCP programs are charged with maintaining operations through implementing responses to disruptions. This effectively inserts resilience into a company's operations, including its supply chain. Since BCP affects all areas of the company, ownership of the BCP program is often assigned to cross-functional committees at the executive level. Because of the cross-functional nature of BCP programs, however, ownership is often ambiguous. These cross-functional committees identify potential threats and vulnerabilities and craft exercise disruption scenarios to identify potential response and mitigation efforts. Responsibility for these exercises usually falls on the shoulders of local or regional emergency response or crisis management groups that report to the BCP leadership. These emergency response groups are managed at the regional, country, or local level, and focus more on immediate crisis response and less on actual resumption of all business functions.

The degree of interaction between security and business continuity programs at both the corporate and field level varies greatly. The majority of companies recognize that security and business continuity should go hand in hand, and work together to develop plans at the executive level. Some companies do admit, however, that their BCP program is an area that needs much improvement.

The companies with strong BCP programs recognize the need for buy-in from all departments, including security, to respond to a crisis situation and ensure continuity of the business. At Company I, for example, safety, security and contingency planning work closely together to ensure the safety of their personnel during a crisis. At Company Q, the security program has initiated their company's business continuity efforts, utilizing their Global Security Operations Center to draft a generic business continuity plan that can be modified for each site to address crisis management, crisis recovery, and business continuity planning. Company U uses a Crisis Management Committee, either chaired or co-chaired by security, to

respond to disruptions. This Committee is made up of representatives from the Risk Management, HR, Operations and Legal departments. Subdivisions within the committee deal with every discipline in the company. At Company K, security actually owns the emergency management program and provides infrastructure to help the emergency operations centers respond.

Company C's centralized BCP program addresses two types of crises: immediate disasters, for example, from fires or computer viruses, and those with some advance warning, such as hurricanes or planned system disruption. At this centralized level, security is integrally involved with relocating work to other areas, starting up in an initially unsecured environment, and getting security measures in place once the business is up and running. On the local side, Company C's decentralized facilities rely heavily on local plans. As a result, when disaster strikes a yard or terminal, the Company C police force and Regional Response Teams are the first responders. A good example of this type of response was during a tunnel fire in a major metropolitan area. During this incident, Company C security personnel worked closely with the local police department to ensure rapid and effective response to the fire. Company C's departments worked closely together during the response, taking a conservative approach to ensure the safety of city's people and surroundings.

Company E also integrates their business continuity and security programs through their emergency response group and business response group, who manage local business resumption plans and emergency response teams respectively. The emergency response and business resumption groups run annual tabletop drills for each group that address crises of all kinds, including transportation, fire, etc. A tabletop drill is one where parties meet to discuss their potential response to a given scenario, but do not actually act anything out physically. These exercises are conducted locally, and escalated as necessary. If a local response team cannot handle a crisis, management moves up to country and regional teams. A corporate emergency response teams exists for the more extreme responses, and it integrates the CEO and the Legal, Human Resources (HR), and Information Technology (IT) departments to tackle the most difficult of situations. Company E also utilizes their 24-hour crisis center to help coordinate responses.

Not all companies have BCP programs that are integrated with security. Some have extensive security and business continuity programs, but that only interact when making recommendations to each other. At Company M, for example, BCP falls under the Logistics

Group, and their wholly owned subsidiary that is charged with implementing and enforcing security regulations only gets involved when making recommendations of potential scenarios to consider in their plans. At Company G, the business continuity program historically resided in the IT department, but they recently initiated a pilot program to include all aspects of getting a facility up and running again, including the IT, Facilities, HR, and Security departments. Although this initiative is not spearheaded by the security program, they have remained involved.

Many companies recognize the need for integration with BCP, and that their particular programs need improvement. Company J, for example, has a strong emergency planning and response planning group, but their focus on business continuity is only really robust in the IT department. According to their Director of Security, "that's an area where, using some of [MIT's] specific research, as a matter of fact, we've been able to convince the integrated supply chain that they need to have a continuity plan for that entire organization." Despite the lack of initiative in that area, security does feel that they will be a member of that team when it happens.

Company B is another company that feels that their BCP program needs improvement. According to their VP of Security, "we do have business continuity plans in place...but it's an area that [Company B] really needs to beef up...we've spent a lot of time on the critical locations, but not so good a job in terms of the less critical. I personally believe we need to refocus our efforts and do a better job in that area."

4.2 Human Resources Practices

This section describes two important human resources practices that affect supply chain security programs: employee background screening and distribution and duties of security personnel.

4.2.1 Employee Background Screening

One of the most significant aspects of instilling a cultural value in an organization involves selecting personnel who have values that inherently align with those of the organization, or who demonstrate the capability to adjust accordingly. While it is standard

practice at many companies to conduct a background screening process that examines employees' personal background and former employment, some take this screening to a higher level and include personality tests. The results of this background screening process allow the employers to determine if the employee would be a good fit within the organization and its culture. Although many companies already utilize background screening to make the most effective hires, C-TPAT has brought the issue to the attention of security executives for the purposes of their own companies and their suppliers. C-TPAT includes employee background screening as an important requirement of their validation process.

Company J, for example, used to apply background screening criteria only to their own personnel in their facilities, but they have recently extended this, as permitted by law, to their suppliers' employees. They have also used C-TPAT as a vehicle for requiring their suppliers to conduct background checks on their employees. According to their Director of Security, "the possibility that one of our products or shipments could be used as a conveyance for something other than our product has caused us to look at [background screening] completely differently."

Extending background screening to suppliers is important, but not widely practiced. The Director of Import Operations at Company R describes this dilemma, "obviously we do background checks as part of our response, we go through more than routine background checks for all employees that we hire, but the issue is what about subcontractors and third party providers... we do it, but it doesn't help us doing that in the U.S. because we have to push out the borders."

Another aspect of employee selection is seeking specific experience that will bring desired competencies to the company. This method is used primarily to identify strong candidates for security-specific positions within a company. At Company F, for example, the VP of Corporate Security formerly worked for the U.S. State Department. This position provided him with a skill set that has worked well with the company's corporate objectives. As a result, Company F continues to seek out personnel who have worked internationally, and specifically within the State Department. Company T also seeks personnel with international experience, and a variety of law enforcement experience, including the Central Intelligence Agency (CIA), the Federal Bureau of Investigation (FBI), and the U.S. military. They feel that

this wider variety of experience, combined with international exposure, result in a level of comfort with the global nature of Company T's business.

When looking to hire security-specific personnel, Company K pulls from the premiere law enforcement agency of regions where they operate. They do this because they recognize that their background will bring invaluable country-specific knowledge to the job. According to their Director of Security, "it's not going to do any good for someone with my [American] background to talk to Israel; you need linkages back to the country."

Sometimes a company may not require specific experience, but may seek out aptitude in areas important to their security program. Company Q's Global Security Group, for example, seeks out people with investigative experience who are comfortable conducting risk assessments and investigations, or who show aptitude to learn those competencies. They also look for personnel with certifications, such as Certified Protection Professional (CPP) or Certified Fraud Examiner (CFE), as proof of competencies.

4.2.2 Distribution and Duties of Security Personnel

Security personnel are globally distributed across regions and countries to meet security objectives. While the distribution and duties of personnel differ on some levels, common themes present themselves. As discussed in Section 4.4.1, the corporate security program usually resides at corporate headquarters, with security personnel scattered throughout global facilities as warranted. Most companies also have full time security managers at the regional or country level.

Security personnel located at facilities are either full or part time, depending on the location, size, risk, and activity of each facility. Part time security personnel often hold other responsibilities, usually Safety or Human Resources. As we see throughout this study and discussed in Section 4.1.1.1, safety duties align well with security duties since they overlap in many areas. The most significant of these areas is providing a safe and secure workplace. A secondary reason why these duties often overlap is their regulatory nature. Personnel that are used to navigating complex safety regulations such as OSHA standards, or people in the

Human Resources department who deal with regulatory issues every day, are easily able to understand security guidelines that may be imposed based on corporate or C-TPAT standards.

At Company F, for example, each principal manufacturing site has a full time security manager, but at their smaller facilities and those of their partners, the security manager is a collateral duty for another manager on site. These collateral duty managers hold a number of different positions, including HR, Finance, Administration, and Environmental Health and Safety (EHS). Company B maintains a small corporate security group, regional security managers, and many field personnel. The field personnel are either full time or collateral duty, depending on the size of the facility.

Company J uses a different model, maintaining that security is the responsibility of each and every employee. As a result, they do not have dedicated security personnel, but rather integrated supply chain employees who have security as one of their many responsibilities. According to the Director of Security, " through many years of experience, I've found that if you have a separate function or organization having that responsibility, and they are separate from the entity or the particular division that we're trying to protect, it does not work."

At Company O, the security program has the ability to promote as many regional or country security officers as they see fit. Instead of picking a number and trying to reach that, they actually look for people who are competent advocates for security, and assign them the position. They then empower that person to employ as many people as necessary within the organization to get the job done.

Some companies contract out their security personnel to third party providers, while others feel that they have more control when the security personnel are direct employees of the corporation. At Company E, for example, they outsourced their global security function in North America to a security provider. When they initially outsourced, they experienced a communication disconnect. They eventually realized that this was due to the lack of a Company E manager in place to oversee the third party personnel. As a result, they put regional and division security supervisors in place who worked with the third party to ensure that the company's security objectives were being met.

Company U also does not like to use outside contractors for their security positions, because they feel that it takes outsiders a long time to understand their business. They also feel that part of an effective security program is working with people, making contacts, and cultivating sources for intelligence. According to their Director of Security, "you have to know your operation; it's like a police officer on the beat. Most crimes aren't solved by crime scene investigation-type of work...most good cops have a couple of sources that they can rely on, and we try to employ the same type of strategy, to get close to the people."

4.3 Education

Supply chain security-focused education takes place on two important levels, internally within the company, and externally with a company's suppliers.

4.3.1 Employee Education

Every company we spoke with conducts some type of employee education regarding security. At the most basic level, this training takes place as part of the new employee orientation program, where security is included as one module among many. Employees must attend this training, or sign a document stating that they have read and understood the company policy on security, within a specified time period from the initiation of their employment.

Many companies we spoke to have taken this security education further and required that all their employees participate in regularly scheduled security training. The Internet is a very useful tool in administering training to all employees throughout a company. Internet training is available at any time, allows employees to conduct the training when convenient for their schedule, and provides an accurate record of when employees completed the training.

Company I, for example, requires each employee to take an on-line environmental, health, safety and security course that provides the employee with background information on each program, defines their responsibilities, and provides them with resources and contacts for assistance. At Company B, all corporate personnel must take an Internet-based security training module, while terminal personnel follow standards set by the Maritime

Transportation Security Act (MTSA) of 2001 and the International Ship and Port Security Code (ISPS) (See Appendix A for brief descriptions of these programs). Company Q requires general security training for their new hires, and they offer a security awareness course for voluntary training. They only administer this training if requested, however, since they feel that it is most effective of the people being trained really want to learn.

Company L offers an online training program based on commercial software. This program includes five modules that employees must complete within 30 days of employment. This training is then supplemented with annual training seminars. At Company O, nobody is allowed to continue with their job after the 30-day mark without having taken a C-TPAT awareness course. This consists of a three hour online course that provides a description of the history of terrorism, the C-TPAT program, and their company's role in the program. This course also requires a test at the end, and employees must receive 80% or more to pass.

Despite Company S's heavily supply chain-focused strategy, they realized that their general employees didn't have a solid concept of what supply chain means. They therefore created a training program focused solely on supply chain. This 24-hour course, which includes a security module, was initially created for executives, but is now offered to all Company S employees upon request.

In addition to conducting corporate security training at headquarters, some companies travel to their global facilities to conduct regular training with field security personnel. Company F, for example, conducts security road shows on a regular basis. They have had more than 100% participation in these trainings, meaning that security employees are bringing their bosses to learn about security. Company I also recently started a regional training program where they bring all their site security officers together to conduct training on a broad range of issues, from physical security to workplace violence.

Companies without a substantial security budget or personnel must rely primarily on socialization to imbue the importance of security into their employees' decision making process. Company R, for example, has a limited security budget. As a result, they've tried to socialize security, instead of enlisting third party firms to get them into compliance with C-TPAT or conduct audits. According to their Director of Import Operations, "when C-TPAT occurred...we didn't have much of a budget so we tried to socialize it more to use our existing

resources." Company J has also focused on socialization to educate their suppliers, rather than using an iron hand. They feel that this approach has been much more effective, especially with their suppliers.

