2003

What are the Elements of a Successful Training Model, as Perceived by Global Corporate Security Heads Working in the Ethical Pharmaceutical Industry?

Kevin P. Schatzle
Seton Hall University

Abstract

The issue of *properly* trained security personnel has received more focus and attention since the terrorist attacks on New York City and Washington, D.C. on September 11, 2001. However, there remains a dearth of material on security training, as detailed in Chapter II. Available material is not comprehensive.

The purpose of this qualitative study was to identify the elements of an effective training model for security personnel as perceived by global corporate security heads working for the top ten ethical pharmaceutical companies. The significance of this study rests with the impact that key elements gleaned from the interviews with these global heads will have on developing the training model. "Only through the development of a researched body of knowledge would security gain its place in academia and be properly prepared to equip the security practitioners of the future"(Koletar, 1999, p. 220).

Nine of the ten global security heads solicited agreed to participate in this study. The investigator conducted one-on-one interviews with each global security head. Interviews ranged from thirty minutes to sixty minutes in length and were conducted in person or by telephone, depending upon each respondent's preference. Each person as asked seven identical questions.

Findings of the study included common descriptions of barriers, best practices, ineffective practices, and the effect of budget on security training. Where applicable, comparative information from Chapter II was incorporated with responses from the nine global heads.

It was found that the issue of budget, and how it is administered toward security training, is a key element in providing successful training.

The elements of keeping security training a priority while responsibly administering budgets with all other corporate demands; incorporating business-related information into training sessions; utilizing various learning techniques; and including all levels within the security organization were recommended as key elements to an effective training model for security personnel. Recommendations for future research were also included.

What Are the Elements of a Successful Training Model, as Perceived by Global Corporate Security Heads Working in the Ethical Pharmaceutical Industry?

Kevin P. Schatzle

Dissertation Committee

Anthony J. Colella, Ph.D, Mentor

Drew Cangelosi, Ph.D

Reverend Christopher J. Hynes, D. Min.

Edward A. Schmalz, Ed.D

Submitted in Partial Fulfillment of the Requirements of the Degree of

Doctor of Education

Seton Hall University

2003

DEDICATION

To Patricia Schatzle, my Mom. Your love, guidance and spirit are my inspiration. I love you.

ACKNOWLEDGEMENTS

The most difficult part of the dissertation process is probably writing this section, where I have the opportunity to acknowledge and thank those who have helped, guided, supported, and loved me during this process. The number of people who were part of it in one way or another is quite overwhelming. Some, though no longer living, still live in my heart, specifically my grandparents, Charlie and Grace Waugh and William and Viola Schatzle: Thank you for your early love and support. Also gone, but not forgotten, is the late Charles Hetzel, "Papa Charlie," who, from the moment I entered the master's program, refused to call me anything other than "Dr. Schatzle." Papa Charlie, I did it. Thank you!

Thank-you to my mentor, Dr. Anthony Colella, for your guidance, support and encouragement. My committee, Rev., Dr. Chris Hynes, Dr. Edward Schmalz, and Dr. Drew Cangelosi provided invaluable insights and guidance. Thank you all for helping me get through.

Finally, thanks to my family and friends for your support, love, and inspiration to finish this project. Mom, Dad, Robert, Thomas, Eileen and Sonny

Iasenza, my "other" mom and dad, and Paul Brady, I am glad for having you in my life and I love you dearly. Brady you're next to do this!

Thank-you Dana Milligan for the time, effort, support, empathy and caring that you gave that helped me complete the study. I don't think anyone else would have so patiently sat through all the hours of tape transcription and edits that you did.

Thanks and much gratitude also to Jim Christian, and Dr. Daniel Vasella, you are truly marvelous leaders and very special people. To Ross Volk for your allowing me the tools and time I needed, the nine security heads who dedicated their time and perceptions and to those many other individuals, too numerous to mention, thank you. May God bless all of you!

TABLE OF CONTENTS

CHAPTER I

Introduction

Prior to September 11, 2001 the term *security* was to many people an abstract notion. It was often associated with an image of a security guard sleeping at his desk, standing in a booth checking in visitors, or sitting behind an x-ray machine at the airport. Few people were aware of the level of professionalism among security practitioners. Even further overlooked was the way in which security personnel, at all levels, were trained to do their jobs. According to Roth 2001, "For years the U.S. Security market has been based almost entirely on price" (p. 6).

The aftermath of September 11, 2001 changed many things, including the focus on security. Since the attacks on September 11, 2001, the most visual example of the change in focus on security is illustrated with the new approach to airport security. Airport security, once considered to be a formality and a bother, is now under constant scrutiny and has become part of the newly formed federal agency known as the Transportation Security Administration, or T.S.A.

Among other duties, the T.S.A. has taken over responsibility for providing security personnel at airport facilities across the United States (T.S.A., 2001). Along with providing personnel, the agency is charged with "properly" training the individuals manning x-ray machines, metal detectors, and other screening devices. It seems that people now want security check points and question why the need for them has not been taken as seriously as it should have been before the attacks. America has been threatened and its citizens are

eager to employ whatever security needs are necessary and are now ready to spend time and money on security upgrades.

Much discussion has taken place about the apparent lack of training provided to the airport security personnel prior to September 11, 2001, now known simply as "9-11." Television reporters are continuously producing stories about how easy it is to get past airport security with some of the prohibited items now on the FAA's *Prohibited Items List*. Many people are now calling for better training for airport security personnel.

The importance of training security personnel is not limited to those working in airport security, nor is it only applicable to certain levels within a security organization. Unfortunately, the airline industry has been placed under the microscope because of the events of September 11, 2001. Undeniably, the safety and security of those flying aboard airplanes is important: The airline industry is still reeling from the after math of September 11, 2001 and will most likely never be the same. Other industries are also vulnerable, and the security of some of them is now a national priority. These industries are in high need of properly trained security personnel at all levels.

One such industry is the pharmaceutical industry. Not only does this industry need security for personnel, intellectual property, and company assets; it is also heavily engaged in research projects, some of which are closely scrutinized by the government, and all of which are especially vulnerable. Coupled with this is the additional element of companies potentially working with toxins and other biological and chemical substances, making it all

the more important for security personnel working at pharmaceutical companies to be properly trained.

Before September 11th many of these concerns existed mainly on the part of industry personnel. However, the letters contaminated with anthrax that were sent out through the mail in October and November 2001 raised most people's awareness to the potential damage that could be done by virtually anyone. The deaths attributed to anthrax poisoning and the fear that was instilled every time someone opened a letter with a "strange" substance in it will long be remembered. Furthermore, by most estimates, over 85% of the country's infrastructure is privately owned. This leaves a large responsibility on the part of security organizations. There is now a sense of urgency to provide a broad blanket of protection.

Small amounts of toxic material can be used to harm relatively large numbers of people, so can other measures if not properly prepared for. Despite these dangers, there is a dearth of material on security training in this area.

Statement of the Problem

As borne out by the results of the literature review for this study, reported in Chapter II, literature on security training is not plentiful, nor is it comprehensive. With only one peer-reviewed American journal in the field, *Security Journal*, and one widely read magazine, *Security Magazine*, both of which are published by the largest professional security organization, the American Society for Industrial Security (ASIS), the choices for security professionals with a serious interest in enhancing training programs are limited.

These sources and others generally address narrow security-related issues, such as loss prevention, fire safety, and information security. There is little material in the periodical literature about training security personnel. It appears that the contract security service companies attempting to sell their services use the word "training", as do security managers who are frequently quoted in journals and magazines. However, surprisingly little has been written about the specific training needs or, more importantly, the best ways to meet them. There certainly are no easy answers. Vaill (1996) defines learning as follows: "Learning: changes a person makes in himself or herself that increase the know-why and/or the know-what and/or the know-how the person possesses with respect to a given subject" p. 96. Vaill also asserts that there are formidable barriers to conducting the kind of continual learning that is needed.

Purpose of the Study

The literature review outlines several philosophies on the topic of training security personnel. The limited amount of information on training models successfully keeping up with the seemingly alarming pace for which professionals are being required to provide competent personnel may be placing security heads in a difficult position.

The purpose of this study is to identify the elements of an effective training model for security personnel as perceived by global corporate security heads working in the ethical pharmaceutical industry. Research that depicts perceived best practices for establishing a training model by those individuals ultimately responsible for their security departments will help address the areas most needed for a successful operation. The

researcher will attempt to identify those ideal best practices for security training as perceived by global security heads working in the ethical pharmaceutical industry.

Significance of the Study

The importance of having properly trained security personnel from the head of the organization on down cannot be emphasized enough. According to Goodboe (1995), "There may be a temptation to view concern with training methodology as unwarranted in an industry characterized by high turnover and a fairly transient workforce. But security professionals should recognize that quality service is impossible without effective training... The better the training of the security workforce, the better service they will provide, and the more respect the industry will gain" (p. 4). However, the demographics of the lowest levels of security force employment--their lack of formal education, their willingness to accept low wages, and the high rate of turnover--are all factors leading many companies to spend as little of their resources as possible on training these individuals. In addition, the *culture* of the security business, with its vaguely military/police-like traditions and structure may also explain some of the problems with the quality of training among security personnel.

Quite a bit has been written about the need for having properly trained security personnel; however, as of this writing, little has been done to implement effective training programs. The government has attempted to look at the issue with funded reports but this too has been limited in both scope and effectiveness. Also, heads of security organizations have not been queried in a concerted effort to collect their perceptions on the issue of training. As the potential *change agent*, the perceptions on security training from individuals heading the security organization is a key element currently missing from the

literature. According to Leedy & Ormrod (2001), perceptions obtained from a phenomenological study allows the researcher to "look at multiple perspectives in the same situation and then make some generalization of what something is like from an insider's perspective" (p. 153). The collection of this "insider's perspective has the potential of allowing for the development of a model that contains key elements for successful training. These key elements can then be utilized by security practioners in setting up training programs more adequately suited for providing their personnel with the necessary tools to accomplish the job. "Only through the development of a researched body of knowledge would security gain its place in academia and be properly prepared to equip the security practitioners of the future" (Koletar, 1999, p. 2).

Primary Research Question

The primary question to be addressed by this study is: What are the elements of a successful training model, as perceived by global corporate security heads working in the ethical pharmaceutical industry?

Secondary Research Questions

Secondary research questions that will be addressed are as follows:

1. What do you perceive to be the ideal best practices for a global corporate security training program?
2. What practices are ineffective in setting up successfully run security departments?
3. What impact does budget have on training security personnel?

4. How does the placement of training within the organization affect training security personnel?
5. What do you perceive to be barriers to setting up training for security personnel?
6. How does the training of security personnel for the ethical pharmaceutical industry differ from the training of other security personnel?

Definition of Terms

For the purpose of this study, the following definitions will be used:

American Society for Industrial Security (ASIS): A professional organization of security professionals from around the world which issues professional certifications of competency.

Contract Security Services: Personnel paid by an outside service company.

Global Corporate Security Department: A department in which there is global responsibility for the protection of company personnel and assets.

Global Head of Security: An individual ultimately responsible for administrative, technical, strategic, and budgetary issues of the global department.

HealthAce, Inc.: A private entity that compiles financial data about companies and then ranks each company according to the market value.

Properly Trained: Individuals who receive the elements of training that appear to provide them with the tools necessary to complete the many tasks required of them.

Proprietary Security Services: Personnel performing the duties of security whose salary and benefits are paid directly by the company and not by a contracted service provider.

Security Journal: The publication which is published by ASIS on a quarterly basis and is peer reviewed prior to articles appearing in the journal.

Security Management Magazine: The monthly non-peer reviewed publication of ASIS.

Top 10 Ethical Pharmaceutical Companies: A business primarily centered on the research, development, patenting, and branding of prescription drug products listed in order of Market Capital as reported by (HealthAce, Intelligence Briefing August 2003).

Training Program: The courses taught to security personnel prior to their being deemed to be ready for duty.

Population to be Studied

The population to be studied are the global corporate heads of security working in the top 10 companies within the ethical pharmaceutical industry that have global security organizations. It should be noted that all of these, as well as those heads of security who were mentioned by name and quoted, were male. The investigator realizes and acknowledges the non-sexist nature of this work and has referred to those authors as *he* because of the nature of the population and for ease of reading.

Limitations

The following limitations apply to this study and thereby affect the internal validity and reliability of information gathered:

1. Position titles may be different. In addition, position responsibilities and their perceived influence on their departments may vary based on the culture or mores of an individual company.
2. Global corporate security departments will vary in size of staff, budget, and span of control.
3. Matrix management schemes may affect the influence of the global corporate security heads.

Delimitation

The study is limited to the top 10 ethical pharmaceutical companies with global corporate security departments. Results may therefore not be generalizable to other pharmaceutical companies or to other security personnel.

Organization of the Study

The study consists of five chapters, which are organized as follows:

Chapter I contains the Introduction, a Statement of the Problem, the Purpose of the Study, the Significance of the Study, Primary and Secondary Research Questions, Definitions of Terms, the Population to be Studied, Limitations and Delimitations of the Study, and the Organization of the Study.

Chapter II provides a Review of the Literature related to security training and educational programs. It includes The State of Research and Publication, the Organizational Environment, Pharmaceutical Organizational Environment, Conceptual Framework, Adult

Learning, Learning Styles, Teaching Styles, Electronic Media and Distance Learning, Security Education and Training Models, Professional Training, Certification and Professional Standards, Academic Programs, Security Training Content and Training Methodologies.

Chapter III is the Research Design and Methodology section. The Research Design, Subjects of the study, Instrumentation, Data collection, and Treatment of the data are described.

Chapter IV presents the Findings of the study derived from responses to interview questions posed to selected global corporate security heads.

Chapter V contains the Summary and Discussions of the study. The researcher will interpret the results and provide a discussion related to interview responses and the related Literature on the subject. Recommendations for further study and research will also be included.

A reference list and appropriate Appendices will follow Chapter V.

CHAPTER II

Review of the Literature

Introduction

Since the September 11, 2001 attacks on the World Trade Center in New York and the Pentagon in Washington, D.C., there has been an upsurge in demand in the security guard industry, currently valued at about $17 billion a year, as well as increased media attention to the many issues related to security (Roth, 2001). For most of America's manufacturing corporations, however, security has long been part of the organizational environment and its budget. While the increasing use of private security personnel and services in roles traditionally filled by public police and law enforcement agencies is not within the scope of this research, the long-running debate over the use of *contract* security by corporations is of current interest.