4.3.2 Supplier Education

In addition to educating their own employees, many companies have made great efforts to educate their suppliers. As discussed further in Section 4.1.2, many companies now put C-TPAT security requirements in contracts with suppliers. This has resulted in improved supplier understanding of security expectations. For some companies, the security education stops there. Certain proactive companies have taken it a step further, however, to ensure that their suppliers understand the importance of security throughout the organization.

This additional effort often comes in the form of supplier conferences. These are held at overseas facilities, or in a neutral location where all the security personnel from a certain country or region can gather to conduct training. Company J, for example, held an Asian supplier conference where they intended to "scare their suppliers into action." They used this training opportunity to discuss threats, supplier experiences, security measures, and prior incidents. Throughout this program, they purposely made it a point to not focus on C-TPAT, since many of their suppliers didn't know what that was, but to focus more on their company-specific security requirements. As a result of this training, security personnel formed work groups that continue to address security issues throughout the region.

Company G conducted a similar conference with 130 of their Asian suppliers. In order to increase buy-in from the suppliers, they invited local government officials to the training. Company M conducts several levels of training with their suppliers in country groups of factories, and with individual factories that struggle. They do this because they feel that "audit-only training programs are ridiculous, and that 80% of effort in all successful programs should be in the training."

Company E maintains a strong focus on educating their suppliers about security. They require all of their logistics carriers to be C-TPAT certified, but they understand that by doing so, they have to assist them with compliance. Company E has therefore used C-TPAT as a vehicle for getting suppliers to conduct self-assessments of their own security programs. They

are trying to promote C-TPAT objectives to their suppliers as well, but recognize the difficulty in this since often their suppliers serve many other companies.

Company S conducts extensive security training with their freight forwarders, in the hopes that they will in turn educate their suppliers. Their goal is to ensure that when any of their forwarders' personnel are handling Company S product, they are thinking of security. According to Company S's Director of Supply Chain Security, "if this disconnect [between Company S and their forwarders] is visible to the customer, I pay the bill."

4.4 Measurement Systems

Measurement systems are necessary to quantify the success of security programs. Two forms of measurement stood out during our research, the use of financial analysis and auditing. Companies use financial analysis to determine what areas need the most attention, and the effectiveness of existing measures. Audits help to ensure that security standards are being followed, and provide visible reminders to employees of the importance of adhering to the security program.

4.4.1 Financial Analysis

Many of the companies we interviewed use financial analysis to justify security investments, although specific analytical methods vary widely. In general, those companies that feel security must be viewed as part of the business realize that they must rely on analysis to make their case to corporate leadership. Another purpose of conducting financial analysis is to formally tie security into the company's overall objectives. Some of these analyses include risk assessment, cost of delays due to security inspections, measurement of historical or potential losses in order to identify high-risk areas ripe for mitigation, and use of Six Sigma™ methods to analyze security-specific incidents.

The Investigations Manager at Company D, a Certified Public Accountant (CPA), conducts his financial analysis primarily through quantifying the cost of delays of raw material and finished product at borders, as well as potential losses through gray market diversion. He states "I've tried to make security concerns a part of the business process to show that a good approach to security problems can lead to one of two things: a safer working environment and a better financial outlook long term."

Company T has put extensive time and effort into measuring the cost of border delays and its effect on the company's bottom line. They have assessed the direct cost of inspection delays at border crossings per container, including forecasts of their projected container growth. These numbers based on delay alone are significant, and would most likely increase substantially when you add in the harder to quantify indirect cost to the overall company for not getting product on time. Company S, for example, estimates that indirect costs affect the company's bottom line 5-7 times more than the direct loss to the company.

Some additional steps Company T has taken include securing a promise from the company President that if a supplier is not adhering to their security requirements, they will cease to do business with them. They have also pursued technology such as radio frequency identification (RFID) that has a clear business purpose, and provides increased security as a by-product. According to their Manager of Operations and Investigations, "our first job is definitely security, but our focus is in the business in terms of sourcing and selling."

Company J relies on an in-depth incident tracking system to demonstrate the need for security to upper management. They can provide incident data on a real-time basis to different groups in the company indicating problems in their line of business, and how can they work with them to address them. Their Director of Security feels that this works better than a person from the security group coming in and saying, 'I have a law enforcement background so you should listen to me.' According to this Director, "we find it is critical that you're an integral part of business and can show the value added to your client in terms of them taking advantage of the security resources we bring to the table."

Company J has also used C-TPAT to broaden their security program beyond the logistics process. For example, as part of the C-TPAT validation process, Company J analyzed their U.S.-Mexico border crossing procedures and realized that, from a security standpoint, they were utilizing too many storage yards for trucks waiting to cross the border. As a result, they decided to combine their yards. This decision not only helped them ensure the security of their trucks, but also increased efficiency of the border-crossing process. According to their Director of Security, "ultimately we believe we're going to help the business not only from a security standpoint, but also from the standpoint of identifying business efficiencies by focusing attention on supply chain security."

At Company A, The VP of Asset Protection states that the company is very driven by return on investment (ROI) driven, but that their senior management treats the soft benefits of certain investments, such as safety and security, as equally important as financial numbers. As an example, they described an initiative to install digital closed circuit television (CCTV) systems in all of their retail stores, even those that have not recently been renovated or remodeled. Although this might cost the company tens of millions of dollars, they have been able to present the additional benefits of digital CCTV to the company, and they feel 85% sure that the initiative will be passed. This VP states, "if the senior executives didn't hold [security] in such high priority, I don't know that we would be able to accomplish everything we have since 9/11. A lot has to do with buy-in of upper management."

Company A's security program was also recently moved under the Supply Chain Group. This move was made because the analytically driven Supply Chain Group is very could provide resources to help quantify the impact and ROI of various security initiatives. Some methods of doing this include measuring the effect of various preventative strategies on losses, and how these would impact the success of failure of various initiatives. This process has always been used within the company for food safety, but more recently for security.

Many security groups have taken the risk assessment function on internally, relying on instead of relying solely on centralized corporate risk assessment groups. Company I, for example, has found that expressing potential losses through statistical methods is very difficult, so they have focused on measuring actual losses. As a result, they have been able to demonstrate very solid numbers about what has been lost, and how security measures have reduced losses. They have also employed trending and analysis based on information from their global claims database to identify high-risk areas. In one instance, they were able to identify that their trucks were being targeted at rest areas within a 200-mile radius of a specifically vulnerable area. This risk assessment allowed them to implement policies for drivers to not stop at rest areas within these 200 miles, greatly reducing losses in that area.

Company F uses a spreadsheet-based tool called an "asset protection tool" to identify areas requiring security investments at the local level. This tool is used widely throughout the company to rank security measures at facilities. Five versions of the tool exist, for use at different facilities such as manufacturing, transportation, or commercial office spaces. Use of this tool has become so widespread that employees regularly discuss their "asset protection tool" scores, and these scores are included in performance evaluations. Company F has also

built use of this tool into contracts with their suppliers, some of whom have used it to make operational decisions surrounding their facilities. In addition to this tool, Company F has a multidisciplinary Loss Control Committee that tracks supply chain related losses to "get better visibility against what we're losing, where we're losing it, why and how, as well as to develop counter measures." This Committee includes representatives from the Security, Value Chain, Legal, Audit, and Risk Management departments.

Despite efforts to quantify the effect of security on the company's bottom line, some companies indicate that they have received less support since the terrorist attacks of September 11, 2001. At Company E, for example, they had no problems justifying security expenditures post September 11, 2001, but as time passes it has gotten more difficult. They look closely at government programs such as the Container Security Initiative (CSI) to justify expenditures based on security benefits from tracking their material. According to their Security Administrator, "to justify expenditures, if they say you can save money because you're tracking your supplies, then logistics can use that type of savings to justify the expense, and we acquire security as a by-product." They also state that security expenditures are much more easily justified when beginning a project, rather than modifying an existing facility or process.

Several companies conduct financial analyses, but always view security as a cost-added function. Company F, for example, uses their "asset protection tool" as described above to drive local spending, but they say these efforts "are never going to get a return on investment." The VP for Security at Company B also thinks that arguments for security improving efficiency "are good in terms of hypothetical, theoretical, conceptual thinking...[but] I can't give too many examples of security initiatives that make us more efficient."

Only one company we spoke with clearly views security as a revenue provider. Company O maintains that additional security costs to comply with C-TPAT and other security regulations since September 11, 2001 have amounted to less than $1 per twenty foot equivalent unit (TEU). These costs, however, have been outstripped by additional revenue that has been brought in through marketing security as a new service area. According to Company O's Security Officer, "[security] has created a new product line for us. In fact, any cost that we've had to date has had an equaling return on investment, so as of this moment...we've been able to cost justify any expenses."

Company P has also seen some unexpected benefit from increased security regulations. They initially feared that the 24-Hour Rule would constitute a huge added cost to the company (see Appendix A for a brief description of this program). They did incur costs to comply with the program, for example opening a 24-hour operations center, but as a result they no longer have to chase their customers for information, or print dummy bills of lading with incomplete information. Instead of increasing costs, the rule has forced Company P and their customers to be much more efficient in their documentation processes, which has reduced company costs. The company has used the success of this initiative as an example to gain strength for other security initiatives.

Another method used to conduct analysis, although not specifically financial, is Six Sigma™. Two firms we spoke with have adopted Six Sigma™ practices to analyze security incidents affecting their firms. Company I analyzes security events using 7-step problem solving, to determine why the event occurred and what corrective actions should be put in place to prevent reoccurrence. For example, when they encountered security issues in the warranty program, they formed a team of business and security personnel to meet with a high level quality Six Sigma™-trained Black Belts to resolve the problems. The results of this analysis were presented to the senior level of management, and will be used to create additional programs and processes in this space. The use of these methods aligns well with certain aspects of their corporate culture, specifically the company's analytical nature rooted in its engineering heritage.

Company S also uses Six Sigma™ methodology to address security issues. For example, they have used root cause analysis of the losses over a period of years, to come up with security requirements language to use in their contracts. All Company S executives must attend Brown and Black Belt level training, so security issues are understood across the company when using this common language. According to their Supply Chain Security Director, "we're a very metrics driven company, we subscribe very heavily to the Six Sigma™ methodology, and in order to be a Director at Company S, you have to have taken the 160 hour Six Sigma™ Black and Brown Belt level course...It helps all of us understand what the cost impacts are. We measure everything."

Some companies do not conduct financial analysis at all. Company M has not bothered conducting financial analysis of the effectiveness of security measures, since they feel that any delay is unacceptable and that further analysis would be a waste of time.

Company G indicated that they have not used financial analysis since nobody from the corporate leadership has asked for it. Finally at Company L, they purposely do not conduct centralized financial analysis so that security spending decisions remain at the local level.

4.4.2 Audits

The majority of companies we interviewed conduct some form of auditing to ensure that their security program standards are being applied and followed. Audit teams are usually composed of corporate personnel who are either located full time overseas and conduct regular audits, or who travel to each global location from a central location on regular intervals. Some companies hire third parties to conduct these audits, but the majority keeps control of the audits within the company. Many of the companies we interviewed have added to their existing financial, safety, or quality auditing programs to address security requirements. These teams are trained in basic security principles, and have added security items to their existing audit checklists. This technique has allowed many companies to obtain C-TPAT compliance with limited costs.

Company G, for example, utilizes an existing quality assurance (QA) auditing team who visits their facilities in the Far East four to five times a year. They initially hired a third party to conduct their security audits, but realized that the quality of their internal audits exceeded those of the third party so they discontinued the use and cost of these extra personnel. At Company L, the security program has capitalized on the quality principles engrained in their culture this to meet security objectives, specifically through the auditing process. They have trained quality auditors, who already regularly visit their global facilities, to be aware of security issues.

Company M has trained their administrative and financial auditing teams in security practices, and they feel that utilizing this existing resource has helped them implement C-TPAT requirements with minimal cost. Company B also conducted training with their financial auditing team to observe security practices during their facility visits. This company, however, purposefully uses third party auditors, in addition to their internal audit teams, to conduct security–specific audits. Their goal in this process is to ensure that security issues are not overlooked by Company B auditors who are extremely familiar with each facility. At Company D, the global safety auditor who regularly visits all of their facilities looks at physical security items and reports back to headquarters regarding any significant issues. If he

does find a significant issue, the manager for special investigations will visit the facility, along with the global safety auditor, to address it.