The private security industry tends to promote its law enforcement and military discipline as a sales benefit (Roth, 2001), but this approach has not always had the desired effect. "In 1992, *Time* [Magazine] labeled security officers 'thugs in uniform' after a constant stream of stories about guards stealing, murdering, or maybe just setting a business afire. The horror stories slowed when, in response, states started pushing through minimum hiring and training requirements. Still, the stigma never quite wore off" (p. 3).

Contract security personnel for-hire have existed since the Middle Ages, in one form or another. In the United States, civil and labor unrest and concerns about espionage in the first part of the 20th century led many companies to form their own *proprietary*

security forces, generally for the intangible benefits of perceived company loyalty, lower turnover (and, therefore, lower training costs), and quality. However, over the years, the cost of proprietary security kept pace with rising employee costs, encouraging many companies to begin to contract out their security services. As Roth (2001) says, "For years the U.S. security market has been one based almost entirely on price" (p. 2).

Because contract security arrangements are strictly fee-for-service, the hourly rate is usually lower than it would be for proprietary employees, especially because most security companies pay for benefits packages. In 1994, Simonsen and Nelson reported these lower hourly rates, but the American Society for Industrial Security (ASIS) 2001 Employment Survey, cosponsored by Pinkerton, reports that while unarmed contract personnel did earn $1.00-$3.00 less per hour than proprietary employees, armed proprietary employees were less expensive than contract personnel (*ASIS International*, 2002, p. xvi). In the 1990s, proprietary security forces made up less than 20% of all those employed in security (Cunningham, *et al.*, 1990, as cited in Simonsen & Nelson, 1994, p. 197).

Respondents in *Security Management*/Pinkertons survey were asked to identify those security functions which are handled in-house and which are outsourced or performed by a hybrid operational staff. The findings were that physical asset protective services were more likely to be contracted out than services designed to protect sensitive information or processes. For example, just over one-third of the respondents indicated that the company used outside patrol services, while more than three-fourths said that they use

proprietary personnel for computer/network security, proprietary information protection, crisis management, and contingency planning (Harowitz, 1997).

Ledoux (1995), security services manager for Syntex, Inc., a pharmaceutical firm, conducted his own research to determine whether his department and his corporation should outsource security services. Initially, he believed that doing so would neither save money nor provide the corporation with professional-quality security services. When he analyzed his budget, he realized that personnel costs were extremely high, primarily due to the corporation's policy of treating "all employees, including security officers and receptionists, as though they were upwardly mobile members of the corporate culture, promotable to higher positions in other corporate divisions, rather than as service providers with limited upward mobility" (p. 2).

The next step Ledoux (1995) took was to poll more than a dozen other large pharmaceutical corporations across the country, and found, to his surprise, that only one was using only proprietary security personnel. The rest offered high wages to contract personnel and used their in-house security professionals to supervise, manage, and train them. On another issue, none of the corporations surveyed said that they accepted the lowest contractor bid. In terms of training, Ledoux found that his counterparts were setting their own training standards and managing their contracts so that those standards were maintained.

At the same time that contract services are being used more frequently, technology is making some security personnel unnecessary, so that those who remain in the field need

more technical qualifications, more education, and more sophisticated training (Simonsen & Nelson, 1994, p. 197). Another growing trend in both proprietary and contract security services is toward building professionalization. Roth (2001) profiles Securitas, the security services firm which holds approximately 20% of the U. S. security market and owns Pinkertons and Burns, two of the largest American firms. The firm's "goal is to turn the industry from one dominated by lowest-bidder-wins contracting to one in which companies are willing to pay more for better quality," according to the New York-New Jersey regional president at Securitas, Jack Donohue (quoted in Roth, 2001, pp. 2-3). According to Donohue, it has been so easy to start a private security company, that there were always enough to underbid. He points out that "the median earnings for a guard last year [2000] were $8.45 an hour, less than those of telemarketers, movers, and secretaries—yet a guard's chances of dying on the job are at least two to three times higher than in those other professions. That explains why turnover for American guards' falls somewhere between 120% and 200%" (Roth, 2001, p. 4).

The State of Research and Publication

"Only through the development of a researched body of knowledge would security gain its place in academia and be properly prepared to equip the security practitioners of the future" (Koletar, 1999, p. 220). The American Society for Industrial Security (ASIS) publishes *Security Management*, a monthly journal, which is also available online, including archives and an interactive online bulletin board, *SM Forums* (www.asisonline.org). In the information and computer security field, both *Information*

Security, a journal, and *Security Wire*, an online newsletter, are published. A number of the journals in the safety field cover security, such as *Professional Safety*. Newsletters cover specific aspects of the field, such as *Private Security Case Law Reporter*, *Security Law Newsletter*, and *Corporate Security*. A number of Canadian and British publications address corporate and industrial security. Relevant articles may be found in the criminal justice and law enforcement magazines and journals and in industry-specific and corporate literature. The fastest-growing segment of publications related to security has to do with information and computer technology.

The primary publications in the field, however, remain those published by the ASIS International, the monthly *Security Management*, for anecdotal material, and *Security Journal*, a quarterly peer-reviewed journal for research and analysis. As practitioners continue to professionalize, presumably the research work will expand. As things stand now, this literature review relies heavily on articles published in *Security Management* for material about security and organizational issues and solutions. The contextual framework underlying security training, adult learning, was found in training and social science journals.

The Organizational Environment

The most important factors in the organizational environment in relation to training the security force are the position of the security function and its role in the organization's operations. Underlying these factors is the scope of the security function. Traditionally, protection of a corporation's physical assets (*i.e.*, buildings, grounds, and equipment) is the first priority for security. More recently, however, top management has come to realize that its human resources and intangible assets (*i.e.*, intellectual property) are also at risk.

One further characteristic of the security function that makes it a complex training challenge is that the modern organization requires both proactive and reactive contributions. That is, the corporation needs security's expertise in responding effectively to accidents, incidents, criminal activity, and other crisis situations at the same time that it needs security's expertise in assessing risks, preventing losses, defusing potential crisis situations, and planning for responses to emergencies. These needs represent the range of *customers* for security services within an organization.

Freimuth (1996) notes that in most corporations, security's customers are internal, although many corporations have multiple manufacturing and research facilities, sometimes widespread geographically, and many have outsourced some manufacturing or quality control processes. In terms of internal customers, the most prominent example is perhaps the human resources department, where most hiring, firing, and dealing with difficult or troubled employees takes place.

Millwee (1999) urges security professionals to "step up and lend [their] expertise" (p. 1) to three specific functions: terminating potentially violent employees, screening applicants' backgrounds, and conducting sensitive interviews. In Millwee's view, security should be concerned with identifying risks, conducting threat assessments and background investigations, and dealing with terminated employees who might be at risk for retaliation against the corporation.

In order to describe how security departments operate within corporate organizational structures, *Security Management* and Pinkertons, Inc. sent a survey to security professionals in Fortune 1000 companies and security managers from among the journal's subscribers. The survey questions pertained to budgets, security's relationship to and interaction with senior management, use of outsourcing for security services, quality issues (*e.g.*, measurements and benchmarking), and strategic planning (Harowitz, 1997).

Ten percent of those surveyed responded that their security departments reported directly to the head of the organization; 73 percent said the department reported to the executive level. The others reported to human resources (22%), administration (20%), facilities (19%), and operations (14%) (Harowitz, 1997, p. 3).

In an attempt to capture information about security's proactive role, the survey included a list of ten issues addressing whether, and how often, security had been consulted about them. The respondents reported that they are "most likely to be consulted on matters relating to risk management (33% always, 59% sometimes), facility consolidation (29% always, 49% sometimes), staffing/hiring (20% always, 56 % sometimes). They also

indicated that they are often—if not always—consulted with regard to global exposure, real estate, acquisitions, and strategic planning (Harowitz, 1997).

Dalton (2001) contends that "the issue is not where security should report but what its function within the organization should be" (p. 1). Dalton describes several models of the security function, including the *Green Shack* model (referring to the traditional physical location of the security department at or near the front gate), with its emphasis on facility protection; the *Physical Security* model, with its emphasis on escorting visitors, patrolling buildings and grounds, controlling traffic, and staffing the front desk; and the more recent *Corporate Security* model. The latter, the most recent to take hold, expanded the role of security from the front gate into protecting executives and developing quality standards (*i.e.,* systems engineering), while at the same time streamlining (*i.e.,* downsizing).

In the Corporate Security model, both the departmental structure and the ways in which security services are delivered are redefined. Outsourcing some services and integrating security into other corporate functional areas has gradually evolved into the model that characterizes many security departments today--the *Consulting* model. There has been a shift from operations-oriented staffing to "a small cadre of professionals offering in-house consulting and specialized services" (Dalton, 2001, p. 3). In addition to wide and deep knowledge of security issues and practices, in-house consulting security professionals need considerable skills in selling their internal customers on the risks and benefits to them of the security strategies they recommend. With regard to strategic planning, one-third of the respondents in the *Security Management*/Pinkertons survey cited

the need for security involvement as a top priority, behind risk management and staffing/hiring. More than two-thirds reported that their organizations had developed a security strategy, and that the security function developed the operational plans linked to it (Harowitz, 1997).

As Dalton (2001) describes it, the *Consulting* model of security "is built on collaboration with internal partners and not on competition with them" (p. 3). The Consulting model has not abandoned all of the traditional security responsibilities, but rather has refined them. For example, investigation is still a priority, but is more likely to involve theft of intellectual property than of an office's petty cash. While executive protection is still a priority, it is more likely to be proactive, concerned with creating policies and procedures, conducting management advance briefings, and collaborating in planning important events than providing bodyguard services.

Today, security managers are integrating the protection of intangible assets into their protective function as collaborators with the information management department. More than half of the respondents in the *Security Management*/Pinkertons survey reported at least some informal interaction with the information professionals in their organizations. In one company, outside consultants recommended that the organization form an information protection committee, including the physical security function as a member (Harowitz, 1997).

Dalton (2001) calls this focus the *Asset Protection* model, which addresses all of the corporation's assets, both tangible and intangible. With this focus, the security department

works with other corporate functions to proactively protect all kinds of intellectual property, including sensitive competitive, proprietary, and confidential information. This collaborative approach emphasizes teamwork, as security assumes the role of advisor rather than direct manager of processes.

Rothke (2001) sees corporate espionage as a major threat to modern organizations and cites the guidelines developed by the National Counterintelligence Center (http://www.nacic.gov) to help corporations protect their information. It is interesting to note how many of the Center's recommendations could benefit from the experience and expertise of security professionals:

1. Obtain support for information security from senior management.

2. Do not waste resources protecting that which does not require protection.

3. If extremely sensitive, information should be hand-carried or transmitted using encryption techniques.

4. Identify what information should be protected and for how long.

5. To dispose of sensitive information, shred it or make it unreadable.

6. Valuable company information must not be left unattended in hotel rooms; this includes printed copies and removable media.

7. E-mail and voice-mail passwords must be protected and changed frequently.

8. All sensitive materials must be removed from conference rooms, and chalkboards and whiteboards must be erased after meetings.

9. Where possible, conduct background investigations on all individuals with access to sensitive information.

10. Obtain nondisclosure agreements from employees, vendors, and others with access to proprietary information.

11. The disgruntled employee is the greatest threat to your organization.

12. Telephone conversations, both fixed and mobile, are vulnerable to intercept.

13. Information regarding the movement of your company aircraft, including routes and destinations, is available for sale on the Internet.

14. Be knowledgeable regarding your organization's physical assets, information assets, and vulnerabilities (pp. 3-4).

The first essential step to protect data and information is to do a comprehensive risk assessment, something security professionals are trained to do, so that a preventive program can be developed. Once policies and procedures are developed, the security department would ideally be involved in training the appropriate supervisors and staff members in implementing them. In addition, the security professional can be helpful in conducting periodic reviews, to ensure that standards are met.

Rothke (2001) lists a number of resources for the security professional involved in protecting intangible corporate assets, including the Society of Competitive Intelligence Professionals (www.scip.org) and a training program for Certified Confidentiality Officers (CCO) (http://www.espionbusiness.com/faq.ivnu).

In Dalton's (2001) Asset Protection model, security professionals "need to truly understand their company's business. This means extending their knowledge base into the very heart of their company's products or services" (p. 3). With reference to the security of data and sensitive information, for example, Dalton recommends "a close working relationship" between the manager responsible for corporate-wide security and the manager responsible for data security (p.4). In this collaborative-advisory model, reporting relationships do not inhibit intangible property protection, but enhance it. When the primary responsibility for protecting information rests with the managers of key processes, the security professional is responsible for advice, planning, and educating both managers and their staffs, increasing both their awareness and their responsibility to secure their *own* intellectual property.

In support of this concept of *delegating* responsibility for security to managers, the *Security Management*/Pinkertons survey (Harowitz, 1997) identified a growing trend in budget allocation: "Security line items are going into the budget of the unit or project requiring the service rather than into the security department's operating budget" (p. 2) When end users are paying for security services out of their own budgets, they can control those costs to a certain extent. That means that they become security's customers, challenging security "not only to be competitive but also to develop sales skills" (p. 2) to convince unit managers of the cost-effectiveness of proposed security measures.

Harowitz (1997) offers an example from the multinational pharmaceutical industry, citing the case of a new assistant vice president of security who made it a top priority to

convene a meeting with senior management to obtain support for making security integral to the organization. Once he had their support, he met with his internal customers, the department managers, to increase their awareness of security concerns in their areas. He followed the same process with the members of his own team, meeting with them off-site, bringing in a consultant to help map out goals, and in general solidifying the department's mission. As the new vice president put it, "My idea was to start at ground zero and ask ourselves, what do we do, who are we, who are our customers?" (p. 5).

The Pharmaceutical Organizational Environment

There is surprisingly little material to be found in the security literature related to the pharmaceutical industry or in the pharmaceutical industry literature related to security. The most recent material to appear is, perhaps, suggestive of current priorities in the field. The huge trade in counterfeit drugs, an estimated 5 to 8% of total international pharmaceutical trade, puts patients at risk, but also undermines the public's confidence in the industry and exposes pharmaceutical manufacturers to complex liability issues (Gips, 2001). While the global problem of counterfeit drugs is outside the scope of this research, the related security issues demonstrate how the scope of the security professional's role has changed. In the referenced, two corporate security directors are quoted, suggesting that at least two major pharmaceutical corporations consider the problem to be a security issue.