Company A conducts asset protection audits that deal with such issues as security, store sanitation, and food safety. They use these audits to train managers on their responsibilities in each area. The process they use includes familiarizing managers with the audit program, conducting a mock audit, and then encouraging managers to conduct self audits in order to identify areas of weakness. According to their VP of Asset Protection, the "goal of an audit is not to catch people doing things wrong, but to catch them doing things right." In this industry, where high turnover is common, this audit process has proven to be a useful tool to keep employees aware of security responsibilities.

Only one company explicitly addressed expanding their auditing capabilities from their facilities to those of their suppliers. Company F has done this through securing the right to audit and conduct investigations at their suppliers' facilities. They have worked internally with their Value Chain department to ensure that when their security auditors arrive at their supplier's doorstep, there will be a previously arranged understanding of their intentions.

4.5 Communication

Effective communication is fundamental in conveying the importance of security to all members of an organization. Every company in the study communicates their security objectives to employees, customers, and suppliers using varying methods. One of the primary means of communication is through company Intranet sites. Company sites are updated regularly with security information, and employees are encouraged to access these sites on a regular basis.

At Company O, for example, if an important issue comes to the forefront of the company's concerns, they will post a bulletin on their global homepage that can be accessed by all of their employees. Company K uses a similar method, posting interesting issues or cases on their internal corporate homepage, but their interface also allows employees to post questions and receive answers electronically in a timely fashion. Other common methods of communication include security briefs, reports, newsletters, and hotlines.

Some companies, specifically those with 24-hour operations centers, conduct routine intelligence gathering and disseminate intelligence updates to their employees, external

partners, and government authorities as necessary. This is especially helpful for companies with scattered global operations to keep apprised of political happenings near their facilities. Company E, for example, distributes intelligence information to their executives and local law enforcement on a regular basis. Company T also globally distributes regular intelligence bulletins that track international incidents in the countries where they operate, as well as activity surrounding U.S. embassies or major religious buildings near their facilities. One example of the success of this process took place in Jakarta in 2004. The company's operations center decided to focus on Australia, when they heard that elections would be happening there in the near future. At the same time, they noticed an increase of related activity in Jakarta, and sent a message about that to their office there. The next day, a suicide bomb went off outside the Australian embassy in Jakarta.

Regardless of the methods used to communicate security information, many companies expressed the importance of communication as a key factor in the success of their security program. Company D, for example, communicates security information to their employees through a safety and security hotline, email notices, and General Safety Committees that are located at each facility. When a security issue arises, such as creating a corporate drug testing policy or responding to a specific threat, they use these channels to communicate with their employees, exchange valuable information, and identify best solutions. Their Investigations Manager sums up their overall philosophy with "the more you tell [the general population], they more you find out about what you want to know."

Company F regards communication as one of the five pillars of their security program. This communication focus includes a robust internal corporate website and monthly emailed travel advisories, as well as regular security briefings at facilities. This focus on communication has "removed the whole idea of 'nobody ever told me,' or 'we've always done it that way.'...people know where to go now, whereas before [security] was a bit more nebulous or never addressed."

Company E relies heavily on their Communications Group, who has representatives at each of their facilities, to distribute security related information to their employee base. Company A has used the U.S. Food and the Drug Administration (FDA) guidance to build a security awareness program for their stores. This program included a series of posters placed in stores common areas depicting suspicious situations, and information with how to address

them. Although Company A hasn't explicitly measured the campaign's effectiveness, their VP of Assets Protection feels that it has definitely increased exposure.

5 Espoused Values

Schein defines espoused values as strategies, goals, and philosophies, that when combined form espoused justifications. An example of this might be a belief of a certain group member that may or not become a group assumption until acted upon and/or proven, or an organization's espoused values that may or may not be in line with what the company actually does (Schein, 1992). As discussed in Section 2.2, espoused values often begin as the reflection of someone's original values, for example the leader of an organization. It is not until these espoused values are acted upon and tested by members of the organization that they become shared values or beliefs.

Leadership, responsibility and value system are categorized under espoused values because they dictate, either explicitly or through example, how members of the organization should behave. The different levels of leadership within an organization embody role models for the general population. The responsibilities assigned to the members of an organization also help them to understand how they should behave, specifically during performance of their duties. Finally, the value systems communicated to the general population of an organization act as guidelines for use during the decision making process. The following espoused values that apply to supply chain security are discussed in this chapter:

- Leadership
- Responsibility
    - Placement in Corporate Structure
    - Individual Performance Evaluations
- Value System

5.1 Leadership

As discussed in Section 4.1.1, most companies have a corporate security program that is led by a senior security official. The level of this person varies from company to company, but they include Vice Presidents (VPs) and Directors, and are often considered an integral part of the executive leadership.

When security officers are located one or two levels below the Chief Executive Officer (CEO) in the corporate hierarchy, they often make great efforts to maintain their voice through direct communication with their leaders. For example, the VP for Corporate Security at Company F reports directly to the Chief Financial Officer (CFO), who sits on the CEO's Operating Committee. This ensures that security is discussed at this committee on a regular basis. At Company M, the security program reports to the Executive VP for Law, who is a member of the senior leadership team, and also makes security a regular agenda item at each meeting.

While the presence of a senior executive charged with security is important, the general corporate leadership must also express commitment to their security agenda to all levels of the company. At Company I, for example, every employee is provided with a security policy that is signed by the CEO. This one page document describes the company's philosophy and emphasizes the fact that security is everyone's responsibility and affects the company's overall performance. At Company Q, the CEO holds security as a high priority and communicates the importance of security to the organization on a regular basis. Surprisingly, only about a quarter of the companies in the study identified support of the CEO as an integral part of their program.

Company J includes security as a key part of their business conduct guidelines, and employees are reviewed on the basis of these guidelines throughout their tenure, so they feel that its importance is ingrained in every employee from day one. As a result of this demonstrates commitment, the security program is viewed as driven from the Chairman and CEO. At Company T, the Assets Protection Group has received commitment from the

President of the company to sever relationships with suppliers who are not meeting security requirements set forth in their contracts

At Company A, the Chairman himself made the decision to move the Assets Protection program from reporting to the General Counsel to the Supply Chain Group. In addition to this level of involvement, the results of asset protection audits are placed on an executive level dashboard that has helped inspire other members of the senior leadership to pay attention to security issues. According to their VP of Assets Protection, "if the senior executives didn't hold [security] in such high priority, I don't know that we would be able to accomplish everything we have since 9/11. A lot has to do with buy-in of upper management."

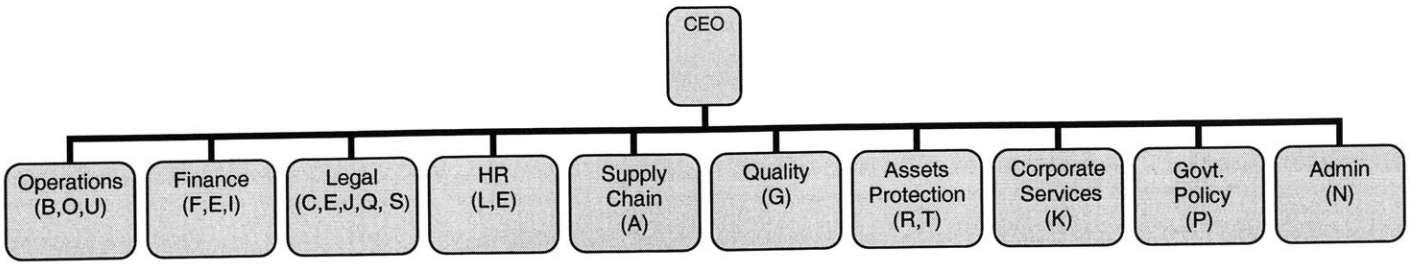
5.2 Responsibility

Responsibility for security takes place at two distinct levels in the corporate structure. The first level is the corporate security program that creates standards and conduct oversight to ensure those standards are being followed. At this level, the security program's placement in the corporate structure affects the way it is viewed by the company, and therefore its leadership's ability to manage the program. At the local level, responsibility for overall security falls on the general manager of a location who is also charged with all other aspects of that locations performance. At this level, individual performance objectives play an important role in security program implementation. In addition to individual performance measures, incentives are also often used to encourage employees to embrace security objectives.

5.2.1 Placement in Corporate Structure

There appears to be no standard reporting structure for corporate security programs. Across the twenty-one companies interviewed in this study, security reports to ten different corporate departments (Figure 5-1).

Figure 5-1 Generalized Security Reporting Structures



Note: Letters represent companies with security reporting to that department. Security programs reporting to multiple departments are included in each department, and companies where the security program reporting structure is unknown are not included.

Three of the most common reporting relationships encountered were Finance, Operations, and Legal departments. At Company F, for example, the VP of Corporate Security reports to the CFO, because historically the security function of Company F grew out of a risk management and theft prevention mindset. He also feels that his position under the CFO has "fostered some reporting and communications that maybe weren't there before. People know where to go now, whereas before it was a bit more nebulous or never addressed." At Company I, the security program reports to the CFO, and security is therefore considered a financial function. As a result, their Security Manager thinks that they are structured as a group within the company to try and explore more of those business issues, including counterfeit, gray market, supply chain, and warranty fraud.

At Company B, security falls under Operations. They view this as essential since they are an operations driven company. This affiliation also allows the security leadership to be taken seriously when making a recommendation to an operations manager, as opposed to if the recommendation were coming from HR or another administrative group. At Company U, their security program reports to the Senior VP for U.S. Operations, who is a member of the Board of Directors and is the Senior Operations Manager reporting to the Chief Operating Officer (COO). Security once resided under Business Development in that company, but they shifted to Operations within the last four to five years because so much of what they do relies on the operators' cooperation. At Company O, security falls under Operations. According to their Security Officer, this placement fits their objectives well because "security is really a

business process issue, and finance and compliance people are generally lawyers and accountants. How to secure the supply chain may not necessarily be in their toolkit."

Company C considers security a legal function. Their Executive VP for Law is charged, among other things, with legal responsibilities, corporate communications, compliance, and security. This placement fits well within the company, since they have a fully deputized law enforcement group that often interfaces with local, state, and federal law enforcement agencies. Security at Company S also reports to the Legal department. Their Director of Supply Chain Security feels that this location gives them "teeth" to do the things they want to do, such as conducting investigations and being involved in contracting with supply chain partners. He also feels that this placement is much more effective than human resources or facilities would be. For example, in line with their legal function, Company S's security personnel conduct almost 100% of the investigations that take place across the company, from the IT department to the Audit department.

At Company P, the Director of Governmental Policy is charged with security, and he reports directly to the CEO. After September 11, 2001, the company decided to give security responsibilities to this Director, since they viewed security concerns as primarily a regulatory problem that would require frequent interaction with the U.S. government. This Director then appointed the senior business official in each region as the people charged with security, because he felt that these people were already tied into the corporate culture, versus new positions brought in from the outside.

Company E's security program reports jointly to the CFO, General Counsel, and Human Resources department. This multiple reporting structure benefits security in different ways, since their policy and procedures branch aligns closely with HR, while their investigations arm aligns more closely with the Legal and Audit branches. The Security Group at Company L also reports to the VP of Global HR Strategy, who then reports to HR. They feel that this placement works well within the company, since HR is very influential in the company. According to their Senior Director of Security, "typically not much gets done without HR's blessing, they have a foothold on the organization, and they are pretty powerful."

Company T has a designated Supply Chain Assets Protection (AP) Group. This group contains three divisions: a stores environment, an operations environment, and a supply chain environment. The larger AP Group is charged with ensuring the security of Company T's

people, products, and buildings throughout the world and relies on a culture of "safeness," which is discussed further in Section 4.1.1.1. The AP group has identified twelve different groups within Company T that affect security, and they spend a lot of time coordinating with these groups in order to maximize effectiveness.

Company M has created a wholly owned subsidiary as an independent organization charged with implementing and enforcing compliance issues such as security, risk mitigation, quality issues, labor standards, and country of origin laws. Company M formed this subsidiary to ensure objectivity in their compliance processes. The Senior Vice President of this subsidiary reports directly to the Executive VP of Company M, who is the President and CEO of Company M's logistics services.

At Company A, security falls under the Asset Protection Group, who reports to the Supply Chain Group. Before 2005, however, the security program reported to the General Counsel. The Chairman of the company decided to make this shift since the Supply Chain Group is run by a very analytically driven Executive VP. AP at Company A also includes many responsibilities, including safety, food safety, environmental protection, quality assurance and store sanitation. These functions are bundled together because they are all compliance driven and require familiarity with working with regulatory agencies.

At Company K, security resides within Corporate Services which includes, among others, Environmental, Health, and Safety, and Facility Based Services. This group resides under the Technology and Manufacturing group, which is largest group at the company and is responsible for manufacturing and delivering services associated with manufacturing the product. Their Director of Security finds this placement beneficial because "it allows us to interact with our customer base more efficiently. We're not beholden to legal aspects or HR, we're seen as a service provider, rather than one business group in our organization."

5.2.2 Individual Performance Evaluations

Performance evaluations are a common measure of responsibility for employees. In general, security-specific personnel within companies are regularly evaluated on their adherence to security objectives, but this accountability rarely extends to the general employees of the company. Some interviewees expressed an interest in requiring security metrics to be included in employee performance objectives, but this does not appear to be widespread.

At Company U, their vehicle drivers are measured on security metrics, including stolen vehicles and loss occurrences. Company U has a very low tolerance for security lapses, and will terminate employment if they feel a driver has been negligent in adhering to security protocol. At Company D, they feel that their focus on communication to convey the importance of security to their employees imposes a certain level of responsibility on them. Employees, if properly informed, cannot claim ignorance of a specific issue that has been communicated to them numerous times through various channels.

At Company I, security is part of everyone's evaluations. Each employee is required to take an on-line environmental, health, safety and security course, and completion of the course is factored into performance evaluations. Company I has also introduced a security component to their driver performance evaluations, especially in high risk areas. In areas where security has been an issue, this change has resulted in behavioral change. According to their Security Manager, "drivers say they have been written up for not following guidelines, and they now appreciate what Security has been doing."

Another way that individuals or groups are judged on their performance of security objectives is through financial incentives. Company N, for example, utilizes a corporate program to influence employees' security actions. In this program, a certain percentage of employees' compensation is based on meeting performance objectives at both the company and individual level. Security objectives are included in this, so employees have a clearly defined stake in whether they follow them. Company U, for example, offers a one-time incentive program, where they will pay a $5000 reward to personnel who bring security related information to the attention of the company. This program effectively communicates the importance of security to Company U personnel, and provides incentives for them to become more aware of their surroundings.

Company L has recently developed a security awareness initiative. This program involves distributing brochures and other training materials to facilities, and provides a website that employees can access to learn more about security concerns such as identity theft and travel warnings. This program also offers an incentive system, where each facility may make proposals to the corporate security group in order to make their facility more secure. If a proposal is accepted, then the corporate group will help fund it. As an example, one site

developed a streaming video Protection of Proprietary Information (POPI) program that was funded partly by the corporate security group. Their Senior Director of Security feels that this program has helped to spark individual involvement in reaching security objectives.

5.3 Value System

Many organizations provide their employees with an explicitly stated value system in the form of a mission statement, motto, core values, or business conduct guidelines. These items offer a clear and concise manifestation of the company's values that may be used to provide motivation or help in the decision making process. Another less obvious measure of a company's value system, is the overall corporate culture and how that is perceived by employees. While many of the companies we spoke to could readily identify the former, referring us to their company website or referring to a reminder card located within arm's reach, most interviewees struggled to articulate the latter.

When asked about their corporate culture, in fact, most interviewees reached immediately for a document stating their company's stated value system, or described their culture as being aligned with a specific function, such as speed or flexibility. When pushed further to discuss their perception of the corporate culture, the answers were slow to come and varied widely in thought and clarity. It is important to note that one person's perception of corporate culture says little about that culture, but it may be helpful to identify general awareness in this area.

Company C's Assistant VP for Customer Service quoted a defined set of five core values that is well articulated and communicated throughout the company, emphasizing items such as customer service, focus on people, and safety. Company C also has a strong sense of family that stems from the history of the railroad industry, where often great grandfathers, grandfathers, mothers, sisters, and cousins all work for the railroad. This instills a sense of pride that the interviewee feels sets Company C apart from other industries. When asked about his company's culture, the Senior Director of Security at Company L referenced their company's mantra, core values, and mission statement. These three messages combined focus on such items as helping others, innovation, respect, quality, being a responsible citizen, and being the consumer's first choice.

Company B provides their employees with a security mission statement, which is a subset of their overall mission statement. As a company, they view themselves as extremely customer focused and supply chain focused. This is a result of the fact that they touch freight at many instances along the supply chain (i.e. origin, destination, transport), and sometimes even take custody of the freight from the manufacturer to the retail store. Security ties into this process since they have moved to servicing many aspects of their customers supply chains out of their customers' desires to use fewer providers, in large part for security reasons.

Company M's Senior VP aligns their perceived corporate culture with speed and flexibility, two goals that reflect directly on their supply chain security practices. Security ties to this through the potential for delays from increased border inspections. As a result, he states that C-TPAT became a company priority "the minute it was viewed as an impediment to speed," and if it hadn't intersected with flexibility and speed, "nobody would have cared."

According to Company I's Security Manager, their corporate culture focuses on the customer and the community. They enforce these values through communications, action, and training. As a demonstration of this commitment, Company I has an entire organization dedicated to helping their employees help their customers with unanticipated or complex problems. Security ties into this customer-focused value system through helping to ensure on-time delivery of their products and overall customer satisfaction.

Company J has experienced a return to their basic beliefs, which include performing every task in a superior manner, customer first, respect for the individual, and doing the right thing. They feel that these beliefs align well with the security organization. Company J's Director of Security indicates, "if there's the potential that a country or individuals in a country could be harmed, then we step up and do the right thing and take that responsibility." He feels that sets Company I apart from other companies who feel that if security doesn't affect them, they should not care about it.

Company T has a strong culture of "safeness," which encompasses aspect of safety and security. This concept differs from safety in that "safety is cleaning up spillage in the store so someone does not fall over. Safeness is the well being of our guests when they come in the store." This concept translates from the store to the workplace, in the form of wider aisles and bright parking lot lighting, to tracking of executives traveling around the world. The concept of safeness is so engrained in the company, that they even have a safeness manager.

Company O is an Asian company with a strong focus on protecting the environment. Their Security Group has capitalized on this by including security in their corporate environmental structure and reporting process. According to their Security Officer, this has been a "sneaky, or effective way, to weave within that culture some awareness of security." Another aspect of Company O's culture is that they are very methodical, leaving no stone unturned when approaching a new issue. As a result, the company sometimes takes longer than their competitors to address an issue. Their Security Officer states that "[Company O] will be the best; they just won't be the best first."

6 Basic Underlying Assumptions

Schein (1992) defines basic underlying assumptions as "unconscious, taken-for granted beliefs, perceptions, thoughts, and feelings that are the ultimate source of values and action." He further states that "culture as a set of basic assumptions defines for us what to pay attention to, what things mean, how to reach emotionally to what is going on, and what actions to take in various kinds of situations." Throughout the research process, three basic underlying assumptions emerged that appear to support creation of a supply chain security culture.

- Basic Assumption #1: That supply chain security affects employees' safety
    - Employees believe that security affects their safety and would understand the connection in the following example: if a shipment of product coming from a manufacturer abroad is not adequately monitored during loading, a biological agent could be introduced to the shipment. In this case of terrorism, employees receiving the product at the U.S. distribution center might be harmed when opening the shipment.

- Basic Assumption #2: That supply chain security affects employees' livelihood
    - Employees believe that security affects their livelihood, and would understand the connection, in the above example: if the biological agent in the shipment did in fact harm employees or customers, this incident would negatively affect the company's reputation, and most likely reduce market share. Employees might therefore lose their jobs as a result of this incident that could have been prevented with proper supply chain security.

- Basic Assumption #3: That security is the "right thing to do"
    - Employees feel that security is the right thing to do, as demonstrated in the above example: when personnel at the manufacturing facility decide whether to ignore the security guidelines for loading procedures in order to save time and increase productivity, or follow them to ensure proper security. In this case, employees are faced with more than one "right thing to do," increase productivity and ensure security. This dilemma is further discussed in section 6.3.

6.1 Security Affects Employees' Safety

The success of a company's security program rests on the actions of its employees. The research suggests that if employees feel that security affects their personal safety, for example that not following security guidelines will result in personal harm, they will make decisions in accordance with the company's security objectives. This basic underlying assumption is often facilitated by a strong existing safety culture.

Company D, for example, focuses on providing a work environment where employees feel secure. According to their Investigations Manager, "if you provide employees with a safe and secure working environment, you eliminate a whole host of issues." As an example of this, when the company was considering instituting a mandatory drug-testing program, their security manager used the existing General Safety Committee to discuss the issue with employees. This openness helped the employees understand that the company was implementing this program in order to create a safe and secure workplace, and they unanimously approved the program.

At Company E, personnel safety is viewed as the number one priority, as evidenced by safety videos required for all visitors, and safety briefings that begin every meeting, even those occurring in an office setting. According to their Security Administrator, "it's been drummed into the people at [Company E] that [security is] protection of our employees...we look at the people as our biggest assets. So it's not only facilities, but protection of our people too." As a result of this focus on safety, employees feel comfortable requesting, and praising, increased security, for example in instances when the Department of Homeland Security (DHS) raises their Homeland Security Advisory System threat level (see Appendix A for a brief description of this program).

Company T's Assets Protection Group's responsibilities include "safeness, theft, and fraud." The concept of safeness falls between security and safety, and is described as "safety is cleaning up spillage in the store so that someone does not fall over, safeness is the well being of our guests when they come into the store." The concept of safeness applies equally to employees and customers. Company T has an executive manager whose job is safeness, and that manager projects the concept to their workforce through introductory security training for new employees, and ongoing training on subjects such as workplace violence.

6.2 Security Affects Employees' Livelihood

The research also suggests that instilling the basic underlying assumption that security impacts employees' livelihood will motivate employees to embrace security principles. As described in the example above, a tarnished reputation may affect the company's market share and therefore employee compensation. In addition to this risk, poor security might result in an incident so severe that a company goes out of business. Throughout this research, three different approaches to motivate employees in this way were observed: focusing on protecting the company's overall bottom line, focusing on protecting the customer, and focusing on protecting the product.

Company K focuses on security's impacts to the company's bottom line. According to their Director of Security, "where security might appear to contradict or conflict with what an individual wants, we always have to provide the rationale behind it. But at the end of the day, they employee knows we need to protect the intellectual property, our assets, and contribute to the bottom line, so long as you're seen contributing to that, they are supportive."

One of Company S's corporate goals is to protect their assets, so they use whatever strategy works to protect cargo theft from terrorism. In order to do this, the Director of Supply Chain security has developed strategies for his group and its employees to have a better understanding of the risks that their products are exposed to, and what it means to the company when they lose product. For example, they communicate to employees an estimated indirect cost of five to seven times the cost of a direct loss to the bottom line of the company.

Company A conducts security audits of each of their stores, observing items such as check levels, cash levels, and shrink rates. They then expose all of their managers to the results of these audits. This exposure forces the employees to understand that the financial impact of poor security on the store. Employees then make the connection to their compensation, because they know that merit increases and bonuses are directly tied into the results of security audits.

Company J uses security's competitive advantage to convey its importance to their personnel. According to their Director of Security, "we try to convey to our employee population that it's a key to our competitiveness...that we have threats from terrorist situations that might target multinational corporations like [Company J], and we try to convey that it's in the individual's and corporation's best interest to do things in this area."

Some companies focus on protecting the customer as the motivating factor for their personnel. One common example of this is the prevalent adoption of C-TPAT, even in companies that do not have a strong need for security. Although C-TPAT is voluntary[1], companies have adopted the program because they know that if they do not, they believe that their business may be impacted by increased delays and the inability to get product to their customers on time. If they cannot get the products to their customers in a timely fashion, it may affect their market share. Company G, for example, views themselves as a low-risk importer with high volumes of low-value product that don't justify extensive security investments. They realize, however, that if they do not comply with C-TPAT, they will no longer be considered a low-risk importer and will be subject to additional inspections, eventually affecting availability of product to their customer and their position in the market.

At Company I, their Security Manager states "our focus really is the customer and the community, trying to be a good corporate citizen and the number one supplier to the customer base. I think where security ties into that is through customer satisfaction model, making sure the customer is receiving the product that they want on time." Company U also views their company as customer service driven. They continually measure customer service levels and customer satisfaction in order to remain conscious of their customers and the market in general. This focus clearly communicates to employees that customer service has an impact on the company's overall performance.