Related to the counterfeiting problem is international pharmaceutical cargo theft, the subject of a symposium held in the Spring, 2002, co-sponsored by the American Society for Industrial Security (ASIS) and the National Cargo Security Council, and

described by the co-sponsors as the first of its kind. An examination of the speakers and the topics covered in the program indicate that pharmaceutical corporate security directors are closely involved with the problem. For example, the first session, addressing the vulnerability of drugs in storage or in transit, a manager of corporate investigations and a corporate director of security were on the panel with a police supervisor of one state's cargo theft unit and an FBI Special Agent. In another session, on packaging, two corporate security directors, an industry consultant, and a shipper's security director were scheduled to speak. A review of the topics covered suggests the collaborative role of corporate security directors with state and federal law enforcement agencies, insurers, carriers, shippers, and external investigators. The topics also reveal a balance between proactive and reactive strategies that manufacturers' security departments can adopt, including policies and procedures for storing and shipping pharmaceuticals, identifying potential thieves, investigating when employees are involved in theft, and collaborating with law enforcement in reporting thefts and recovering stolen goods.

Gips (1999b) profiled the security program at Glaxo Wellcome, one of the largest multinational pharmaceutical manufacturers, with half a dozen manufacturing and research facilities adjacent to each other in greater London, England, including a large animal breeding farm which had been a target of animal activists. As a result of the latter's activities, the corporation's security department regards preventing sabotage and intrusion as a major priority. A comprehensive range of physical security measures have been put in place, including fencing, intruder and fire alarms, cameras, motion detectors, back-up

response teams, and traffic control of both vehicles and pedestrians. Those are the perimeter measures; further systems are in place to control access to buildings and to critical areas within buildings.

According to Gips (1999b), another major priority at Glaxo Wellcome is prevention of physical property theft. The program includes policies and procedures designed to reduce the risk of theft by the many contract workers with access to the company's facilities, as well as by employees. In effect, the security department has educated and trained the entire work force to take responsibility for their own and the corporation's property. In terms of protection of information, those employees with access to sensitive information receive security awareness training when they are hired and regular bulletins thereafter. Access by visitors is controlled and when on-site conferences are held, trained members of the security department perform surveillance sweeps. To deal with bomb threats in various facilities, the security department has trained staff members to check their individual offices and work areas, coordinated by designated supervisors and supplemented by grounds and engineering staff.

The Glaxo Wellcome program attempts to address every risk area in the corporation and is highly detailed and comprehensive. It is included here because it represents the consultative, collaborative role of the modern security professional in a challenging organizational environment. In this organization, detailed risk analyses have been performed, vulnerabilities identified, and plans made—all with the advice and expertise of the security department. In addition, procedures and policies have been developed for all of

the corporation's managers, supervisors, and employees to follow in order to support the security of the corporation.

The Conceptual Framework

Adult Learning

Goodboe (1995) cautions that the focus of security training programs has typically been on topics to be covered, rather than methods used to teach program content. He believes that content and training methods are both essential to effective training, yet most security training employs traditional methods used in schools for children (*i.e.*, pedagogy) instead of methods designed for adult learners (*i.e.*, andragogy). Most educators agree that andragogy rests on the fundamental characteristics of the way adults learn: They prefer to be self-directed, rather than instructor-directed. They bring their unique life experiences with them and use that experience to determine what they need to learn. Their readiness to learn is directly related to the relevance of the material to their lives. Finally, they want to be able to apply what they have learned immediately in realistic circumstances. Kaupins (1997) adds that adults learn more when they somehow participate in their own learning experiences, which is the reason that role playing, on-the-job training exercises, case studies, and even interaction using electronic media are more likely to appeal to adult learners and the content is more likely to be retained.

Goodboe (1995) sees adult learning as a matter of attitude adjustment for instructors and learners. Instructors should see their role as facilitating, not dictating, and learners should take responsibility for their learning, rather than expecting it to be imposed on them.

The effectiveness of any training program depends on the instructor's or designer's awareness of the learners' styles of learning, as well as on awareness of the various styles of teaching than can be used.

Learning Styles

Grasha and Yangarber-Hicks (2000) offer these brief descriptions of learning styles:

Competitive: Students who learn material in order to perform better than others in the class. Believe they must compete with other students in a course for the rewards that are offered. Like to be the center of attention and to receive recognition for their accomplishments in class.

Collaborative: Typical of students who feel they can learn by sharing ideas and talents. They cooperate with teachers and like to work with others.

Avoidant: Describes students who are not enthusiastic about learning content and attending class. Do not participate with students and teachers in the classroom. They are typically uninterested and overwhelmed by what happens in class.

Participant: Try to be good citizens in class. Enjoy going to class and taking part in as much of the course activities as possible. Typically eager to do as much of the required and optional course requirements as they can.

Dependent: Show little intellectual curiosity and learn only what is required. View teacher and peers as sources of structure and support and look to authority figures for specific guidelines on what to do.

Independent: Students who like to think for themselves and are confident in their learning abilities. Prefer to learn the content that they feel is important and would prefer to work alone on course projects than to work with other students.(pp. 12-13)

The authors suggest that the way instructors present information will match some learning styles and not be compatible with others at any given point in a training program. They recommend that the method of instruction be varied, to challenge learners and support their learning in the long run. They say, for example, "A learner with a concrete-sequential thinking style, who prefers linear problem solving, could benefit from working on an ill-defined task in order to find a new way to think about issues" (p. 5).

Vaill (1996) suggests that seven qualities or modes of learning as a way of being are "especially important for learning in permanent white water" (p. 56). Although not to be viewed just as a list, the seven modes are: Self-directed learning, Creative Learning, Expressive learning, Feeling learning, On-line learning, Continual learning and Reflexive learning (p. 56).

Teaching Styles

Students' learning styles are useful to instructors designing training material, but instructors often neglect to consider their own teaching styles. Grasha (1994) developed a conceptual model of teaching style as multidimensional, affecting "how people presented information, interacted with students, managed classroom tasks, supervised coursework, socialized students to the field, and mentored students" (p. 2). His model describes five different styles: 'expert,' 'formal authority,' 'personal model,' 'facilitator,' and 'delegator,'

(p. 2) although he found that all five styles were present in teachers he studied, leading him to hypothesize four clusters made up of combinations of these styles. Grasha's research was also concerned with developing ways that teachers could adapt or modify their predominant teaching styles.

Grasha (1994) developed a Teaching Styles inventory, comprised of forty items referring to the attitudes and behaviors associated with each of the five teaching styles (p. 7). The styles are described as follows:

> *Expert*: Possesses knowledge and expertise that students need. Strives to maintain status as an expert among students by displaying detailed knowledge and by challenging students to enhance their competence. Concerned with transmitting information and ensuring that students are well prepared.
>
> *Formal Authority*: Possesses status among students because of knowledge and role.... Concerned with providing positive and negative feedback, establishing learning goals, expectations, and rules of conduct for students. Concerned with the 'correct, acceptable, and standard ways to do things.'
>
> *Personal Model*: Believes in 'teaching by personal example' and establishes a prototype for how to think and behave. Oversees, guides, and directs by showing how to do things, and encouraging students to observe and then to emulate the instructor's approach.
>
> *Facilitator*: Emphasizes the personal nature of teacher-student interactions. Guides students by asking questions, exploring options, suggesting alternatives, and

encouraging them to develop criteria to make informed choices. Overall goal is to develop in students the capacity for independent action and responsibility. Works with students on projects in a consultative fashion and provides much support and encouragement.

Delegator: Concerned with developing students' capacity to function autonomously. Students work independently on projects or as part of autonomous teams. The teacher is available at the request of students as a resource person.(pp 10-11)

Along with these descriptions, Grasha (1994) briefly notes the advantages and disadvantages of each style. In addition, Grasha provides a brief list of teaching methodologies that *fit* with each predominant style cluster. For example, the expert/facilitator/personal model style employs small group discussion, laboratory projects, instructor-designed group projects, self-discovery activities, learning pairs/debates, case studies, role-plays and simulations, problem-based learning, and guided readings (p. 12).

Finally, Grasha (1994) provides an outline of the factors associated with selecting a teaching style:

First: The capability of the students to handle the demands of the course, determined by the students' knowledge of the course content, ability to take initiative and responsibility, emotional maturity, and motivation and ability.

Second: The need for the teacher to directly control what goes on in the classroom, which is maintained by how the instructor organizes the course and defines what

must be learned, specifies performance levels for the students, maintains control over the classroom, and closely monitors students' progress.

Third, the willingness of the teacher to build and maintain relationships with the students, indicated by how much the teacher encourages two-way communication, listens carefully to students, helps resolve conflicts, provides positive feedback and encouragement, stresses good interpersonal communication skills, builds rapport, and shows students how to work together.(p. 13)

Grasha (1994) identifies four clusters or combinations of teaching styles and says that the *expert/formal authority* combination is most effective when learners know less about the content of the course and when instructors want to control class activities. In the combination style, the instructor does not see the need to work on developing relationships with learners or to help learners build relationships with each other.

The *expert/facilitative/delegative* combination is most effective when learners know the course content and are willing to exercise initiative and assume responsibility for their learning. To use this learner-centered style, instructors have to relinquish control over some class activities and empower learners. In this model, instructors spend time helping to develop relationships with and among learners in order to work effectively with them in a consultative role and to foster their ability to work together.

The *expert/personal model/formal authority* combination style appears to suit instructors who are confident as role models and coaches. The learners must be very capable in the course content, able to use their own initiative, and be willing to take

responsibility for accomplishing the tasks that the instructor has designed for the course (Grasha, 1994).

Instructors who use the expert/facilitator/personal style combination typically offer learners experiences that require self-direction and collaboration with others. This combination suits an instructor who is willing to design activities and then supervise learners participating in them. The instructors who adopt this combination also devote time to building interpersonal relationships with and among learners and showing them how to collaborate.

Grasha's (1994) work is based on the leadership theories first developed by Blanchard and Hersey in the late 1960s and 1970s. In a more recent article reviewing those original theories, Blanchard and Hersey (1996) noted that while change is now the rule rather than the exception in most organizations and it is "generally accepted that leadership is done with people, not to people" (p. 2.), the authors believe that their original simple model still holds true. They see leadership now as requiring high levels of both art and skill, but still postulate four basic styles: telling or directing, persuading or coaching, participating or supporting, and delegating. Their current view is that leadership style needs to be based not on the organizational hierarchy, but on the needs of *followers* (*i.e.*, employees). They find a powerful simplicity for leaders in the phrase *ready, willing, and able* as it applies to employees with a task to do.

As Blanchard puts it:

> Generally, "readiness" is the amount of willingness and ability a follower demonstrates while performing a specific task.... The number one error in diagnosing willingness is to view someone who is insecure or apprehensive as unmotivated. Willingness is a combination of varying degrees of confidence, commitment, and motivation.... For example, I may be completely committed to a job, quality, and the organization. I may be motivated to do well. But if I am insecure about my ability to do the job, my insecurity must be addressed before I can move toward full readiness. Someone or something will have to help me over the hurdle.
>
> Ability is determined by the amount of knowledge, experience, and demonstrated skills a follower brings to a task. A diagnosis is based on the actual display of ability. It's important not to select a leadership style based on beliefs about what followers should know. A frequent error is to affect knowledge and then hold followers accountable for skills they haven't had an opportunity to demonstrate. Being task-specific is critical to the success of a correct diagnosis, surpassing the implication that readiness is linear or that it's accomplished in a highly predictable progression.(Blanchard & Hersey, 1996, p. 9)

These thoughts continue to be solid advice for the leader and trainer alike.

Electronic Media and Distance Learning

A brief review of the concepts related to learning through electronic media (*e.g.*, the Internet, video-based instruction, interactive video, or computer-based instruction), is

included here because of the prevalence of those methods in programs and courses directed at students in security, law enforcement, and other career-related fields (See below in the review of certificate and degree programs being offered). Those who are interested in a career will need some post-secondary education, but because they are employed in the field, they will likely be studying part-time and are likely to be enrolled in a program that is self-directed to one degree or another.

Distance education is primarily designed for part-time students who for various reasons cannot attend school on a campus. The very nature of *students* in post-secondary and higher education programs is changing profoundly. According to the U.S. Department of Education (National Center for Education Statistics, 1998, as cited in Christensen, Anakwe, & Kessler, 2001, p. 11), the percentage of 25- to 34-year-olds enrolled as college undergraduates increased by almost one-third between 1972 and 1994. Between 1976 and 1994, the percentage of undergraduates age 35 and older also increased by approximately one-third (Duguet, 1995, as cited in Christensen, Anakwe, & Kessler, 2001, p. 11). Higher education institutions that offer distance education courses are targeting employed people who want to update their skills or training (49% of institutions) and working professionals who want to renew certification in their fields (39% of institutions)(National Center for Education Statistics, 1998, as cited in Christensen, *et al.*, p. 3). Turoff (as cited in Christensen, Anakwe, & Kessler, 2001, p. 11) adds that there will be an increasing percentage of working college students who, because of other obligations, cannot attend school in the traditional way.

Research by Biner and Dean (1998) shows that the distance learning students who performed better had more demands on their time, such as full-time employment. Christensen, Anakwe, and Kessler (2001) also studied the concept of receptivity to distance learning. Their basic hypothesis was that:

> Students with more external responsibilities (e.g., in their work or homes lives) will have a more positive attitude toward distance learning classes. That is these students will have a greater need for flexibility and, thus, will perceive distance learning as better addressing their needs than will students with lower flexibility needs.(p. 3)

Conceptually, receptivity to technology-based distance learning is measured by students' perceptions of its usefulness, their familiarity with the technology, and their access to it (Christensen, et al., 2001). These three factors were positively associated with receptivity to distance learning. The researchers also factored in such elements as cost, quality (based on the reputation of the teachers, the program and the institution, and the type of technology used), and students' need for flexibility because of family responsibilities, work demands, and work schedules. They clustered these factors as *reputation* and *constraints.*

Although research conducted by Christensen, *et al.* (2001) concerned college students (of traditional college age), some of their findings are of value to this research. For example, their study showed that students were more receptive to distance learning when the medium provided interactive *richness*, which was related to "greater feedback,

beneficial small-group learning processes, and more frequent contact with the instructor" (p. 10). The research also confirmed that students who have greater needs for flexibility will be more receptive to distance learning.