Some companies focus on protecting their product, because they recognize that poor quality products could affect not only their brand, but in some cases, the health of their customers. Companies in the food and pharmaceutical industries, for example, view security as key to not only their competitiveness, but also to their long term viability. A public health tragedy resulting from poor quality might mean dire consequences for the company, a very direct threat that is visible to employees. According to Company Q's Director of Security, "the number one issue that sets apart from other industries is public health. If somebody counterfeits a pair of jeans, or a computer device, or a CD, nobody is going to fall ill. If you do that to something you put in your body to alleviate an ailment, and you suffer an adverse effect or worse, that kind of issue rocks this industry." Company A's VP for Asset Protection echoes this sentiment. He states "our philosophy is if there is an issue going on with food

[1] C-TPAT has been a voluntary program since its implementation in November 2001. As of March 2005, U.S. Customs and Border Patrol has issued new C-TPAT guidelines which are still voluntary, but more stringent. See

safety, we will always err on the side of safety versus cost to pull the merchandise. Our Chairman, if he even thought we were thinking of costs, I'd be fired. He has told me that."

6.3 Security is "The Right Thing to Do"

During this study, interviewees were asked to describe their corporate culture and how it relates to the company's security objectives. Many interviewees had a difficult time communicating the tenets of their corporate culture, but approximately half of them indicated that one aspect of their culture is "doing the right thing." When asked to clarify, interviewees offered many descriptions of what this means, from providing a safe workplace, to being a good corporate citizen, to supporting philanthropic efforts in their local community. The basic underlying assumption that security is the right thing to do implies that when employees are faced with a difficult decision involving security and they want to do the right thing, they will choose the course of action resulting in the most secure supply chain.

Company F, for example, recently released a Code of Conduct as a result of a high-profile prosecution of one of their employees involved in financial impropriety. This Code of Conduct addresses items such as financial propriety, the way to treat people, relationships with third parties, and commitment to diversity, and it has been pushed down to very low levels by the CEO. As a result, Company F has been more focused on compliance issues such as the Sarbanes-Oxley Act of 2002 (see Appendix A for a brief description of this Act), insider trading, prevention of sexual harassment, and "doing the right thing." According to their VP for Corporate Security, "doing the right thing is ingrained here, top to bottom, and I like to think most people live it."

Company G also views one part of their culture as doing the right thing, but they relate this to philanthropic efforts. When asked to define doing the right thing, their Director of Corporate Security replied, "I don't mean do the right thing because you're worried about the Securities and Exchange Commission (SEC) or an audit after say Enron. When I say do the right thing, I mean the company gives away millions of dollar a year for local charities and charities around the world." Although a public company, they were until very recently managed by a family who instilled the importance of taking care of their employees and their community. The company provides excellent benefits, including offering eight paid hours a

---

Section 9.1 for further discussion on the evolution of C-TPAT.

month to its employees participating in community service. According to Company D's Investigations Manager, doing the right thing is "a combination of doing what's required by law/regulations, what produces a good/safe/secure work environment, what provides adequate return for investors, and what provides an environment where you want to attract and retain qualified employees."

Doing the right thing obviously encompasses a broad variety of actions, and often more than one. In this case, the company must provide their employees with ways to identify what constitutes doing the right thing, and tools to set priorities and make decisions according to the company's objectives. For example, if a company's primary goal is to offer their products at the least cost possible, while also maintaining strong supply chain security that requires added cost, this conflict will challenge employees when performing their duties. Regardless of where it falls in the hierarchy of good deeds, accomplishing the company's security objectives should fundamentally be considered doing the right thing.

7 Supply Chain Security Culture Key Success Factors

Chapter Six identifies three basic underlying assumptions that the research suggests support adoption of a supply chain security culture. First, that security affects employees' safety. Second, that security affects employees' livelihoods, and finally, that security is the right thing to do. Observations from this study suggest several key success factors that, when implemented, should help employees of all levels form these basic underlying assumptions.

This chapter outlines these key success factors that were derived from the artifacts and espoused values outlined in Chapters Four and Five. These key success factors were selected based on three primary criteria; first, practices that appeared frequently across multiple companies; second, practices that demonstrated the most direct action-result relationship; and third, practices that appeared unique, interesting, and progressive when compared to other observations in the study. Table 7-1 provides a summary of these key success factors.

Table 7-1 Key Success Factors for Creating a Supply Chain Security Culture

Area	Key Success Factors
Supply Chain Security Program	• Decentralized - Senior business manager at each location responsible for security - Corporate security staff as "consultant" - Safety or quality programs used as model where appropriate - Part- or full- time security personnel utilized. If using third party retain management within company • Shift to corporate reporting relationship where security will have the most leverage • Integrate C-TPAT guidelines into program
Supply Chain Security Program Implementation	• Make business case for security - Identify relationship between security and business objectives - Undertake security-specific risk assessment in security program - Measure potential or historical losses - Quantify direct and indirect costs of not complying with security - Identify and value collateral benefits - Utilize Six Sigma (if used in other areas of the company) • Collaborate on three levels - Internal collaboration at the executive level - External collaboration with industry - External collaboration with government • Integrate at executive and local level with BCP program - Develop joint objectives and exercises • Seek support from senior leadership across all business functions
Personal and Professional Performance	• Conduct background screening according to security objectives - personality traits for general employee, specific experience for security-specific personnel • Seek specific work experience (i.e. law enforcement, international) • Educate employees on supply chain and security objectives - Capitalize on existing safety or quality culture as relates to security • Educate suppliers on security objectives • Communicate security objectives to organization on a regular basis • Include security in espoused values (motto, core values, code of conduct, etc) • Include security metrics in individual performance objectives • Create incentives to meet security objectives • Conduct audits to ensure adherence to security program - Build upon safety, finance or quality audits when possible - Share results, and impact, with employees

7.1 Supply Chain Security Program

The research suggests that a decentralized security program that encompasses supply chain security concerns is a key success factor. This program utilizes a corporate staff charged with creating policies and procedures and disseminating them to the global organization, and is led by an executive ideally no more than two steps removed from the Chief Executive Officer (CEO), typically a Vice President or Director. This corporate staff might also include regional or country security mangers where appropriate. The senior business manager at each facility is charged with responsibility for security, and has access to the corporate security staff as consultants to provide assistance on local issues when necessary. The senior business manager at each facility may be assisted by either part- or full-time local, security-specific personnel, depending on each facility's size and vulnerability. If local security responsibilities are outsourced, the company maintains close oversight. When creating a new security program, or reorganizing an existing program, companies may find it helpful to capitalize upon existing safety or quality programs that share these decentralized characteristics.

Another key success factor involves placement in the corporate structure. Observations from this study indicate that security program reporting relationship is not standard across companies or industries (Section 5.2.1), but that companies aim to place security in the corporate department that will give it the most leverage within the organization. For example, the Operations department might be the most effective placement for an operations-driven company, the Finance department might the best fit for an analytically focused company, and the Compliance department might be the best fit for a company with a strong environmental, health, and safety focus.

Another key success factor is participation in the Customs Trade Partnership Against Terrorism (C-TPAT). Every company we interviewed, except one, has integrated C-TPAT guidelines into its core. Although C-TPAT has been criticized in many ways since its inception for its long application approval delays, vague standards (Gooley, 2002), and voluntary nature (Keane, 2004), the program appears to be effective in many ways. In particular, C-TPAT forces companies to document security procedures already in place, provides guidance to create or improve existing security procedures, provides a mechanism to

require security terms in supplier contracts, and results in increased awareness of supply chain security through all levels of the organization.

7.2 Supply Chain Security Program Implementation

This study revealed many key success factors that security programs, as described in Section 7.1, may implement to increase overall supply chain security and resilience. These key success factors cover a wide variety of activities, and may be implemented at different levels of the security program structure.

Financial analysis of security measures appears to be very effective in garnering support for security throughout the organization. Many security programs conduct financial analysis to make the business case for security and align security objectives with overall business objectives. This analysis is especially challenging, however, due to the difficulty of measuring the value of preventing security breaches. This effort requires working within your organization and with industry partners to identify common methods to quantify return on investment (ROI) for security expenditures. Some common methods observed in this study include conducting risk assessment within the security program, instead of relying on centralized risk management groups, and quantifying historical losses, potential losses, and the cost of delays before and after mitigation efforts. Financial analysis should attempt to measure direct costs, such as actual losses due to a security incident, as well as indirect losses, such as loss of customers due to persistent delivery delays. Holley (2005) defines these indirect costs, which he calls "no-see-ums," as losses that cannot be paid by typical cargo insurance policies.

Another way to make the business case for security is to identify and value collateral benefits that have arisen from improved security. Rice and Spayd (2005) categorizes these collateral benefits as resulting from security in a variety of areas including asset visibility and tracking, personnel management, physical security, and development of standards. Finally, some companies have utilized Six Sigma™ methods, which are used widely in organizations with strong quality cultures, to conduct root cause analysis of security incidents. This type of analysis may help to quantify potential or actual losses. Regardless of the methods used, making the business case for security appears to be vitally important in creating a supply

chain security culture, but extremely difficult to do. Section 9.1 addresses the need for further research in this area.

In addition to financial analysis, the research suggests that collaboration plays an important role in creating a supply chain security culture. This collaboration occurs at three levels: internal collaboration with other executive leadership, external collaboration with industry partners, and external collaboration with the government. Internal collaboration, often in the form of cross-functional committees, helps increase security awareness throughout all areas of the company. This appears to be particularly effective when security becomes involved in sourcing decisions and business continuity planning efforts, as discussed further below.

Formal collaboration with industry partners allows for sharing of threat information and best practices for response and mitigation. These forums also provide an opportunity for standardization of technical definitions that may help companies define the business case for security, as described above. In areas where these collaborative efforts appear to be most fruitful, companies do not view the fundamentals of their security programs as a competitive advantage. Companies must balance benefits to the industry as a whole with the individual benefits of keeping security best practices confidential. Finally, collaboration with government facilitates information sharing, and creates relationships that may be helpful in the event of a crisis. This collaboration is also particularly effective when companies engage in public-private partnerships such as C-TPAT or are bound by regulations, such as the Maritime Transportation Security Act of 2001 (MTSA).

One important area of internal collaboration is with the companies' security and business continuity planning (BCP) programs. This collaboration helps to facilitate creation of secure and resilient supply chains because security and BCP programs utilize each others' expertise and perspective to truly understand the threats facing the company, and the best strategies to mitigate these threats. Integration between these two programs should take place at both the corporate level, where policies and planning take place, and the local level, where these policies and plans are exercised. Many interviewees indicated that their comprehensive BCP planning efforts were relatively new, and in need of improvement. This presents the perfect opportunity for security programs to become more involved in BCP at both the corporate and local level.

Finally, this research suggests that the support of executive leadership across all departments of the company and, if possible, the CEO, is a key success factor. This support helps demonstrate to employees the company's clear commitment to supply chain security, and may assist security leadership to make difficult decisions based on security, such as discontinuing service with an incompliant external partner or avoiding operations in a specific geographic area.

7.3 Personal and Professional Performance

Chapter Six suggests three basic underlying assumptions that support creation of a supply chain security culture: that security affects employees' safety and livelihoods, and that security is the "right thing to do." This process of inculcating supply chain security cultural values often begins before an employee is even hired. One key success factor is working with a company's Human Resources (HR) Department to screen potential employees for experience and personality traits that align with the company's security objectives. Some companies also extend this background screening effort to their suppliers' employees. C-TPAT guidelines on background screening provide a helpful tool to help to communicate security screening objectives to the HR department, and the HR department of suppliers. These desired experience and personality traits may differ for the general employee and security-specific personnel. The research suggests that some general employee traits that might contribute to supply chain security objectives include loyalty, ability to see the big picture, effective communicator, self-awareness, and the ability to work in teams. When looking to hire security-specific personnel, it may be helpful to draw from law enforcement communities of countries in which a company operates, or seek out personnel who understand the international nature of security.

Security education appears to be another key success factor. Some methods of education include training new and existing personnel on the company's security objectives and inculcating these values through socialization. This education should begin upon orientation to the company, and continue on a regular basis through workshops or other training seminars. The Internet appears to be an effective tool to provide continuously updated training to employees that can be conducted at their convenience. In the absence of, and in addition to available resources, socialization techniques such as informal security briefings or

word of mouth communication may also help to convey the importance of security to your employees. When applicable, companies may capitalize on existing safety or quality cultures to emphasize the need for security. In the case of safety, an effective bridge between the two programs might be the focus on creating a safe workplace. In companies with a strong quality culture, an effective bridge might be a focus on protecting product quality.

An extension of this key success factor is security education of suppliers' employees regarding security objectives, regardless of whether these objectives are included in supplier contracts. When training foreign suppliers, companies should avoid referring to C-TPAT, but instead focus on the guidelines as being company-specific. This helps to remove any feelings of intimidation or confusion surrounding U.S. regulations. In addition, inviting local influential figures to attend security-focused training sessions may help improve supplier buy-in.

Regular communication of security objectives to employees and suppliers is another key success factor. Effective communication demonstrates to employees that security is a high priority of the company, and removes opportunities for them to claim that they were not aware of their security responsibilities. Some common communication tools include posters, hotlines, intelligence bulletins, and the Internet. A company's home page provides an easily accessible forum to post security information of immediate concern to a global audience.

Another way to demonstrate commitment to security objectives is to include security in the company's mission statement, motto, business conduct guidelines, or core values. Although these items are the company's stated, or espoused, values, and not necessarily the values that employees actually act on, interviewees in this study referred to them often. This demonstrates that employees are aware of these espoused values, and most likely use them during the decision making process.

Once employees are trained and constantly reminded of security objectives, including security metrics in individual employee performance evaluations provides additional incentive for employees to adhere to the security program. Employees generally prioritize their performance of duties as they align with performance objectives, so this is an area that could be used to improve employees' understanding and willingness to embrace security principles. This not only holds employees responsible for meeting security objectives, but also increases

the company's "eyes and ears" to detect security incidents. In addition, monetary or merit-based incentives may help spark individual involvement in the company security program.

Finally, implementing an audit program to ensure that security objectives are being met at company facilities and suppliers' facilities helps to reinforce the importance of security objectives. Companies may take advantage of existing safety, quality, or administrative auditing teams when possible, by training them in basic security principles and adding security items to their responsibilities. Many interviewees indicated that this assisted them to meet security objectives at a low cost. These audits should, however, be supplemented with security-specific audits on a less frequent basis, or as issues arise, to ensure that subtle security issues are detected. Keeping employees apprised of audit procedures and results also reinforces the impact of security on their well-being and that of the company.

8 Supply Chain Security Context

Implementation of the key success factors outlined in Chapter Seven should assist companies in creating a supply chain security culture. Before embarking on this process, however, companies should understand the context within which they operate. This context is especially useful when addressing differences across a company's operating or service areas, and how to apply the key success factors in an appropriate fashion. For example security concerns at a U.S. facility that does not handle imports or exports may be very different than at a South American facility that routinely ships and receives foreign materials. The research suggests three considerations that, when fully evaluated and accounted for, should help in the adoption of a supply chain security culture.

First, companies should assess whether their business model necessitates a supply chain security culture. A pharmaceutical company, for example, may perceive a strong need for security to protect public health, while an apparel company may view security concerns as secondary to lowering costs. Second, companies should understand the primary drivers behind their supply chain security effort, as these will ultimately shape their security objectives. For example, the pharmaceutical company referenced above may be primarily focused on protecting products from tampering, while the apparel company may be solely focused on theft prevention.

Finally, a company should understand their overall corporate culture in order to champion effective change within the organization. A company with a tradition-focused culture such as a railroad may treat security objectives very differently than a company with an innovation-focused culture, such as a technology firm. A comprehensive understanding of these three contextual factors should help companies adopt and apply the key success factors outlined in Chapter Seven, with the goal of creating a supply chain security culture in alignment with their security objectives.

8.1 Need for Supply Chain Security

The observations in this study suggest that companies view security objectives differently, depending on their need for supply chain security. This need may vary across product lines, service lines, or operating areas. For example, an aircraft engine manufacturer may have a higher need for security than a consumer goods retailer, since the consequences of potential security breaches will vary in severity. A technology company handling high value products might also have a very different risk profile than a toy company handling lower value product.

Only one company included in this survey took action to explicitly measure their need for security. This company hired a consultant to conduct benchmarking on security costs and service, in order to clarify what level of security their company required. A number of companies were evaluated using a matrix that included company characteristics such as size, number of employees, number of government contracts, and corporate culture. This matrix then gave each company a demand index which helped them understand what the company needed from them as a security provider. Expectations of the companies in the study varied, from those that value security very highly to those that do not value it much at all. The differences in these values were often based on the opinion of upper management in a company, or its corporate culture. This benchmarking process allowed the company to understand their particular perspective on security, why there were cost differentials between them and other companies, and what their company's expectations were for the security program.

Another important distinction is the need for security in different areas of a company's global operations, as security concerns vary depending on the local operating environment. Companies that operate in a high risk country with a history of terrorism, such as Indonesia, might place more emphasis on security in that country than in their U.S. based operations. The need for security is also viewed differently in many countries from a cultural perspective. For example, several companies we spoke to indicated that Chinese suppliers view security as something they have to do because their U.S. customers have asked for it, as opposed to something that do because they feel it is important. One non-U.S.-based company we spoke to indicated that in their view, security is an "American problem." As a result, they located their

security headquarters in the U.S. instead of co-locating with their headquarters abroad. Another company implemented their supply chain security program in North America two years before extending the program to other operating areas. Companies should attempt to fully understand the need for security across all geographic and operating areas, and customize implementation of supply chain security culture key success factors to meet those needs.

8.2 Primary Drivers of Supply Chain Security

Another contextual area of interest is understanding the company's primary driver for creating a supply chain security culture. Although many companies have improved their security and business continuity programs since the terrorist attacks of September 11, 2001 and the advent of C-TPAT, terrorism does not appear to be the primary driver behind many security programs. In fact, only nine of the twenty-one companies included in this survey explicitly mentioned terrorism as a security concern. Some other common drivers include theft, counterfeit, tampering, gray market diversion, and protection from trade delays caused by increased security inspections at border crossings.

Theft, for example, is a concern that has historically plagued the low-margin apparel industry, and it seemed to be the main focus of one apparel company despite their participation in C-TPAT. Ensuring smooth trade flow also appeared to be a motivating factor for many companies, for example those in the toy and electronics industries who have joined C-TPAT not because they view their cargo at high risk, but in order to reduce border crossing delays. The two food industry interviewees indicated that they have joined C-TPAT in order to help protect their products from tampering of any kind that may result in a public health crisis. While the key success factors outlined in Chapter Seven apply to any company, regardless of their primary security drivers, the awareness of what these are will assist the company in tailoring the program appropriately.

8.3 Corporate Culture

As discussed in the literature, and evidenced throughout this study, corporate culture is a difficult thing to describe, and cannot be fully understood by an outsider through interaction with one person at a company. When interviewees were asked about their corporate culture, however, people's perception of what values were important to their company and how they related to security were revealing. In general, interviewees cited their company's espoused values (business conduct guidelines, core values, mission statement, etc.), and then added one or two less tangible items that they felt were important.

Some examples of these additional responses include "doing the right thing," "nothing is ever good enough," a drive to be the fastest company in the industry, or a tendency to be very analytically oriented. These items might relate to security objectives in the following ways. Doing the right thing for a transportation provider might mean protecting customers' cargo at all costs. Doing the right thing for a pharmaceutical company might mean protecting your products in order to preserve public health. Nothing is ever good enough might indicate a company's push to always be proactive in the security arena, regardless of past successes. This might also indicate a company's desire to benchmark constantly with competitors to ensure that their supply chain security practices are considered the best in the industry. The drive to be the fastest company in the industry might indicate a propensity for participating in public-private partnerships like C-TPAT in order to reduce border crossing delays. An analytically driven company might rely on in-depth analysis to make the case for security, using such methods as security-specific risk assessment and Six Sigma™ root cause analysis.

Gathering a full understanding of a corporate culture is a complex task, and one that is not easily done by someone assimilated into that culture, for example an employee of the corporation. It is useful, however, for companies to study their organization's culture and how it is perceived by employees. Schein's framework used throughout this study, as well as references provided in Chapters Two and Three, may prove useful for companies wishing to further understand their corporate culture. This understanding may help security leadership align the company's overall corporate culture with the company's security objectives, and communicate these objectives in a common language throughout the company. Supply chain

security initiatives based on this understanding will be more effective in motivating employees to embrace security principles and advance the company toward creating a supply chain security culture.

9 Conclusion

The thesis was motivated by the increased focus on supply chain security and resilience in the four years since the terrorist attacks of September 11, 2001. These attacks alerted private industry and governments to the potential for disruptions from high impact/low probability events such as terrorism and, in the United States, resulted in the advent of public-private partnerships such as the Customs Trade Partnership Against Terrorism (C-TPAT). These public-private partnerships have encouraged industry to address supply chain security both internally and externally, and to broaden the historically narrow scope of supply chain security, focused on theft, to include disruptions such as natural disasters, sabotage, and terrorism. The companies selected for this research have demonstrated high levels of performance in creating secure and resilient supply chains. This thesis aims to study how these companies manage their security and business continuity programs, and specifically the role that organizational culture plays in creating secure and resilient supply chains.

Schein's organizational culture framework (Figure 2-1) was used to analyze interviews with senior security executives from twenty-one companies across a wide variety of industries. Schein's framework defines culture as having three levels: *artifacts*, which are visible organizational structures and processes; *espoused values* which include strategies, goals, and philosophies; and *basic underlying assumptions*, which include unconscious, taken for granted beliefs, perceptions, thoughts and feelings. Observations from these interviews, which focused on supply chain security programs, business continuity programs, and corporate culture, were categorized according to an expanded version of Schein's framework provided in Figure 3-1. This expanded framework identifies artifacts, espoused values, and basic underlying assumptions that are specific to supply chain security.

Key success factors for creating a supply chain security culture were then drawn from these artifacts, espoused values, and basic underlying assumptions (Table 7-1). These key success factors were selected based on commonality across multiple companies, or on their progressive nature when compared with other companies in the survey. These key success factors address three areas: supply chain security programs, supply chain security program

implementation, and personal and professional performance. In summary, these key success factors include implementing a decentralized security program, integrating C-TPAT guidelines into this security program, making the business case for security, collaborating internally with other business units and externally with industry and government, integrating supply chain security and business continuity planning, educating and measuring internal employees and suppliers' employees on supply chain security objectives, and including security as an official espoused value of the company.

Before implementing these key success factors, it is recommended that companies understand the supply chain security context. The research suggests that three areas should be assessed: the company's need for supply chain security, the company's primary drivers behind supply chain security, and the company's overall corporate culture. An understanding of this context will assist the company in tailoring the key success factors to their needs. The high performance of the companies included in this study suggest that implementation of the proposed key success factors, in alignment with a company's supply chain security objectives and corporate culture, should increase supply chain security and resilience performance throughout the company.

9.1 Recommended Areas for Further Study

This research exposed many areas ripe for further study. The most intriguing and elusive of these is how to measure the financial effects of supply chain security. Interviewees provided anecdotal descriptions of what measures they were taking to conduct financial analyses to justify supply chain security measures, but analytical methods varied widely company to company. This task is challenging on many levels. Most importantly, it is extremely difficult to measure incidents that have not yet occurred and may or may not have a known probability. In addition, external analysis of these financial methods is hampered by companies' disinclination to share loss information. Further research in this area would be useful in assisting companies in making the business case for security.

Another area of interest is the overlap between safety and security programs and cultures. This research indicates that many companies have benefited from building on

existing safety programs to both administer security programs and motivate employees to embrace security objectives. Some interviewees did indicate, however, that they feel security is most effective when treated as an entirely separate discipline. The positive and negative repercussions of integrating these two disciplines will certainly be of interest as attention to supply chain security increases in the future.

This research focused on interviewing senior security executives about their company's security programs and their interaction with business continuity planning (BCP) programs. In many cases, security and BCP programs do interact in the form of joint oversight committees, planning, and exercises. Many interviewees indicated, however, that the move toward comprehensive BCP is relatively new and that their programs are in need of improvement. This presents a unique opportunity for increased integration between security and BCP. A similar study focused on BCP executives, in order to assess their perception of integrating with security, would no doubt prove useful in furthering this objective.