There is little evidence in the research literature supporting the ability of technology-based instructional methods to promote learning. Typically, technology-based methods are promoted for their ease of delivery, rather than their ability to provide learners with a learning experience (Neal as cited in Grasha & Yangarber-Hicks, 2000, p. 2). Nor is there any published evidence to date on how learners learn using technology-based methods, although Grasha and Yangarber-Hicks, (2000) suspect that a learner's learning style is a key factor: "Students interested in technology based courses are independent learners who prefer a more abstract way of thinking" (p. 4). However, as has already been noted, adult learners, particularly those employed in the field about which they are learning, are typically not abstract thinkers, but more focused on concrete, readily applied ideas and practices. This does not necessarily mean that the style adult learners prefer is the only factor that provokes their interest or that only learners with certain styles will benefit from technology-based programs. Their motivations are personal, unique, and changeable over time.

Security Education and Training Models

Deming (1989) provides a brief history of security education. In the mid-20th century, fewer than a dozen academic programs existed, mostly criminology programs offered by departments of sociology, and roughly equivalent to a bachelor's degree

program in criminal justice today. They generally attracted people interested in preparing to work in the correctional field, although a few programs were designed for law enforcement. The most notable among the early programs were Michigan State's School of Police Administration and Public Safety and the School of Criminology at the University of California-Berkeley, both of which were established in the 1930s. The number and types of programs available to people working in industrial security have greatly expanded, as described in this section of the review.

Deming (1989) rightly points out that the boundaries of the modern security profession need clearer definition. Part of the problem is that traditionally, "the boundary separating security administration from criminal justice administration has been *private* versus *public*" (p. 17). Deming distinguishes security administration from law enforcement/police administration "using the criteria of emphasis, responsibility, and power of arrest" (p. 19). The emphasis of security administration is on crime prevention (in police/law enforcement, it is on enforcement of laws and apprehension of violators); security management has specific responsibility to a specific organization (police have general responsibility for the public welfare); security administration has no or very limited arrest power (police have full arrest powers). Deming's concern is that the term *private* as appended to *security* has made the discipline a kind of stepchild to professional and academic programs in criminal justice studies.

Nalla, Christian, Morash, and Schram (1995) conclude that typically security management or administration programs have been built onto criminal justice education,

specifically, added to traditional law enforcement curricula. The authors emphasize, however, that it is time to change these traditional models, particularly because of the increasingly global nature of business, with American corporations operating in many other countries, and with foreign corporations operating in the United States. In addition, the authors assert, the demographics of the workplace are changing, as a reflection of the American multicultural society; technologies are rapidly automating many security functions; and security managers are increasingly called on to protect intangible corporate assets.

Nalla, et al. (1995) conducted a survey to determine which topics security managers thought most deserved emphasis in graduate security education. The authors' findings show that practitioners in the field saw an emphatic need for general business and oral and written communications skills at the graduate level. Respondents called for a variety of courses more typically found in a business curriculum:

> ...business skills, with courses such as motivation techniques, negotiation skills, employee training; security/ethics, with courses such as intelligence gathering, privacy issues and ethics, security administration, and operations security; and communications, with courses such as computer preparation, public relations and the media, public speaking, and writing. (Nalla, et al., 11995, p. 95)

Nalla, et al. (1995) interpreted their findings as a call on the part of security professionals to tailor graduate education in their field to the demands of the global markets in which their employers were operating. Their respondents emphasized their need to be

able to communicate with top management, particularly those whose positions involved large staffs and budgets.

Morley, Vogel, and Huegel (1993) also surveyed security professionals about their needs for post-secondary education, including inquiry about preferred methodologies. Their stated purposes were to identify the priorities placed on certain courses by security professionals in terms of their personal and professional development and to describe which educational methodologies were most attractive to them (within certain budgetary and technological parameters). Their sample consisted of members of ASIS in the contiguous United States, about whom certain demographic information was also collected. The survey asked the respondents to rank a list of courses typically found in a general college curriculum according to their importance in the education of security professionals. Most important for this group were courses in management, English, and speech communications. The researchers' results varied widely, but they believe that this in itself is was relevant finding, commenting: "It may be that the field of private security is so diversified, and in such a state of flux, that developing a concise core curriculum is fraught with difficulty". (Morley Vogel and Hugel, 1993 p. 126).

Goodboe (1995), when he was vice president for training at the Wackenhut Training Institute (a major provider of security services and training), advocated the use of adult learning principles (*andragogy*) in the design and implementation of security officer training. The Institute surveyed nearly 600 field security employees to determine which training and education methods they preferred and found that their results were similar to

those in earlier research among both police and industrial security personnel, in characterizing people drawn to law enforcement and security as "traditional and conservative," with a tendency to "hold onto old ways of teaching and learning" (p.2).

Consistent with the conceptual framework of adult learning, the security personnel that Goodboe (1995) surveyed were strongly in favor of training methods that made cause and effect relationships clear, that explained why they were learning certain material, and that described concretely the application of what they were learning to their work. The respondents also approved hands-on learning experiences. While there was some recognition among them "that the traditional 'I'll talk, you listen' lecture method [was] still applicable in some contexts" (p. 2), they were not convinced that it was the most effective training method for security personnel. Five other items unique to Wackenhut's worker population were strongly demonstrated:

> Security employees have a concern for competent instruction; they prefer logical sequencing of subject matter; they are detail oriented; they like to participate in the learning experience; and they have a high need to 'feel' the impact of the training, not just to perceive it (p. 2).

Professional Training

The American Society for Industrial Security (ASIS) is perhaps the best known supplier of training and education outside of the academic institutions, holding annual conferences and symposia and offering online recertification and other courses (*e.g.*, courses on information technology, knowledge management, presentations for senior

management, and ethical issues). The annual ASIS Academic/Practitioner Symposium brings security academicians and field security personnel together "to address the future of security education" (American Society for Industrial Security, 1999, p. 1). At the 1999 symposium, for example, participants examined the relationships among various corporate functional areas in which security has an interest, such as loss prevention, asset protection, risk management, and resource protection. They looked at what security's involvement should be in fire science and protection, disaster recovery, antiterrorism, and emergency management. Finally, they discussed the relationships and interactions among the disciplines of security, law enforcement, and criminal justice administration" (American Society for Inudstrial Security, 1999, p. 1).

Meetings like the 1999 American Society for Industrial Security Academic/Practitioner Symposium are working meetings, in which groups address specific problems and propose practical solutions. For example, one group attempted to differentiate a security degree from a degree in criminal justice and other related fields. They concluded, in this case, that the focus of security programs should be on identifying problems and preventing them, rather than on learning how to react (American Society for Industrial Security, 1999, p. 2).

Joseph W. Koletar, then director of forensic and investigative services for Deloitte and Touche LLP, proposed that a security degree require preparation similar to that required for any other undergraduate liberal arts degree, with these additions: oral and written communication; criminal justice operations; criminal and civil prosecution

procedure; statistics and quantitative methods; business operations and risk management; business economics; marketing; and technical courses such as access control systems or fire and safety (American Society for Industrial Security, 1999, p. 2).

The Proceedings of the 2001 Symposium are a detailed indicator of how the field is developing. In addition, ASIS training programs scheduled throughout the year appear to be based on demand from the organization's membership, and are therefore another indicator of educational priorities among security personnel. For example, American Society for Industrial Education, (2002) *Managing Your Physical Security Program*, scheduled for spring 2002, offered in-depth training for security professionals in maintaining electronic systems, training staff, producing written procedures, handling privacy issues, and dealing with human resource concerns. The topics included: the changing role of the security manager; threat analysis; benchmarking; planning a physical security system for vulnerability reduction; using outside assistance; system maintenance; CCTV systems; contingency planning; legal concerns; safety and security; managing and training a guard force; and selling the physical security program (presumably to top management).

Also scheduled for spring of 2002 were two *Assets Protection* courses, part of a multi-course series. Part II, *Practical Applications,* included sessions on terrorism and executive protection, financial background checks, information technology security, interrogation techniques, drug testing, legal aspects of investigation, communications skills, labor conflicts, and shipping security. Part III, *Functional Management*, covered

communications styles, leadership, time management, strategic planning, and "Selling the Intangible," which included "new methods of internal and external self-promotion and customer service" American Soecity for Industrial Security (*Assets Protection*, 2002, p. 2).

Several privately-owned organizations also offered extensive arrays of training, such as the World Institute for Security Enhancement in Miami, Florida (www.worldinstitute.org), which runs programs in the United States and Europe that offer continuing education units, and Certified Protection Professional (CPP) recertification. The Professional Security Training Network (www.pstn.com) is a subscription video training service offering a variety of video courses with accompanying testing materials. Their *Basic Security Officer Training Series*, for example, consists of a dozen video modules that cover asset protection, physical security and crime prevention, fire protection and life safety, criminal law and liability, two modules on human and public relations, communications, civil law and liability, ethics and professional conduct, report writing, and emergency situations. The contents of these association and private programs are included here because they very likely represent the current training concerns of security professionals, they capture the topics of major current interest, and they are an invaluable resource for the security professional responsible for developing an in-house training program.

John Jay College of Criminal Justice also annually presents a 44-hour Professional Security Management Course, organized around the American Society for Industrial Security examination for the Certified Protection Professional (CPP) credential and

designed to help those seeking the credential to prepare for the examination. The course covers emergency planning, physical security, investigations, protection of sensitive information, legal aspects of security, security management, personnel security, substance abuse, loss prevention, and liaison--the subject areas covered by the examination (*Security Management Institute,* 2002).

Marsh (1991) observes that while supervisors, managers, and directors of security are becoming better educated, their employees have not had the same experience, "due in part to low salaries and the employers' fear that if the officers are provided with better training and increased education they will seek a higher paying job" (p. 180), thus summarizing the Catch-22 dilemma for the security profession. Marsh believes, however, that cooperative corporate/university security education programs "have the potential to professionalize the security industry" (p. 181).

Certification and Professional Standards

The American Society for Industrial Security (ASIS), founded in 1955, formed a task force in 1972 to look at certification based on education, experience, and a written examination (first given in 1977). Membership in ASIS was originally only available in America, but by 1998, chapters in the United Kingdom, Australia, Bahrain, Canada, Singapore, and South Africa had been formed, and there appears to be growing recognition of ASIS certification as a Certified Protection Professional (CPP).

To be eligible for certification an applicant needs at least two years of security management experience, at five different levels in an organization. At the lowest level,

applicants must have been employed full-time in a security or loss prevention position for at least nine years, two of them as a supervisor, or in a position where they have made independent decisions. At the highest level, applicants with a doctoral degree from an accredited university are required to have only four years of experience, two of them in security management (McAinsh, 1999).

The written test for CPP certification is extensive, covering the following subjects in different proportions: security management, 20%; physical security (physical, electronic, and manned security), 16%; loss prevention, 14%; investigations, 14%; liaison, 8%; protection of sensitive information, 7%; personnel security, 7%; emergency planning, 6%; legal aspects, 5%; substance abuse, 3% (McAinsh, 1999, pp. 3-4). Recertification is required every three years.

ASIS itself offers a CPP Review Course online, as mentioned above, which consists of a videotape of the live course presentation, a transcript, self-testing material, and other tools to prepare for the examination (*Professional Development,* n.d.).

Other credentials available to the security professional include two certifications by the International Foundation for Protection Officers (IFPO), the Certified Protection Officer (CPO) credential, and the Certified Security Supervisor (CSS). The ASIS has agreed to give credit toward re-certification for successful completion of the IFPO's CPO, CSS, and Security Supervisor Program courses. In addition, the IFPO offers these programs: Entry-level Protection Officer, Basic Protection Officer, Certified Protection

Officer Instructor, plus an online study guide for the CPO examination, and a variety of professional development courses (www.ifpo.org/programs/programs.html).

One of the indicators that the security discipline is steadily professionalizing is the movement to develop nationally or internationally recognized standards. Simonsen and Nelson (1994) offer the following general test to determine whether an occupation is a profession. A profession, they contend, has these elements:

1. Specific standards and a code of ethics and conduct that govern the actions of the members of that profession;
2. A body of knowledge, professional journals, and a historical perspective that acts as a guide for new members of the profession;
3. A recognized association that provides a forum for the continuing discussion and development of the profession;
4. A certification program that ensures that members of the profession are competent to practice in the field; and
5. An educational discipline that prepares students in the specific functions and philosophies of that profession. (p. 187)

Bondi (1993) cites the parameters that Bottom and Kostanoski used in 1990, as cited in Bondi, 1993): "Full-time status, active practitioner associations, a working code of ethics, licensing and certification, educational resources, a philosophy or theory" (p. 28).

In a survey conducted at the 38th Annual ASIS Seminar and Exhibits in 1992, 69% of the ASIS members attending and 68% of nonmembers felt that national regulations for

security officers were a good idea (Davies, 1997), but there was no consensus over whether the security industry itself or the federal government should set the standards. The states of New York and Oregon have since developed minimum training standards and licensing procedures for security officers. In all, 22 state legislatures have passed regulations governing the training requirements of security officers; 11 others have requirements for armed officers only. The National Association of Security and Investigative Regulators (NASIR), formed in 1993, today represents 33 states and two Canadian provinces. The association's primary purpose is to lobby effectively for state-level training and education regulations, including training requirements, in order "to protect the public and boost the caliber of the security profession without/overburdening licensees, developing enhanced communication with law enforcement, and creating a model law for states to use as a legislative template" (Davies, 1997, pp. 4-5).

The American Society for Industrial Security (ASIS) has published a code of ethics (quoted in Simonsen & Nelson, 1994, p. 189). The landmark *Private Security: Report of the Task Force on Private Security* produced by the federal government in 1976 proposed 76 standards for the profession, covering everything from personnel selection to sanctions and punishments for infractions of standards (p. 190). The *Report* "recommended 32-40 hours of training for armed security guards, but left whole areas of security with little or no standards for training" (p. 190). The recommended minimums that were included in the *Report* were largely ambiguous, as this example shows: "2.4 Private security employers should ensure that training programs are designed, presented, and evaluated in relation to

the job functions to be performed" (*Report of the Task Force on Private Security,* 1976, as quoted in Simonsen & Nelson, 1994, p. 190).

Academic Programs

The American Society for Industrial Security maintains a list of colleges and universities offering various programs leading to degrees or certificates. The range of security education, available in a variety of disciplines, can be bewildering. Typically, security courses are offered within criminal justice programs, such as at the University of Alabama, but some institutions offer a minor, specialization, or concentration. California State University, for example, offers a minor in Security Administration in its BS and MS programs; George Washington University offers a concentration in Security Management or Computer Fraud Investigation in its Master's program; and Michigan State University offers both residential and online specializations in Security Management. Within the Criminal Justice programs, Grand Valley State University (Michigan) and St. Cloud State University (Minnesota) are typical, perhaps, of those institutions offering an emphasis or minor in Private Security. Grand Valley State and Michigan State also have Police Academies on campus.

Security concentrations are also found in four-year degree programs in Justice and Public Safety (*e.g.,* Auburn University-Montgomery, Alabama); Risk Management (*e.g.,* Florida State University; Bradley University, Illinois); and Loss Prevention and Safety (*e.g.,* Eastern Kentucky University). It is possible to get an undergraduate degree in Private Security or Loss Prevention Management at Lewis University (Illinois) and at John Jay

College (New York, where an M.A. in Protection Management is also offered). St. John's University in Louisiana is a distance learning institution, offering Associate, BA, BS, MA, and MS degrees in Security Management and Security Administration.

Among the two-year degrees and certificate programs, Grossmont College (California) maintains a Security Academy and offers a security management emphasis in an Associate of Arts degree in Administration of Justice program, along with certification in the use of firearms and other weapons. A number of community colleges across the country offer associate degrees in such majors as Safety Management Technology (Pikes Peak, Colorado), Safety and Security Technology (Macomb, Michigan), Safety and Security (Truckee Meadows, Nevada), and Security and Loss Prevention (online by Fox Valley Technical, Wisconsin). Mercy College (New York) offers a Certificate in Private Security, as do Indiana State and American Military University (Virginia).

A closer look at the programs available at the institutions committed to education in this area reveals the depth of resources available at some of them. John Jay College of Criminal Justice in New York established its Criminal Justice Center in 1975 "in response to the need for a unit that would serve as a bridge between the academic community and a variety of practitioner requirements" (*Mission*, n.d., p. 1). The Center is the site of the Regional Training Center for the New York/New Jersey High Intensity Drug Trafficking Area and a Northeast Regional Training Facility for the New York Field office of the FBI. In addition, the Center's director is the Technical Assistance Coordinator for the New York State Regional Community Policing Institute, funded by the U.S. Department of Justice.

Finally, the Center is authorized by the New York State Division of Criminal Justice Services to provide Peace Officer Training and as a Security Guard Training School.

The Certificate in Security Management Studies offered by John Jay College is a non-degree undergraduate program requiring 15 hours of study, including required courses in Law for Security Personnel and Introduction to Security (which may be waived based on experience), and three elective courses chosen from among these: The Investigative Function; Security of Computers and Their Data; Methods of Security; Security Management; Emergency Planning; and Seminar in Security Problems (*Certificate*, n.d.).

A review of the curricula in the associate and certificate programs shows that even though offerings differ at individual institutions, most include courses in criminal justice, legal issues, criminal or investigative procedure, sociology, psychology, and written and speech communications, as well as specialized courses in protection of physical property, information, and personnel. A number of institutions have modeled their curricula around the ASIS credentialing examinations.

This literature review identified two articles profiling the process of establishing a private security specialization at a university, Penn State University (Lieb, 1991; Bondi, 1993). Bondi (1993) conducted an 8-year trend analysis of the private security specialization at Penn State University by cross-tabulating the class rosters of the security courses to determine how many of the courses each student completed, and found that most of the students took at least one security course, even though it was not one of the requirements for the Administration of Justice major. An internship, or practicum, is a

requirement, typically lasting 12 weeks, during which the student works 40 hours per week. The inclusion of a practicum is fairly standard across programs, reflecting the experiential nature of the approach, based on adult learning principles.

Security Training Program Content

As the literature on professional and academic education and training cited above shows, there is a rich body of material that can be used to develop the content of security personnel training programs. While the basic subjects reoccur no matter what the context, each program is naturally tailored specifically to the organization in which it will be implemented, which means that the first step in designing a program is to assess the training needs of the security personnel. Training needs can be assessed by reviewing the backgrounds and training of the security employees to be trained, assessing their training history in the organization, and perhaps conducting skill and knowledge testing to determine deficits. Most of the literature reviewed emphasized the following subject categories as being necessary for security training. While no means an exhaustive list of what should be covered in security training, the review of the literature related to these topics provides a snapshot of current thinking among security professionals.

Communications skills.

Millwee (1999) believes that good communication skills are crucial if security professionals are to "sell" other corporate departments on their expertise and willingness to collaborate as an internal consultant. The need for both oral and written communications skills is clear in reviews of the professional training (*e.g.*, ASIS courses) and the academic

curricula. Millwee also suggests that security's professional expertise is needed in interviewing employees, for example, in sexual harassment cases that could lead to legal problems. His contention is that while these interviews are usually conducted by the human resources department, the necessary training and experience may more often by found in the security department.

Emergency response procedures.

Kane (2001) recommends that a comprehensive security training program include individual certification training in CPR, first aid, and possibly automatic external defibrillator (AED) training. The author suggests that, depending on the location and needs of the organization, trainers consider bringing certain security personnel to the EMT or paramedic level. Team training, in which individuals on the security staff learn specific roles in responding to a medical and other emergencies, is also recommended. The role of security in medical emergencies is often supportive, requiring only that an ambulance be summoned, an elevator be isolated, or an escort be provided for outside emergency response workers. Nevertheless, training in these supportive practices is essential if the security department is to fulfill the role effectively.

Hazardous materials management.

Hazmat training, as it is called, is traditionally covered to one degree or another in general fire safety training. However, since the 2001 anthrax threats, corporate security departments are paying more attention to mailrooms and receiving facilities. For instance, a number of companies have sent security officers for training in the use of protective

equipment and x-ray machines in an attempt to manage these vulnerable entry points (Roth, 2001).

Intellectual property theft.

As noted earlier in this review, concern about theft of intellectual property, including computer-based data and information, is growing in the corporate world and the security industry. In a 1997-1998 report, The American Society for Industrial Security (ASIS) reported that United States-based companies could lose more than $250 billion a year through the theft of various categories of intellectual property (*Intellectual,* 1998, p. 1). The kinds of data and information that appear to be particularly vulnerable are those usually referred to as competitive intelligence, such as customer information and plans for marketing and manufacturing. Also targeted are data and information associated with an organization's research and development activities, particularly in the highly competitive pharmaceutical industry. As noted earlier, most modern corporations are populated by a variety of people, not all of whom are full-time employees. Many are visited daily by vendors, suppliers, consultants, and other contract employees, and any could be a theft risk. In addition, former employees of the corporation are considered a high-risk group.

The ASIS survey also reported that formal programs were in place to safeguard sensitive information at only 63% of the Fortune 1000 companies and the Fortune 300 Fastest Growing companies. Of those, only 51% of the companies responding to the survey reported that their programs had been implemented consistently at every employee level in the organization. Interestingly, while most of the respondents rated employee education as

the most important element in theft prevention, they also rated it the least effective method. As a side issue, the survey reported that intellectual property was insured at only 27% of the organizations surveyed (*Intellectual,* 1998).

Executive protection services.

While protection of key executives is an important issue, particularly in multinational corporations, most major corporations choose to outsource these services because they are so specialized. Nevertheless, when a contract service is employed, Nichter (2001) recommends the following comprehensive review and supervision:

1. Check the source of the agents: if they are coming from another agency, it is that much harder to check their credentials, experience, and training.
2. Verify credentials: a reputable agency should be able to provide information about the agent's education, training, and executive protection experience. Proof of background checks. If armed, documentation of firearms training, shooting range practice, and skills tests, specialized training for stun guns, pepper spray, and other non-lethal devices.
3. Examine training: If the agents have completed an in-house program, check to see if it has been accredited or reviewed by an independent agency, such as some states provide. Check the content and methods used: is it all texts and videos and no hands-on.
4. Know the mind-set: The executive protection team should be operating with similar philosophy. "In my experience, graduates of federal programs are pragmatic,

technologically sophisticated, and highly skilled, with a let's-get-the-job-done attitude. They are not intimidated by local law enforcement or other authorities. A civilian agent, on the other hand, is trained to be more cognizant of issues like legality, liability, breaches of contract, cost overruns, and the effect of bad publicity on a client's reputation.

5. Know part-timers: Check the nature of the agent's other employment, even if it is in law enforcement.
6. Assess fitness: Fitness should be tested regularly and documented. Good communication skills are important, as is good judgment, and maturity.
7. Conduct interviews: Conduct personal interviews with the agents to establish compatibility with the client's life on and off the job.
8. Check references:
9. Hold a post-mortem on training exercises. (Nichter, 2001, p. 3)

Nichter is a CPP and ARM (Associate in Risk Management), senior analyst and instructor for The Institute for Strategic Executive Development (Las Vegas, Nevada), and chairman of the ASIS Council on Gaming and Wagering Protection.

While some of these recommendations may seem self-evident, it is characteristic of security professionals to devote this kind of thorough attention to a single issue. Nichter's full recommendations are included here because they represent the wide range of professional security skills that are required for just this one element of a complete corporate security program, and therefore represent a kind of training curriculum.

Workplace violence prevention and response.

This issue has received a great deal of media attention, as well as attention in the corporate and security arenas. Morash, Vitoratos, and O'Connell of Michigan State University (n.d.) reviewed the components of successful workplace violence programs in ten leading companies. They found that the following were critical to the success of these programs:

1. Routine background screening of applicants for employment;
2. A written plan;
3. The active involvement of senior management;
4. The support of employee assistance programs;
5. Formation of a crisis management or emergency response team;
6. A risk assessment team;
7. A written and disseminated process of critical incident review;
8. Services for terminated employees;
9. Positive relationships with local law enforcement agencies;
10. Written and disseminated termination guidelines;
11. A grievance process;
12. Union involvement in planning and response efforts;
13. Communication of information;
14. Working contractual relationships with consultants and outside experts;
15. Regular assessments of the climate in the organization;

16. Regular assessments of security at their facilities;

17. Regular assessments of readiness;

18. Regular assessments of employee or facility risk levels; and

19. Protection for threatened employees.

In terms of training, the best-prepared companies provided training, both for the security staff and for employees in supervisory and managerial positions, as follows: (a) detecting the potential for violence; (b) responding to domestic violence; (c) conflict resolution; (d) cultural diversity; (e) personal safety; (f) dealing with difficult people; (g) effective communication; (h) stress management; (i) diffusing violent situations; and (j) liability issues (Morash, *et al.,n.d.*).

In terms of policies, the companies had a zero tolerance policy regarding threats or violence; a written code of conduct; a written code of sanctions; guidelines to control access of non-employees to facilities; a weapons prohibition; drug/alcohol prohibitions; and sexual harassment prohibitions (Morash, *et al., n.d.)*.

In terms of procedures for reporting and documenting workplace violence, most had a notification process in place for employees to use when they observed potentially violent situations; all had systematic incident reporting procedures; most had a computerized database for incident reporting; all had 24-hour reporting hotlines; and all provided emergency communication equipment for people responding to emergencies (Morash, *et al.*).

Anderson (2002) interviewed security directors at various organizations about their workplace violence plans. At one large research and development organization, for example, the efforts included a standing committee, with members from human resources, security, and operations which develops policy and is responsible for communicating throughout the organization. The other *hand* is an emergency response team, which included members with responsibility for physical security and document control, locksmiths, and contract security personnel. All members receive annual training, including scenario training and practice drills for response team members. Emphasis is on prevention rather than response. In a poll conducted by *Security Management* in connection with Anderson's (2002) article, only 43% of the nearly 30 companies surveyed had a response team in place (p. 6).

From this brief review of the current work that is being done on critical current issues, it should be possible to see where the emphasis is. In addition, the increasingly complex mission of the security department emerges from this material.

Training Methodologies

As noted earlier in this review, training methods are equally as important as training content, particularly when adult learners are being trained. A number of articles have appeared in the literature based on what security training professionals are using to train their personnel. For example, Morley, *et al.* (1993) found that security professionals preferred videotapes as a method of course delivery, followed by interactive computer, correspondence courses, satellite television, and live video conferences (p. 126).

There is general agreement in the professional journals that practical skill development and role-playing are the most effective training methods with adult learners because they are not abstract and are applicable to job tasks, although other methods are also recommended. In the survey conducted by Kaupins (1997), the respondents rated live case studies and internships (or practica) the highest. Quoting one respondent about the reason for preferring *real-life* training methods: "The closer training comes to resembling what a person will be doing on the job, the more participants learn, remember, and use back on the job" (p. 5).

In terms of training program design, Kane (2001) suggests that a security training program should include "objectives, lectures, scenarios, test exercises, individual tests, reviews and refreshers" (p. 1). While this design overview would appear to be heavy on testing and documentation, Kane recommends also recommends outlining objectives for the program and using a *building block* approach "in which individual skills are taught first, followed by team skills" (pp. 1-2), which should then be reinforced with drills and tested by simulated exercises, thus reinforcing the principles of adult learning.

As a result of a survey of nearly 600 security employees of Wackenhut Corporation, a major provider of security services, Goodboe (1995) reports that the Corporation changed most of the traditional lecture style programs at the Corporation's Training Institute. To begin, each lesson plan was accompanied by an overview of adult learning principles, directed at the instructor or facilitator. The lessons themselves were designed to be as interactive as possible, with role-playing and other methodologies integrated into each

lesson and required, along with self-assessment instruments, so that those being trained could evaluate their progress as they mastered each lesson. In addition, Wackenhut redesigned its *train-the-trainer* program. The new program is focused on analyzing learning styles and students' needs, as well as on analyzing teaching styles, so that presentations are more carefully designed and delivered in less traditional ways. Finally, the Corporation developed a program specifically designed to teach adult learners how to learn, "by coming to terms with their own learning preferences, capabilities, and responsibilities" Goodboe (1995). (P. 3).