The recent announcement of new C-TPAT guidelines by U.S. Customs and Border Patrol in March 2005 indicates that this program is ever-evolving. Further study of C-TPAT and its impact on supply chain security, especially in the area of supplier interaction and enforcement, would prove useful. This research indicates that C-TPAT has provided a vehicle for companies to include security guidelines in contracts with suppliers, but few have gone beyond these contractual obligations to ensure that their security objectives are being met through education and auditing. Supply chain security's value is directly related to its application across all links of the supply chain, therefore additional research focused on integration between companies and their suppliers would be useful.

Bibliography

Bierly, P. (1995). Culture and high reliability organizations: The Case of the nuclear submarine. Journal of Management, Vol 21, No. 4, 639-656.

Coutu, D.L. (2002). How resilience works. Harvard Business Review, May, 46-55.

Deal, T & Kennedy, A. (1982). Corporate cultures: The rites and rituals of corporate life. Addison-Wesley Publishing Company: Reading, MA.

Denison, D. (1990). Corporate culture and organizational effectiveness. John Wiley & Sons: New York.

Department of Homeland Security Advisory System (HSAS) URL: http://www.dhs.gov/dhspublic/display?theme=29 (visited 2005, May 3).

Find Law.Com URL: http://news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf (visited 2005, May 3).

Gooley, Toby (2004). C-TPAT: Separating hype from reality. Logistics Management. August;43,8, 77-81.

Grunwald, M.(2001, October 28). A Tower of courage; On September 11, Rick **Rescorla** died as he lived: Like a hero. Washington Post, F01.

Hampden-Turner, C. (1992). Creating corporate culture: From discord to harmony. Addison-Wesley Publishing Company: Reading, MA.

Hofstede, G. (1986). Editorial: The usefulness of the organizational culture concept. Journal of Management Studies. 23:3, May, 253-257.

Hofstede, G., Neujin, B., Ohayv, D., & Sanders, G (1990). Measuring organizational cultures: A qualitative and quantitative study across twenty cases. Administrative Science Quarterly, 35, 286-316.

Holley, R. (2004). The No-See-Um's: The financial impact of cargo losses on the bottom line. Presentation for the 2004 Council on Logistics Management Annual Conference, October 6.

International Maritime Organization URL: http://www.imo.org/home.asp (visited 2005, May 3).

Katzenbach, J. (1999). Firing up the front line. Harvard Business Review. May-June, 107-117.

Keane, A(2004, April 4). Insecurity over ports. Traffic World. Commonwealth Business Media, Washington D.C.

K. L. Strategic Change Consulting URL: http://www.klscc.com/. (visited 2005, May 3).

Kotter, J. & Heskett, J (1992). Corporate culture and performance. The Free Press: New York.

Krafcik, J. (1998). Triumph of the lean system. Sloan Management Review. Fall, 41-52.

Latour, A. (2001, Jan. 29). Ericsson of Sweden gets burned. *Wall Street Journal*, A1.

Lee, H.L., Wolfe, M. (2003). Supply chain security without tears. Supply Chain Management Review, January-February, 12-20.

Lee, H.L, Whang, S. (2003). Higher supply chain security with lower cost: Lessons from total quality management. *Stanford Graduate School of Business Research Paper Series*, No. 1824, October.

Lorsch, J. (1991). Organization design. In J. Gabarro (Eds.), Managing People and Organizations (pp. 313-331). Harvard Business School Publications, Boston, MA.

Martha, J. Subbakrishna, S. (2002). Targeting a just-in-case supply chain for the inevitable next disaster. Supply Chain Management Review, September/October, 18-23.

O'Reilly, C. (1989). Corporations, culture and commitment: Motivations and social control in organizations. California Management Review. 31,4, 9-25.

Pascale, R (1985). The paradox of corporate culture: Reconciling ourselves to socialization. California Management Review, Winter, 26-41.

Pascale, R. (1997). Changing the way we change. Harvard Business Review. November-December, 126-139.

Retail Industry Leader's Association (RILA) URL: http://www.retail-leaders.org/new/index.aspx. (visited 2005, May 3).

Rice, J. and Caniato, F. (2003). Building a secure and resilient supply network. Supply Chain Management Review, September/October, 22-30.

Rice, J. and Spayd, P. (2005). Collateral benefits of security. Special Report Series, IBM Center for The Business of Government. May.

Roberts, K. (1990). Managing high reliability organizations. California Management Review. Summer.101-113.

Schein, E. (1992). Organizational Culture and Leadership. Josey-Bass Publishers. San Francisco.

Schein, E. (1992a). What is culture?. In Frost, P., Moore, L., Lous, M., Lundberg, C. & Martin, J. Eds. (1991). Reframing organizational culture (pp. 243-253). Sage Publications: Newbury Park.

Scholtz, Duncan (2004). Lucent SCN: Leveraging the fully integrated supply chain. Massachusetts Institute of Technology Engineering Systems Division Thesis.

Schwarz, H. Davis, S. (1981). Matching corporate culture and business strategy. Organizational Dynamics, Summer, 30-48.

Sheffi, Y (2001). Supply chain management under the threat of international terrorism. The International Journal of Logistics Management, Vol. 12, No. 2,1-11.

Simon, S. (1999). Breaking the safety barrier: implementing culture change. Professional Safety,Vol. 44, Issue 3, 20-26.

Smith, D. (2003). Sustainability and corporate evolution: Integrating vision and tools at Norm Thompson Outfitters. Journal of Organizational Excellence. Autumn, 3-14.

The Strategic Council on Security Technology URL: http://www.scst.info/joinsst.html (visited 2005, May 3).

Studt, T. (2003). 3M-Where innovation rules. R&D Magazine. April, 20-24.

Technology Assets Protection Association URL: http://www.tapaonline.org/new/engl/index.html (visited 2005, May 3).

U.S. Coast Guard MTSA URL: http://www.uscg.mil/hq/g-m/mp/rules.html (visited 2005, May 3).

U.S. Customs and Border Protection C-TPAT URL: http://www.customs.gov/linkhandler/cgov/import/commercial_enforcement/ctpat/validation_process_guidelines.ctt/validation_process_guidelines.pdf (visited 2005, May 3).

U.S. Customs and Border Protection FAST URL: http://www.customs.gov/xp/cgov/import/commercial_enforcement/ctpat/fast/us_canada/ (visited 2005, May 3).

U.S. Customs and Border Protection CSI URL: http://www.customs.gov/xp/cgov/border_security/international_activities/csi/ (visited 2005, may 3).

U.S. Customs and Border Protection ACE URL: http://www.cbp.gov/xp/cgov/toolbox/about/modernization/ace/ace_fact_sheet.xml (visited 2005, May 3).

U.S. Customs and Border Protection 24-Hour Rule URL: http://www.cbp.gov/xp/cgov/import/carriers/24hour_rule/ (visited 2005, May 3).

Vaghefi, R. (2000). Toyota story 2. Still winning the productivity game. Automotive Design and Production Business Strategy review, Vol. 11, Issue 1, 59-70.

Vasilash, G. (2000). Quality culture at Chrysler. Automotive Design and Production. Vol. 11, Issue 1, p.42.

World Shipping Council URL: http://www.worldshipping.org/. (visited 2005, May 3).

Appendix A

This Appendix contains brief descriptions of:

- Customs Trade Partnership Against Terrorism (C-TPAT)
- Free and Secure Trade (FAST)
- Container Security Initiative (CSI)
- Automated Commercial Environment (ACE)
- 24-hour Rule
- Maritime Transportation Security Act of 2001 (MTSA)
- International Ship and Port Facility Security Code (ISPS)
- Sarbanes-Oxley Act of 2002 (SOX)
- Smart and Secure Trade lanes Initiative (SST)
- Department of Homeland Security Advisory System (HSAS)

Customs Trade Partnership Against Terrorism (C-TPAT)

The United States Customs and Border Protection (CBP) instituted the C-TPAT program in November 2001. This public-private partnership, launched two months after the September 11, 2001 terrorist attacks, was born out of CBP's recognition that close cooperation with industry would be paramount to providing the highest level of supply chain security in the U.S. C-TPAT aims to engage the private sector in securing the global supply chain in exchange for streamlined inspection processes. In addition to these benefits, C-TPAT validation opens the door for participation in other CBP initiatives such as the Free and Secure Trade (FAST) program, the Container Security Initiative (CSI), and the Automated Commercial Environment (ACE).

Free and Secure Trade (FAST)

The FAST program, commenced in December 2002, improves coordination between participants in Mexico, Canada, and the U.S. to improve clearance procedures at border crossings. Some of these procedures include risk management, supply chain security practices, information technology, and partnering techniques. Through the FAST program, importers and carriers who are C-TPAT certified are allowed expedited clearance at border crossings. These C-TPAT carriers will use FAST dedicated border crossing lanes and experience reduced delays.

Container Security Initiative (CSI)

The Container Security Initiative (CSI) places U.S. inspectors at select high-volume ports overseas to improve clearance efficiency for cargo destined for the U.S. This program was initiated in January 2002, with the goal of pushing America's zone of security outward. CSI utilizes intelligence to target certain containers, prescreens targeted containers before they are loaded on to the ship, and uses smarter, more tamper-resistant containers. As of April 2005, CSI included twenty European ports, ten Asian ports, two Canadian ports and two African ports.

Automated Commercial Environment (ACE)

ACE is the new Customs and Border Patrol import information technology system that will replace the current Automated Commercial System (ACS) that has been in place since 1984. ACE aims to eventually automate much of the information processing for cargo crossing at U.S. borders.

24-Hour Rule

The 24-hour rule came into effect on December 22, 2002. This rule requires that all carriers provide CBP with cargo declarations 24-hours before cargo destined for the U.S. is loaded on a vessel at a foreign port.

International Ship and Port Facility Security Code (ISPS)

The International Maritime Organization (IMO) adopted the ISPS Code as an amendment to the Safety of Life at Sea Convention (SOLAS) in December, 2002. The ISPS, which came into effect in July 2004, requires risk assessment of vessels and port facilities, and identification of mitigation measures to address vulnerabilities.

Maritime Transportation Security Act of 2001 (MTSA)

Congress passed the MTSA in November 2001. The MTSA requires security plans and improvements for certain vessels, facilities, and outer continental shelf entities (i.e. offshore oil rigs), mandates the use of the Automatic Identification System for all deep draft vessels subject to the IMO's SOLAS convention, and mandates creation of Area Maritime Security Committees for all commercial ports. An important aspect of the MTSA is that owner/operators is responsible for securing their own facilities, with federal oversight primarily by the U.S. Coast Guard.

Sarbanes-Oxley Act of 2002 (SOX)

Congress passed The Sarbanes-Oxley Act of 2002 in July 2002 in response to a series of high profile company collapses due to poor corporate financial practices. The stated goal of the Act is to "protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws."

Smart and Secure Tradelanes Initiatives (SST)

The Strategic Council on Security Technology launched the Smart and Secure Tradelanes Initiative (SST) in July 2002. This industry-driven program focuses on container security and tracking, utilizing infrastructure and technology advancements. This initiative aims to demonstrate the principles of existing government programs such as C-TPAT, CSI, and MTSA as discussed above.

Department of Homeland Security Advisory System (HSAS)

The HSAS comprises five threat levels, with corresponding colors, that alert U.S. citizens to potential threats, and indicates the level of protective measures to be taken when a specific sector or industry is threatened. The five threat levels include: low (green), guarded (blue), elevated (yellow), high (orange), and severe (red).

Appendix B

Name: _____ **Date:** _____
Title: _____
Company: _____
Contact tel: _____
Contact email: _____
Industry: _____ **Geography:** _____

Thank you for agreeing to speak with us and participate in our research project, we will try to use your time wisely. As part of our research project studying the supply chain response to terrorism, we are contacting senior security executives in various industries to better understand what role organizational culture plays in a firms' supply chain security and resilience practices. Your input will be very useful, as it will provide a data based perspective on the important issues that companies are dealing with in responding to the new threat.

Before we begin, let me give you a brief description of what we hope to accomplish through this interview. First, we are interested in finding out if there is such a thing as a "security culture." Second, we hope to determine what role, if any, your firm's corporate culture or other cultures such as safety or quality, have played in the development of this security culture. Finally, we are interested in determining how your security program and business continuity planning program interact.

Before we start, may we tape the conversation so we can focus on your responses rather than writing down your responses? We will use this only to check what we heard later on and these will not be shared outside of our research team at MIT. If you prefer, we would be happy to sign a Non-Disclosure Agreement (NDA) to assure you that we will protect the confidentiality of the information you provide us.