Goodboe (1995) has a final note of caution for security managers and directors designing and implementing training programs: "There may be a temptation to view concern with training methodology as unwarranted in an industry characterized by high turnover and a fairly transient work force. But security professionals should recognize that quality service is impossible without effective training.... The better the training of the security work force, the better service they will provide, and the more respect the industry will gain" (p. 4).

In terms of methodologies, current thinking in the industry is that the more interactive the medium, the more effective the learning will be. That does not mean, however, that traditional teaching methods have been abandoned entirely. Following is a brief review of the current literature with regard to specific training methodologies.

Lectures.

Kane (2001) notes that the traditional lecture is more suitable to general, routine, or introductory subject matter. Nevertheless, it is vital to keep trainees interested, so Kane recommends incorporating visual elements into lectures, such as slide presentations, videos, and films. Kane even suggests that the lecture format be designed to include discussion beyond a standard question-and-answer period at the end of a lecture. The aim, in keeping with adult learning concepts, is to keep trainees involved in the material in a concrete way.

Role-playing.

Role-playing is favored by nearly every writer on the subject of security training. Kane (2000), for example, prefers this method because it is directly related to the security job at every level, and emphasizes that because security officers need skills in dealing with people, both in their routine interactions and in emergencies, one of the best methods for teaching these skills is role-playing. Kane suggests that these exercises be based on detailed scenarios, that they be designed to be highly realistic, and that they have a direct relationship to both the security officers' daily activities and their responses to emergencies.

For instructors, Kane's (2000) advice is to cast scenarios well, with people capable of performing realistically and adhering to the objectives of the scenario. In addition, post-scenario discussions are the essence of training, since they can provide critical information

about behavior and solutions. As Kane puts it, role-playing "allows the human dimension to be introduced into training in a way that other methods do not" (p. 5).

Scenarios.

Case studies of past incidents or situations, or *hypothetical* scenarios also drawn from real situations are highly effective methods of training security officers. Kane (2000) suggests that security managers developing training scenarios can find ideas in their own incident reports, professional journals and magazines, or even newspapers. The cases or scenarios selected should be as close to the actual experience of the security staff in the particular environment in which they operate. Hypothetical scenarios, based on real situations, should be realistic and designed with various options in terms of their details, such as the level of the threat or the outcome of the events so that trainees have the opportunity to role-play the ways in which they would handle each situation. Kane cautions that not all scenarios need to be full-blown disasters; rather, effective scenarios should include problems that security officers deal with on a daily basis, such as controlling access to a building or dealing with a difficult visitor.

Internet-supported/distance learning.

Although this topic has been discussed earlier in this review, the use of technology-based learning is an increasingly popular methodology for training. Charles Thibodeau, M.Ed., CPP, CSS, a security management instructor in an Applied Sciences (AAS) degree program in security management at Pine Valley Technical College, Pine Valley MN, predicts that technical advances and decreasing costs have made both audio and video

available to the average computer user. Security officer and security management education, he believes, will follow this trend and "provide high-caliber, low-cost, two-way interactive training from whatever computer location the student chooses" (Davies, 1997, p. 2).

Summary

The recent literature on security training is not plentiful, nor is it comprehensive. With only one peer-reviewed American journal in the field (*i.e., Security Journal*), and one widely read magazine (*i.e., Security Management*), both published by the largest professional organization, the American Society for Industrial Security, the choices for security professionals with a serious interest in their field are limited.

Even with these sources, and others dealing with narrow security-related issues, such as loss prevention, life safety, information security, there is a dearth of material in the periodical literature about training security personnel. All of the contract service companies attempting to sell their personnel and services to large corporations use the word *training*, as do all security managers, but there is surprisingly little written about training needs and the best ways to meet them.

The demographics of the lowest levels of security force employment—their lack of formal education, their willingness to accept low wages, their high rate of turnover—might explain why corporations want to spend as little of their resources as possible on training these individuals. In addition, the *culture* of the security business, with its vaguely military, police-like traditions and structure, may also explain why some assumptions are made about the quality of training among security officers. Neither of these concepts entirely explains why corporate top management apparently does not see what return is to be gained from investing in training security personnel.

As noted in this review, there is a continuing emphasis in the anecdotal and professional literature on the need for managers and directors to *connect* with top management, to develop *selling* skills, to improve their communication skills, and to claim functions and processes as rightfully belonging to security rather than to other functional departments in the corporation. What this preponderance of material suggests is that the profession is currently at a crossroads in terms of its development *as* a profession. Certain indicators are on the rise: the number of security professionals seeking nationally-recognized certification; the number enrolled in baccalaureate and master's level academic programs; and the proliferation of conferences, symposia, and other training events. It seems likely that with the growing number of resources available to security personnel to improve their image, their education, their skills, and their importance to their employers, the security profession is moving toward recognition in the corporate world.

CHAPTER III

Research Design and Methodology

Overview

This chapter describes the research design of the study, the subjects involved, the instrument used, the manner of data collection and, the treatment of the data.

Research Design

The purpose of this phenomenological study was to investigate the elements of a successful training model for security personnel as perceived by global heads of corporate security working in the Ethical Pharmaceutical industry. According to Leedy & Ormrod (2001), the phenomenological study approach is used to "understand people's perceptions, perspectives and understandings of a particular situation" (p.153). It allows the researcher to "look at multiple perspectives in the same situation and then make some generalization of what something is like from an insider's perspective" (Leedy & Ormrod, 2001, p. 153).

This *inside perspective*, has been largely ignored in the literature to date and will hopefully aid in the contribution to better training programs designed for security personnel working in the pharmaceutical industry. The importance of having properly trained security personnel cannot be overemphasized. The United States is at a time when almost every individual is eager to be provided the best possible security, whether it is technical or personal in nature.

Subjects

The subjects in this study, also referred to as respondents, are adult males serving as global heads of corporate security in the top ten companies within the ethical pharmaceutical industry with global corporate security organizations. Demographic data revealed that all are white males ranging in age from their early 40s to their early 60s. The level of education ranged from bachelor's degree to master's degree and all had at least 20 years of supervisory experience. It should be noted that in conformance with Seton Hall University's Institutional Review Board (IRB) guidelines mandating that the researcher protect the confidentiality and anonymity of the respondents, no individual profiles are presented. Furthermore, the investigator completed the *Human Participants' Protection Education for Research Teams* online course, sponsored by the National Institutes of Health (see Appendix A).

The determination of the top ten ethical pharmaceutical companies for this study was based on a ranking of the market value of each company as compiled by Health Ace, Inc. (August, 2003), a private entity that collects and compiles such information. It should be noted that one company in HealthAce's top ten listing did not have a global security organization and the 11th ranked company was moved into that position for the purpose of this study.

Ten individuals were solicited to participate in the study. Nine respondents out of the ten agreed to participate.

Instrumentation

Each participant signed a consent form, as directed by Seton Hall University's Institutional Review Board (IRB) (See Appendix C). This consent form detailed participants' voluntary consent to participate in the study; additional rights afforded to them, and consent for interviews to be tape recorded. A letter of solicitation (See Appendix B) was included with the consent form. A Sony Microcassette Recorder M-629V, utilizing Maxell MC 60 microcassettes, was used for all interviews. Study participants were asked the same seven open-ended questions. "The standardized open-ended interview consists of a set of questions carefully worded and arranged for the purpose of taking each respondent through the same sequence and asking each respondent the same questions with essentially the same words" (Patton, 1990,

p. 198). The tape recorded sessions allowed for verbatim answers to each of the open-ended questions. The seven questions asked of each participant were:

1. What is your definition of successful security training?
2. What do you perceive to be the ideal best practices for a global corporate security training program?
3. What impact does budget have on training security personnel?
4. How does the placement of training within the organization effect training security personnel?
5. What do you perceive to be barriers to setting up training for security personnel?
6. What practices are ineffective in setting up successfully run security departments?

7. How does the training of security personnel for the ethical pharmaceutical industry differ from the training of other security personnel?

It should be noted that two questions approved for use by the IRB were omitted by the researcher prior to the interview with Respondent One. The two questions reported below were omitted due to the researcher's belief that these questions were captured in the other questions and therefore should be removed. Omitted questions:

1. From your perception, what are the elements of a successful training model to optimize the training of security personnel?
2. How does the placement of training within the organization effect training security personnel?

Data Collection

The investigator collected data for this research from two sources. These sources were the responses to the seven open-ended questions asked of each participant and the Demographic Survey Form (see Appendix D). The researcher was the only person who collected these data and the only one to evaluate it. Per IRB guidelines, confidentiality and anonymity were promised to each participant and were afforded to each. Prior to the interview process, each respondent was provided a packet containing the Letter of Solicitation, Demographic Survey Form, and Consent Form, all of which were completed by the respondents before their interviews. Interviews were conducted either in person or by telephone, depending on the participant's preference. The interviews ranged in length from thirty minutes to one hour.

In addition to the seven open-ended questions, the short Demographic Survey Form for participants was used. The form asked for respondents' age, race, experience, supervisory years, and level of education.

Treatment of the Data

The data obtained will be kept in locked safes in the researcher's office. The data consist of all materials related to the study and obtained during interviews with participants, i.e., signed consent forms, audio tapes, demographic forms, notes, and written transcripts of taped interviews.

Data were analyzed following guidance offered by Leedy & Ormrod (2001).

1. Identify statements that relate to the topic.
2. Group statements into "meaning units".
3. Seek divergent perspectives.
4. Construct a composite.

Patton (1990) advises, " If a standard, open-ended interview is used, it is fairly easy to do cross-case or cross-interview analysis for each question in the interview. With the interview guide approach, answers from different people can be grouped by topics from the guide, but the relevant data won't be found in the same place in each interview" (p. 376). A "Key Elements Matrix" containing key words or phrases obtained from the Respondents interviews will appear in Appendix E.

After reviewing and reporting the responses in Chapter IV, a summary and interpretation of the data are presented in Chapter V.

CHAPTER IV

Findings

Introduction

Chapter 4 contains the results obtained from interview sessions with nine individuals who offered various perspectives on the issue of elements of a successful training model for security personnel working in the ethical pharmaceutical industry in response to the question: What are the elements of a successful training model, as perceived by global corporate security heads working in the ethical pharmaceutical industry?

The respondents were chosen based upon their heading a global security organization within the pharmaceutical industry with the added criteria that the company is ranked as one of the top ten companies with a global security organization. One company in HealthAces, Inc's actual top ten listing was identified as not having a global security organization. Thus, the 11th ranked company was moved up to the number ten spot.

Of the ten individuals solicited to participate, nine voluntarily agreed to offer their perspectives on the issue of security training. The respondents ranged in educational experience from bachelor's degrees to master's degrees and all had over 20 years experience as managers. All respondents were white males ranging in the age from their early 40s to their early 60s.

The investigator has withheld the identities and places of employment of study participants so that the reader might form a more objective analysis of the responses.

The format used for reporting the interview sessions is as follows: Each question is presented, followed by each respondent's answer to that question. All seven questions and the responses are reported similarly. A "Key Elements Matrix" containing key words or phrases obtained from the Respondents interviews will appear in Appendix E.

Interview Sessions

Question One: What is your definition of successful security training?

Respondent One:

Boy, that's uh… Cause we don't have any. That's our problem. Because we're mainly an investigative unit. Um, oh boy. We don't have a training program. This is a very, very decentralized company and any training that the people that work for me get, or that I get, is either practical, on the job, or its by attending various seminars put on by various organizations such as OSAC or ISMA. ISMA is the one that you get the most to take away from; you get this twice a year. It's your peers. It's pretty high-level stuff that they present. Negotiations, how to position yourself in the corporation from a business stand point, how to fight for budgets. I don't have IT security but there are lots of presentations on that issue. They even have a follow on after the regular meeting they may have an extra day that is strictly on IT issues. We do not have a formal training program for the security folks that work for me…Yes, I'm having a little dispute with ISMA, I just got off of three years on the board with ISMA, and my position in the last several months is the organization has become too academic that the people who are organizing the programs, most are

volunteers, have tended to go the academic route. They bring in a Harvard professor or a Georgetown professor and it's more like a business course. There are some pluses to that, you certainly need to run your organization like a business, you have a budget, you have competing interests that you have to prioritize, so there is some benefit to those programs. But, the bottom line is still you can't survive in a major corporation like yours and mine unless you deliver day to day some type of product. You have to deliver the goods. I mean, that's the way it is and we can be academic as we want to be and talk about being CSOs and all that crap. It's not a reality in my company. There will never be a CSO in this company because the CEOs in this company are committee members, the 11 people who run this company, and the security, will never be that important a function in my company that it would rise to the level of CFO, CIO, COO. That's just not practical. Obviously, it has affected us to some extent, but not my group that much. We're doing a lot more on the physical security side. But training, my guys were all law enforcement professionals who had previous careers. They've either been police officers, one of them was a marine combat veteran sergeant who started from the ground up in security and worked his way up to director. The other ones all have law enforcement backgrounds and we do investigations, that's what my group does. We don't run guard forces, we do active consulting, access controls, etc. From time to time, they go to various training sessions with ASIS, ISMA, OLSAC or some other group, Narcotics Investigators, whatever that National Association is that one of my guys goes too regularly. The PDMA area, that's the training, at will, their choice or my recommendation that they attend. If there's a particular area that I think we

should get involved in, relatively new to us, I might suggest that somebody go to that. Now, in the company, there is a learning consortium within the company and they offer two or three hundred courses that any of my people can take part in. There are tons of courses, you name it, how to manage diversity, hiring skills, problem employee skills, all the usual range that a college or something would offer. In the ten years that I've been here, my guys have not taken one course. They have no interest in taking one course because they are too busy handling their cases, handling their issues whether it's diversion or counterfeiting or workplace violence or the HR issues, which are probably about 60% of the cases we handle. Whether it's terminations or investigations of sales people, they're our lifeblood, sales people, thank God. That's what this company demands of us. They are not looking for empire builders. Its relationships, developing relationships and solving problems for people. So anyways, the bottom line is we don't have a formal training program; my people can take advantage of learning consortium if they want to. I can direct them that way, I haven't because they haven't seen anything over there that they haven't, that they can't do on their own. I have, people that are particularly adept at interviews and information gathering. I have people that are very good on projects and I have people that are very good on big schemes like anti-diversion schemes or setting up counterfeiting task forces around the world. That's what they do. If they take two or three days off, now I've had one of my guys go to a course, and this one here is relatively valuable, it's an ISMA sponsored course, leadership course, put on by Georgetown University. ISMA members can nominate attendees at the courses, I think they're in their third one now, it's a year-long

course. It's going to be someone that has a future in security, this is the kind of thing I think you're looking for, you have to identify a candidate who would possibly succeed you or be in a position to be promoted within the security profession. As a matter of fact, it's a practical thing that we will hopefully use sometime down the road when we want to get regional people here. When the financial picture turns around a little bit. So that is the one valuable course and that's something that beneficial. I think ISMA's going to set one up with Northwestern. I think they are working at that. That's a business school at Northwestern that's interested in doing that type of a course for future security leaders. That I can see is beneficial when the key people that want to move up. That one I would support. But, other than that, these people were practical hands on people and are beyond, they certainly can learn things but they are beyond going to training courses other than the one described.

Within ISMA, there's definitely a division. There are people who think we need to be business leaders at the table and compete with the marketing people and the sales people and the... I just don't think that's a practical solution. We're not going to be at that level. You know, we aren't going to be going out and we're not going to have a forecast that we have to meet every year. We're not going to compete to be a billion dollar profit maker for the company each year. But, we still have to be business people, we impact the business function and certainly you have to be able to work with the budget people and the marketing people to get your share of the budget so you can function and save the company money and protect its people.

My big issue is that the company is here to make money. Obviously to do it in a very ethical way and our perception, and from the complaints that come to us, diversion is a big issue; being a health care services company, is the area where we are getting gored the most. I think I've been able to convince these companies, when they're making lots of money they don't give a sh** but now when things are tight, they realize, my God, you're right, we're losing 50-60 million dollars a year here. That's stuff that we can take care of. We can't eliminate it but we can reduce it. That's been my mantra, as far as the company says hey; you've done a great job for us. That's why I've pushed my guys into the diversion area.

Respondent two:

Well, there are three elements. One, a set of skills and facts; two, an ability to conduct a leadership; and three a team building that comes from having trained within the same system with the same people.

Respondent three:

Well, let's see. You know, first of all, I include both my proprietary officers and the contract officers as part of my total security program. So, it's absolutely important that when you talk about training and you talk about expertise performance, the like, that all those people are included. Because everybody has to understand their job, know what the expectations are in order to be performing in order to have a complete security program. That's the way I feel about it. Now, that said, there are differentiations between the types of training. The proprietary group is more at the higher level from the standpoint of it's, they

have more management responsibility; they have more responsibility for the overall day-to-day responsibilities and reporting up to me. Where the contract organization has responsibilities for primarily physical security, physical security functions and reporting up through the site organization, up to me. So, their responsibilities are focused towards physical security, very specific, very spelled out post orders that we participated in developing so that they, given an individual post, they know what the responsibilities are and the expectations are of them to perform on that particular post. So all that requires training on all those different elements. You have post assignments for the security officers and they need to be trained on those, they need to be trained on customer service, they need to be trained on the customer service area how to deal with staff, how to deal with executives, how to make a professional appearance because big part of that, why I include them into my overall security program is here at this site, for example, we have about 110 of those security officers and the employees see security officers a lot more than they see us. Cause there's a lot more; cause there's only 15 of us. So however they perceive those security officers that's potentially how they perceive us. If they're walking around in a disheveled type of a uniform or have a poor attitude or they're not service conscious or whatever, then that's a reflection on our whole program. So, training has to be an integral part of the whole program. It has to include both contractor and proprietary. And, it gets down to the day-to-day activities of both the proprietary and security personnel to be able to perform appropriately and to be able to provide a quality service to all of our clients which is all of our staff. Training has always been a focus of mine, in order to have a

quality security program. You absolutely have to have it. And there's a couple key things when you're talking about, when you include the contract group of basically bringing them up to the level that you need them to be so that the overall perception of the security organization is one of credibility, professionalism, and so on. And that is they have to have customer service mentality. They have to understand that they are here to provide a service and they have to deal appropriately with staff.

Respondent four:

Well, I think the short definition is one that leads to continual professional development of staff and that development underscores the skills necessary to support the broader enterprise. I think for what we're talking about are corporate or global security organizations and I think I will limit my view to that group because in our organizational model, site security organizations functionally report to us on the dotted line but are embedded within their respective sites which personally I think is the right model. I'm thinking, I guess a bit bigger picture. Not that I'm minimizing what the site security organizations do because they have a very important role. There's a lot of high quality people there whether they're proprietary or contracted but I'm thinking at the more strategic level for the people of my organization.

Respondent five:

A training program which exposes a high potential experienced individual to the business issues and the business problems of a particular company and industry in which you work. So that he can apply his designed, investigative law enforcement and intelligence experience to the business issues of the day. I assume that you didn't just find a mope off the street. And, decided to make him a security expert that you've recruited a person who has high potential and experience and you bring him along if you will. Generally would have previous law enforcement, investigative and intelligence experience and then you bring, you know, that's like when you see some of the guys fail because then they, they come in with that and they don't manipulate, massage, stretch, shrink all that to become, to apply. You not only have to have that experience but you have to have the ability to apply and the common sense to apply to the issues you are facing. Some people can't make that transition so the training would help make that transition where your experience becomes a value added asset and not a detriment. Because in some cases it becomes a detriment.

Guard, locks, alarms are a necessary part of the security program. But, they're not necessarily part of the corporate security program.

Respondent six:

I mean, in my opinion, security is a very broad, it's a very broad profession and what's appropriate for some players of security, training is inadequate in others. I mean, there's the level of training and type of training that you need for guard force that's

responsible for access control in a building in Manhattan and there's security training for the investigators that you need to conduct intellectual property investigations in Eastern Europe. Without writing off the question, I think appropriate security training is the full range of training that's necessary to accomplish whatever objective you have. It's a resource like guns, barriers.

Look, we've got a complex that's got 7 or 8,000 people a day coming in and out. We've got fire safety people who report to security. They have to be up on the fire safety codes, they have to know all of the intricacies of building egress in emergencies, crisis management plans, etc. We employ contract guard force that's responsible for responding to incidents here. They need a certain level of training. We have people that manage them that need a higher level of training. We've got a supply chain that has literally billions of dollars for the product moving from one site to another everyday and we conduct physical security surveys at both sites. We have to have people that know about physical security, about closed circuit television, about alarm systems, about various theft responses, procedures. We've got product that people counterfeit and the people that are involved in security there have to know a good deal about patents, they have to know a good deal about computer technology, they have to know a good deal about complex international investigations so you know, there's a continuum there from pretty basic stuff to very sophisticated stuff and we try to recruit people that have good law enforcement/security and investigation backgrounds and even then we wind up having to afford some training.

So you know, I think it's the responsibility of each line manager to determine what level of training is responsible for the people that report to him and ensure that they get it.

Respondent seven:

Ah. Well it's results-oriented, which in my mind means retention is probably the biggest element of success. It's retention on the part of the individual that's actually receiving the training. It also depends on what type of, whom you're training, and what your goals are for them. Whether it's a security officer, could be you have certain regulatory requirements, you may have standards within your organization that supercedes the regulatory requirements for that officer. You have employees and just general security training that you want to provide to them, be it an orientation or service training, you have management security training, so there's a variety when you talk about training there's a different audience. Retention. Retention to me is the most critical piece because I've just seen too many training experiences from people where you could never accomplish the end result. One of the... So often it doesn't happen depending upon the median and the way you test them, test through retention.

Respondent eight:

To communicate the message on security that will help shape the culture within the organization. Convey policy, procedures, standards, to the workforce. To enable a greater understanding and awareness of the risks and threats to our people, assets, and reputation.

Respondent nine:

Good question. Probably realizing that the outcome, I'm stepping back into my old role cause I'm working products now but, I would say basically an evaluation of status quo are we adequately addressing the issues that we've prioritized and stated to the guard force and others for physical security. I mean that would be the measurement I would use. It's a two-fold process. One is you have to honor or feel good about what you're implementing and what you're emphasizing. And the other is, has the message come through into effective action and I was a big believer in self-auditing. When I had the old job, we do that about monthly. How are we doing in relationship to the number of calls we get? How many people are on hold, you know things like that? Are we really responding in a timely fashion? But I believe you know you have to have assessments based on self audits probably is another way of stating that. And then I would feel comfortable that we weren't missing the mark or making the targets that we initially proposed. So I think it's a two-pronged approach. One is audit of the performance the other is making sure that the instructions are clear and properly given.

Question two: From your perception, what are the elements of a successful training model to optimize the training of security personnel?

Question omitted prior to interview.

Question three: What do you perceive to be the ideal best practices for a global corporate security training program?

Respondent one:

Best practices, there's the regional model as far as I'm concerned. You know, we don't have that. I aspire to that but we've never been able to pull it off. I couldn't even get a guy in Puerto Rico. But, I do think the best model is that you have the three regions on a day-to-day basis and then you have people back in corporate who oversee that but you give them a lot of lead way to service their customers. You give them very basic guidelines. This is a company that abhors policies. We are just not a policy-driven company. Our view is you write a policy generally because of some f***up. That's where policies come from. We have a manual that's five volumes written up. Thou shall not write. After every screw up, there's a policy issue. Well, the next screw up or close to it never quite meets the criteria of that policy. It's sitting there written in stone, you've issued that policy, the next event skirts that policy somehow so you expand the policy and then you expand it again. Then, the next thing you know, you've written these policies you do your business some other way cause you have to do business and someone comes back and sues you cause you didn't follow the written policy of your company. And, it's all discoverable now. So our general counsel just says, you know, I have no problem with guidelines of certain areas where you have to have basic policies like carrying guns on the premises, cell phone cameras, and I have no problems with those individual policies but broad policies we do not issue guidelines. That's our best practices by avoiding rigid policies; we prefer to go with guidelines. But the best practices for global security group I think is the regional model.

Respondent two:

Well, I think the value of a team trained in one system of methodology does a lot more than just provide a skill set. You end up with a bunch of guys which you could benchmark as skills, they trust each other cause they know they've all been trained to respond in the same way. So there's a whole piece that has nothing to do really with the individual skill set, it has to do with the overall functioning of the team. Successful means that it's relevant, it's cost effective, boy that is a big issue cause that's why mostly we don't get any, and it builds this team as universal.

Respondent three:

Very high on the list are security officer training programs. You know, when you relate it to what they have to understand as part of their responsibility, wherever they're assigned, whatever their post, patrol whatever they're assigned to do, they need to understand what's expected of them. Very important. Because, I found over the years that you have security officers, if they don't know what's expected of them, they have a very low level of confidence. They have a very low level of confidence in themselves and what they are doing. They tend to basically be disgruntled because everybody's always coming down on them and they don't know why. Because they're not doing what somebody expects so they're getting, they're getting disciplined or whatever but nobody is really taking the time to tell them what the expectations are. When you do that, when you turn that around and you train these officers and you train them to what your expectations are and what you want them to do regardless of what the post is and specific to the post, they

have a much higher level of confidence, they walk around with their chin up, they're more responsive, they're more prepared to answer questions that our clients or staff pose to them because they understand what they are supposed to do. I think it's very important. That's why training is so important to me. It's so important that they provide that professional credible image. But at the level of the security officer though, you can really see it in the self-confidence, whenever they know what's expected of them, they know what to do on their post vs. somebody that's just thrown out there and expected to get on, on their own.

Respondent four:

Well, I think the first one is understanding the business that you as a professional are supporting. And let me give you a couple of examples to make that point. I have three folks in my group who are highly technical when it comes to the corporate computing environment. I think it's, they are necessarily focused in that area although not exclusively and so because in particular, in the case of one of these individuals he's the primary liaison with our information services organizations and he has achieved and training dollars were provided to the tune of about $30,000 to enable him to get his CISSP and, if you're not familiar with the certification it's a Certified Information Security Systems Professional. That is probably the latest and hottest certification because it really crosses over between traditional corporate security and information security. It is rendered by; I don't have that off the top of my head. It is a body that really comes out of the information security professional domain more than the corporate security professional domain. Not an organization like ASIS or CFE, this is a separate organization that is more tied to the

information security area. So, the training there then has enabled that individual and I've got two others who are pursuing that as well to be able to support that line of business, to be able to meet the needs of this organization from the standpoint of investigation, computer forensics are used more and more commonly in our investigations and so as a result, it's very important to have people on your staff that have that skill set. So that's one example. You know, language skills could be another one. Where it's important that you have people with the diversity of language to be able to effectively do their jobs and function in their respective regions whether it be Latin America, Asia Pacific or Europe, outside of North America. A third example would be the regulatory investigative work that we have to do and all pharmaceutical companies have to do that sell market products related to product samples and it's the prescription drug marketing act and it's very important because our people do, my staff does, about 300 regulatory investigations a year. It is very important for them to constantly be trained by legal staff on the details of the prescription drugs marketing act. And so, it goes back to what I said originally that I think you know, first you have to understand your business, and different people are supporting different segments of the business or different geographic regions of the business and it's very important for them to receive the training to make them top flight professionals to fit in to the business model that they're supporting.

Respondent five:

Best practices would be to have a lot of formalized programs during which a security professional has the opportunity to become a businessman. So that the wealth of experience that he has on the security side can be blended with new-found business to obtain the best results for the company

But to me, a security guy who just silos himself into security issues is not adding much value to the company. I think all security people need to become business people who happen to be doing security. Best practices? In our industry, we're talking about the pharmaceutical industry, there needs to be an opportunity in the training program for people to gain international experience and not be locked in. In our instance, you know with doing the business in 142 countries, we don't need a lot of people who just know how it's done in one country. The last would be as part of the training to instill not only the ability but also the desire to work as a team across the globe. Bringing together Europeans, Americans, Asians, Hispanics together, Africans and so forth towards a common security goal which is to protect the assets, you know globally. Well right. But, most of the issues and problems cross jurisdictional cross borders. Like right now, we've got XXX and XXX working on possible counterfeit XXX out of Chile. So, those people need to, you know, have relationships with one another, be supportive of one another, be enthusiastic about working with one another. And, that isn't a specific training course so much as it is indoctrination into the culture that you're trying to establish within the security department. That is cultural support and sharing.