Our assessment of this questionnaire estimates that it will take approximately 30-45 minutes. We realize, however, that some additional time might allow us to dive deeper into certain subjects of interest and with less time we can prioritize certain questions. In order to be sure we honor your commitments, could you let us know how much time you have available for this interview?

1) *Could you give us your title and a brief overview of your role in the organization?*

2) *Could you provide us with a brief description of how your firm manages its security program?*

3) *What was the impetus behind creation of your security program, and what tools did you use to structure it?*
   a. *Safety program?*
   b. *Regulatory requirements?*
   c. *Public private partnership?*
   d. *Existing security program?*

4) *Where does your group fit in to the overall firm organization?*
   a. *In relation to risk management, security and business continuity planning?*

5) *How does your security program address integration with external partners?*
   a. *Suppliers?*
   b. *Customers?*
   c. *Regulators?*

6) *How is your security program integrated with operations and logistics?*

7) *Are your security personnel primarily responsible for security, or do they have other duties as well? If so, what are these?*
   a. *Human resources?*
   b. *Safety?*
   c. *Quality?*
   d. *Admin?*

8) *Do you feel that certain employee backgrounds are particularly conducive to embracing security principles? If so, why?*

9) *How are employees held accountable for adhering to the security program?*
   a. *Performance evaluations?*
   b. *Employee level or leadership level accountability?*
   c. *Example?*

10) *What kind of educational program do you have in place to educate new hires on security practices?*
   a. *Education?*
   b. *Regular training?*
   c. *Informal?*
   d. *Example?*

11) *How are details of the security program communicated to the broader organization?*
   a. *Reporting practices?*
   b. *Internal communication practices?*
   c. *Communication with external partners?*
   d. *Security to corporate?*
   e. *Example?*

12) *In what other ways do you instill the importance of security into your organization?*

13) *Do you feel that your security program has affected your organization's behavior or core beliefs, sometimes referred to as culture?*

14) *Can you provide an example of how your firm's security program or culture has contributed to avoiding a disruption?*
   a. *Example, training secretaries to keep a look out for unusual people*

15) How does your security culture fit, or not fit, with your organization's overall corporate culture?

a. *Examples?*

16) Can you describe any other programs that have affected your organization's behavior or core beliefs, such as safety or quality?

b. *Safety? Railroad industry, safety briefings not only in the field but during office briefs as well...*
c. *Quality?*
d. *Environmental compliance?*

17) How are these programs related to your security program? Are they coordinated in any way?

18) How has the other program (Safety, Quality) affected your security program?

19) On a scale of 1-5 with 1 being fully satisfied and 5 fully dissatisfied, how satisfied are you and your company with the performance of the security program?

20) Does your firm have a business continuity program?

a. *Business Continuity Plan?*
b. *Test/Revisit/Update the plan?*
c. *Does the BCP address external partners?*

21) How does your firm coordinate its security program with its business continuity planning program?

22) Who leads the business continuity program in your firm, and may we speak with them?

23) Is there anything else that we haven't covered that you feel would be relevant to the purposes of this interview?

24) In your opinion, what companies have a strong security culture?

Appendix C

Matrix outlining interview observations for each company.

Notes:

1) Company names are disguised. See Table 3-1 for general characteristics of each company.

2) Boxes marked with an "x" indicate that that specific practice was discussed during the interview. If a box is not marked with an "x," this does not mean that a company does not conduct that specific practice, but rather that the practice did not come up in the interview. This implies that the practice ism most likely not a core part of the company's security or business continuity program.

3) Some observations have been inferred by the author.

4) The two consulting companies that were also interviewed are not included in this matrix, since their experiences reflect on practices conducted by their clients, not by their own company.

Companies A through K

			A	B	C	D	E	F	G	H	I	J	K
Artifacts		Completed	x	x	x	x	x	x	x	x	x	x	x
Work Practices and Infrastructure	**Security Program Organization**	Decentralized security program	x	x	x	x	x	x	x		x	x	x
		Corporate security refers to themselves as consultant				x	x	x	x			x	x
		Conducts drills	x	x			x	x					x
		Maintains 24-hour crisis center					x						
		Views disconnect between security concerns in US and internationally											
	C-TPAT Initiatives	C-TPAT basis for security program structure/improvements		x		x			x			x	
		Security program in place before C-TPAT											

			A	B	C	D	E	F	G	H	I	J	K
		Security requirements in contract with suppliers	x	x	x	x	x		x		x	x	x
		Say C-TPAT has increased awareness		x			x		x			x	x
		Views C-TPAT as voluntary, but really "involuntary"		x					x				
	Overlap with Safety	Shares structure with safety program		x		x	x				x		
		Has strong safety culture	x	x	x	x	x	x	x				
		Feels safety and security should be separate						x				x	
	Overlap with Quality	Utilizes Six Sigma methods									x		
		Share structure with quality model											
	Overlap with BCP	BCP run by cross-functional committee	x		x	x	x		x				x

			A	B	C	D	E	F	G	H	I	J	K
		Security and BCP interact at corporate level	x		x	x		x			x		x
		Security and BCP interact at emergency response group level	x		x		x				x	x	x
		Feels BCP needs improvement		x					x			x	
	Collaboration	Collaboration with industry			x		x				x		x
		Collaboration with government	x	x	x		x	x					
		Collaboration at executive level with other depts. (formally)			x			x			x	x	x
		Collaboration with sourcing					x						
Human Resource Practices	**Background Screening**	Conducts background screening of employees										x	
		Conducts background screening of supplier's employees										x	

			A	B	C	D	E	F	G	H	I	J	K
		Security seeks people with international or LE experience						x					x
	Distribution and Duties of Personnel	Security collateral duty of local personnel with other duties		x			x	x	x		x	x	x
		Utilizes third party security personnel					x						x
Education	**Employee Education**	Trains employees at orientation	x	x		x		x	x				x
		Uses web-based training		x	x		x				x		
		Uses socialization techniques										x	
	Supplier Education	Conducts supplier education			x		x	x	x			x	
Measurement Systems	**Audits**	Security audits integrated with quality audits							x				
		Security audits integrated with safety audits	x										

			A	B	C	D	E	F	G	H	I	J	K
		Security audits integrated with administrative audits		x									x
	Financial Analysis	Conducts financial analysis/risk management to justify and determine effectiveness of security measures	x	x		x	x	x			x	x	x
		Views making business case for security as fundamental	x			x					x	x	
		Views security always as added cost		x				x					
		View security as competitive advantage					x					x	
		Doesn't view security as a competitive advantage											
		Feels that it's better to get security needs met at the beginning of a project					x		x				

			A	B	C	D	E	F	G	H	I	J	K
		Feels that security has brought financial benefit											
Communication	**Communication**	Uses Internet for communication		x			x					x	x
		Conducts intelligence assessment					x						
		Views communication as essential to security program	x	x	x	x	x	x					
Leadership	**Leadership**	Corporate leadership vocal about security importance	x								x	x	
Responsibility	**Placement in Corporate Structure**	Security falls under operations		x									
		Security falls under HR					x						
		Security falls under legal			x		x					x	
		Security falls under quality							x				
		Security falls under CFO					x	x			x		

			A	B	C	D	E	F	G	H	I	J	K
		Security reports to CEO (admin)											
		Security falls under corporate services											x
		Security falls under supply chain	x										
		Security falls under compliance											
	Individual Performance evaluations	Security included in individual performance evaluations			x						x		
		Financial incentives offered											
Value System	**Value System**	Quoted company mission statement/core values/code of conduct			x			x				x	
		"Doing the right thing" considered element of culture	x			x		x	x		x	x	x
	Inferred Supply Chain Security Drivers	Protect brand	x						x			x	x
		Protect customer	x	x							x		

			A	B	C	D	E	F	G	H	I	J	K
		Protect product quality	x										
		Protect from delays							x				
		Protect employees - safe workplace		x	x	x	x				x		x
		Protect from theft						x					
		Protect from terrorism		x		x		x					x
		Protect environment											
		Being socially responsible											

Companies L through U

			L	M	N	O	P	Q	R	S	T	U
Artifacts		Completed	x	x	x	x	x	x	x	x	x	x
Work Practices and Infrastructure	**Security Program Organization**	Decentralized security program	x		x	x	x	x	x	x	x	x
		Corporate security refers to themselves as consultant			x							
		Conducts drills	x		x	x				x	x	x
		Maintains 24-hour crisis center						x			x	x
		Views disconnect between security concerns in US and internationally				x	x					
	C-TPAT Initiatives	C-TPAT basis for security program structure/improvements	x	x				x	x	x	x	

			L	M	N	O	P	Q	R	S	T	U
		Security program in place before C-TPAT				x						x
		Security requirements in contract with suppliers				x			x	x	x	x
		Say C-TPAT has increased awareness	x				x		x	x	x	
		Views C-TPAT as voluntary, but really "involuntary"					x			x		
	Overlap with Safety	Shares structure with safety program	x			x	x					
		Has strong safety culture				x		x				
		Feels safety and security should be separate						x				
	Overlap with Quality	Utilizes Six Sigma methods								x		
		Share structure with quality model	x									

			L	M	N	O	P	Q	R	S	T	U
	Overlap with BCP	BCP run by cross-functional committee	x				x				x	x
		Security and BCP interact at corporate level	x	x	x			x			x	x
		Security and BCP interact at emergency response group level			x					x		
		Feels BCP needs improvement	x						x			
	Collaboration	Collaboration with industry		x		x	x		x	x		x
		Collaboration with government		x			x					
		Collaboration at executive level with other depts. (formally)	x	x		x		x		x		
		Collaboration with sourcing			x			x	x	x	x	

			L	M	N	O	P	Q	R	S	T	U
Human Resource Practices	**Background Screening**	Conducts background screening of employees					x	x	x			
		Conducts background screening of supplier's employees							x			
		Security seeks people with international or LE experience						x			x	
	Distribution and Duties of Personnel	Security collateral duty of local personnel with other duties	x				x	x		x		x
		Utilizes third party security personnel										x
Education	**Employee Education**	Trains employees at orientation	x			x		x			x	x
		Uses web-based training	x		x	x		x		x	x	
		Uses socialization techniques							x			

			L	M	N	O	P	Q	R	S	T	U
	Supplier Education	Conducts supplier education		x								
Measurement Systems	**Audits**	Security audits integrated with quality audits	x						x			
		Security audits integrated with safety audits										
		Security audits integrated with administrative audits		x						x		
	Financial Analysis	Conducts financial analysis/risk management to justify and determine effectiveness of security measures			x	x	x	x		x	x	
		Views making business case for security as fundamental				x		x			x	
		Views security as added cost										

			L	M	N	O	P	Q	R	S	T	U
		View security as competitive advantage				x						
		Doesn't view security as a competitive advantage		x					x			x
		Feels that it's better to get security needs met at the beginning of a project			x							
		Feels that security has brought financial benefit				x	x					
Communication	**Communication**	Uses Internet for communication	x		x	x		x				
		Conducts intelligence assessment						x			x	
		Views communication as essential to security program					x				x	x
Leadership	**Leadership**	Corporate leadership vocal about security importance						x			x	

			L	M	N	O	P	Q	R	S	T	U
Responsibility	**Placement in Corporate Structure**	Security falls under operations				x						x
		Security falls under HR	x									
		Security falls under legal						x		x		
		Security falls under quality										
		Security falls under CFO										
		Security falls under admin			x							
		Security falls under corporate services										
		Security falls under supply chain										
		Security falls under compliance										
		Security falls under govt. policy					x					
		Security falls under assets protection							x		x	

			L	M	N	O	P	Q	R	S	T	U
	Individual Performance evaluations	Security included in individual performance evaluations			x					x		x
		Financial incentives offered	x		x							x
Value System	**Value System**	Quoted company mission statement/core values/code of conduct	x		x				x		x	
		"Doing the right thing" considered element of culture			*x*				*x*			
	Inferred Supply Chain Security Drivers	Protect brand					x					
		Protect customer									x	x
		Protect product quality	x					x		x	x	

			L	M	N	O	P	Q	R	S	T	U
		Protect from delays								x	x	
		Protect employees - safe workplace	x								x	
		Protect from theft		x						x		x
		Protect from terrorism				x		x		x	x	x
		Protect environment				x						
		Being socially responsible				x			x			