Respondent six:

Best practices entail management and leadership like I just said, knowing every aspect of their responsibilities and both physical and personal and technical and insuring that the people that report to them get the training that they need. It's a very, best practices means in my opinion, knowing the training that's required and making sure the people get it. I feel like I'm not being very helpful to you but you know, look its one thing to train somebody on how to sell pharmaceuticals. We have a training class out at our training center that lasts for months and months and months and we try to train pharmaceutical sales reps in just about every aspect of selling the product. But you don't have a basic security training course cause there's so many different components. So many different elements of security. The training that we give the people that monitor our closed circuit television and handle our incident response things varies dramatically from the training we give other people. So, I think you have to tailor the training to the roles and responsibilities of the position. Look. You know. If you're, you know, if you're involved in, you just picked a good one. Counter terrorism training, September 11th. You know, you're going to give a certain kind of training and a certain amount of training to the TSA passenger screeners that people go through at the airports. Related to the counter terrorism effort is the global intelligence collection effort that might require that you have somebody that's trained in various foreign languages who's trained in technical software used to help analyze incidents and that sort of thing. So again, it's all like security training. It's all

counter terrorism training but it's a pretty broad spectrum and you know you don't train the intelligence analyst to screen passengers and vice versa.

Respondent seven:

It has to be again, you have to start by really understanding the scope of what you're trying, there's a couple pieces to it. One is scope. You have to know who it is you want to train. What you want to train them on. How you want to train them. When you want to train them. You really have a real specific plan that's laid out. The second is the platform. What platform are you willing to use to get this information? Number one to get the information to the people. And then secondly to ensure that they retain the information so those are critical factors. When I look at them.

Respondent eight:

In my experience, the best way to convey a message is through direct presentation with a human being delivering the message in the classroom. And using educational tools such as software, interactive software, breakout groups, engaging the class in projects. Requiring the group to solve a problem and explore the issue themselves in depth with guidance from the tutor. To me that's the optimum but it's not always deliverable because of time resources and geography. The next best thing in my experience is the use of systems, Internet, Internet, electronic gadgets with structured questionnaires followed by electronic presentations.

Respondent nine:

I would have to say that in the 21 years I've been doing this, the most effective feedback that I've received has been from networking in the industry with other security directors. And through that networking, coming up with best practices comparing those best practices with our own program, knowing full well that every company has a little different exposure and profile based on geographic location. I think the geographic location is a big factor. Culture of the company is another big factor. Some companies are, tolerate more security and some companies want less. And how do you meet your goals and objectives based on the culture of the company with the framework of best practices from the other companies? I've benchmarked a lot. Now, some times a company may change as their culture may change or our culture may change. Wherein I don't have a lot of agreement sometimes is when I deal with major city companies, New York, Chicago, New Jersey who have unique things do to their physical location. Some of which have very high security some of which have minimum security. Our standard here is pretty much the same for all our sites. But I can certainly understand why you would have varying degrees of security if I were in the east coast. Right. I think comparative analysis is critical to come up with best practices for the individual company. You can't, I mean it's not something that just sits there and you just pick it up. You have to work at it. And you have to compare cities, companies, cultures. I think it all sounds good but when you get into practical; for instance, it took me forever to get turn styles in here. I mean the thought of a turn style for access was just abhorrent to the largely academic culture. And only after I was able to

benchmark get photographs and to get some very nice turn styles in here did they accept it. Now it's just an accepted practice. But it was like pulling teeth. Just the fact of wearing badges on campus took me 11 years to get accomplished. It was 11 years of effort. Even knowing that benchmarking indicated that others were already there, I had to make a good business case and basically wait till some people retired to tell you the truth.

Question Four: What impact does budget have on training security personnel?

Respondent one:

In my case, there is very little because we just don't deal a great deal with training, but it is a big issue.

I think I have one line in my budget that pays for training courses if they chose. Even our learning consumptions in the company, if we choose to participate, it costs. They charge back. Everything in the company is charge back. I'm charge back.

Kind of a weird system. We don't do it internationally, but it comes out of the same pie. We don't charge back for individual investigations cause that's a way to report problems. That's it. I have a small training budget that I can allot for courses and seminars and things that people want to go to, that's it, and that works for us.

Respondent two:

On guard force training, it's monumental. Because your guard force hours are so tightly impacted. You could have a guy off post and in training or extra hours I mean, it has a very, very strong impact. I don't have to, the kind of individualized training that I like to do with my guys, where I'll send them off to a weekend in Chester to the driving school or

a send a guy to Reid. For some reason that number isn't so bad. Probably because the kind of guys who get that kind of training aren't very, very many.

Well it's the first thing to go. It's the first thing that gets cut is training. At a great cost.

We have here, for instance, I mean I don't know, a global leadership program but, it's an amazing improvement in the whole company. But the improvement isn't so much in people's skill set, I hate to keep going back, beating on this, but the team building and the sense that everybody's reading from the same page, reading from the same book. And, the company's expectation is reinforced in a very common way because when everybody's sitting in the same room and they're told look, yes results are absolutely critical, but what is not a good result is to get the head to step on your employee's moral so badly that, that everybody has to quit.

Which is something that we have here a lot. Used to be there was a whole culture in one of our areas that pissing on people was part of the game.

Respondent three: Well I think it needs to be factored in. It's big. You know if it's a key priority for you, which it should be, then obviously it needs to be factored into the total cost. You can't hide the total cost of security. It's a big number but training is certainly not the first thing you eliminate when you start cutting back a little bit because you know somebody says you have to bring your budget down a few percentage points. The training has to be in there. It's not something that's cut.

It's difficult, it's somewhat difficult to do because either you have to pay overtime for them to train or else you train them on the job and then you don't have somebody out there doing the job. You have to find time for them to do the training if you want them to do it on their particular shift. It's not an easy thing to schedule. It's one of the reasons why, and here's another, going back to the other question that we don't do and I think it's a problem. That is for years and years and years security companies have always abdicated career pathing and all that kind of stuff so you know if you have an outstanding security officer, bring that security officer up the chain in your organization and you know move a patrol officer to a dispatcher to a supervisor, I don't buy that. I don't buy that from a standpoint of you can't move them, you can move them from a patrol officer to a dispatcher but once it gets to the supervisory level, as far as I'm concerned the company needs to move them to another company to make them a supervisor. Because number one, their one of the guys and they're not going to supervise those people unless it's a very outstanding one officer situation that you have with an individual. But I haven't had very good success in that at all and as a result, we bring in, when we want a supervisor or a manager, we bring in managers from the outside. I think that's a fallacy, I think that's a problem because then you have this collusion, you have this you know this, one is protecting the other because they're buddies, they've been here for five years and you know they grew up together and so on and so forth. We've got to get that out of the security business cause it's killing us.

They don't tell you when somebody's out there stealing and you know, all this other stuff goes on. They're protecting each other and that's a, as far as I'm concerned, that is a perception that people have of the security industry and I think it's true. So you have to eliminate that by brining in people and know how to manage and know how to supervise these shifts.

Well, I definitely want a company to do that. OK? But, you know, my responsibility to my company is to provide quality service.

Not to provide a career, not to satisfy the career ambitions of a security guard officer that comes to work and happens to be working here for now. That's not my problem. I hate to be very adamant about it but that's not my problem. My, that's my issue obviously with my people. But that's not the issue with the contract people and I don't let that happen anymore.

Yes, you know there's different levels, I'm sure you and the ten people you're talking to. You're going to see different levels of the expectation of the level of security or the type of security they want at their facility. There's a lot of security managers, a lot of security directors out there that are very interested in basically just meeting the day-to-day needs and you know, basically kind of staying out of trouble. But then, you have others who basically put security you know, obviously their primary responsibility and want it to be a best practices type of organization. And I think if you want a best practices organization basically, you need to have an organization that you have confidence in, that you can trust and you need to build it the way you need to build it. The experience I have is

that you can't have these people coming in to your organization. Unless you have a very unique individual sometimes, I have to admit, there are exceptions out of every situation but it doesn't happen very often. It is not the rule that they come in here and they become you know a patrol officer to a supervisor. But, other organizations wouldn't have any problems with that.

But as far as the different levels looking at that, it almost relates to what level of security do you want at your organization?

Do you just want to stay out of trouble? Do you want kind of a minimum, basically provide the minimum requirements for security or do you want to have a best practices organization? There's a huge difference.

The inquiries and I ran into this at the ASIS conferences, the inquiries go to the consultants who think they know everything. And they don't know everything. They don't know what we want, they only think they do cause they don't ask us either.

Respondent four:

In a real sense I think it has significant impact because you have to have budget to support it and to support the training. In today's corporate environment, one of the first line items that gets a red line through it, unfortunately, when budgets are tight, is training. While I accept that not all training is essential, I do think that it is an important part of continuing professional development. I think the best training anybody gets is on-the-job training and having mentors and tutors but there is training that's not on the job that I think it's important for people to go to as well.

Respondent five:

Well. As anywhere else that last thing the departments sometimes get is a formal training program and the first thing to go is, economic hard times, is perhaps some of the training. It gets canceled. So, um, the budget has a huge impact. I think so. You know, I mean, maybe not the absolute last but it's well down the list. I mean, you've got to be operational, you've got to be adding value to the company or you've got to be in existence because it is required by some law or regulation by an oversight organization like the FDA. Those are all the things, you know, if we hit hard times in the budget, we're not going to cut back on compliance. Because that's mandated. We're not going to cut back on the controls of controlled substances. Because that's mandated. So it's like looking at any budget. It's like George Bush looking at the U.S. budget. The budget may be X trillions of dollars but you know, some of those are locked into paying off the debt when you can't cut there. So you can't cut there you know? So, where can you cut? The number of places you can actually cut, you know when you look at training, you can look at training the way Avis service used to look at the cars. It's a bad year, bad budget year, we'll keep the cars another year and not get new cars this year. Well that can work for a year. But if you got two or three years with no new cars, then it's a problem with people not getting where they need to go and you've got maintenance costs going through the roof that will eventually cost you more than new cars would have cost. So, it's the same thing with training. You know you don't have that hammer falling on your head. We didn't train this year. Bingo, down comes the hammer. Know what? There are impacts. There is an impact but it's not

clearly visible right away. And so you have to, but if you got along to... without training your people, without building up the culture that you're looking to obtain through the training program, then you end up with issues and problems that you wouldn't have had.

Respondent six:

Oh it's um. Its determinative, you know, a lot of companies expect you to have fully competent, fully successful security operations but don't allocate either basic training funds or more importantly professional development funds. You know, I think it's important to hire people with the right qualifications for the job and I think it's important to insure that they get good basic training when they come on board to ensure that they understand what their job is and that they have you know the training and the equipment and the tools necessary to accomplish their job. But I think it's equally important that those people get continuous ongoing professional development opportunities to stay abreast of technical developments, to stay abreast of best practices and that sort of thing in their area of responsibilities. And a lot of companies don't understand that people involved in fairly sophisticated security operations need the same kind of refresher training that attorneys need with continuing legal education. So I think budget's important, I think budget can have a role in professionalizing and ensuring that you have a first class operation or lack of necessary funds can have a detrimental effect. So I think budget is very important. Training and retraining is just as important in security as it is in any other aspect in the business.

Respondent seven:

Big. Which is probably why we don't do a lot of the things we're supposed to do. Training of course is almost always at the bottom of the list. It's always seen as a nice tool instead of a mandatory type of element of the security program. So budgets play a tremendous part which really requires someone again, to scope things out, what you're trying to, it has to be really part of the mission. For instance, our mission is to protect assets, to provide world class services, and to promote education. So it's a part of our mission to begin with. We understand that the educated employees or informed employees add to the overall security of our company making us or putting us in... in greater shape.

You really have to be committed to it and you have to show some results. See, that's where I think we've stubbed our toes. Is not showing the results of training. To really show an improvement that's using metrics to show that training does work.

You've got to have a deliverable, back to the organization that shows that this is a value-added item.

Respondent eight:

Totally. You can't deliver training without a budget. It's vital. You can't call people together for a conference or for the training session. You can't call in experts or consultants to deliver the message in more detail or more depth and you can't pay for the hotel, you can't travel. You know, you can't do anything without a budget. You can't develop software systems or even burn it off the CD Rom.

Respondent nine:

Well obviously, one level it's significant. I think what for most of us though in the major companies, it's the competition for the dollar. Not only for us to get it as a unit but then once we plan the funding for the year, there's competing priorities within the security component. And we've always felt that training and maintaining professional competence is really high on the list. So we not only would save funding for in-house training, we've also saved for out- house training. But we also encourage at least a couple, two or three different exposures outside of the corporate structure. For our higher level individuals. And that's part of our performance management plan.

Well we want to ensure core competency. That's one reason for the training, that there's money that's kept in there. And the other is to enrich individual growth. We feel that's a benefit to the company. So therefore we actually put together a training program or training plan for professional growth annually through our performance management system. And that's done for all management. It is for individual employees as well but the stressing of the core competency development is cleared for management, in the security function anyway.

Question Five: How does the placement of security within the organization effect training security personnel?

Respondent one:

Humm. I think placement of security is very very important but not specifically in the training issue. General Counsel I think is where it belongs. Even though probably 60%

of our work is HR- related but it comes to us from the law department. But, from a training standpoint, I have no correlation at all.

Well, we're in the law department here. Part of the law department. And the law department has a huge online ongoing training program. 100% directed at attorneys. There is no component there for security people. And I don't know what could be put on there that would be beneficial to my guys. I'm not saying that they know everything but these guys have all got 25 or 30 years in the business and we don't have IT so that's the new stuff that we would have to go and get up to speed on and have some training and we don't have to worry about that because we don't do it. Another group within the company does that. We are decentralized to a far thee woe. And I've gone twice and said, you know, I'm not looking for more work but it would make more sense to have him report to one of my guys and I've been shot down. Not even, initials from a good friend of mine who's the VP of Administration. He goes no. We won't consider it. Cause we consider it a part of facilities and we want to keep?? Cafeteria, credit union, you know all that stuff. We want security, an integral part of that, we want to keep all of that. I say, that's fine with me. But it's dumb. That's a disconnect, I think. You know, a company that does not report to the same, no matter where it is, it should report to the same function. That's some of the odd things of various companies. You'll see some major differences.

Respondent two:

I think certain cultures put more emphasis on training than others. For instance, if you find yourself, God forbid, in Environmental and Safety, your getting the sh** trained

out of you. If you're in the law department everybody assumes you're there with the same skill set and you shouldn't get any training. So the culture of the place that you're reporting has a lot to do with the training. Absolutely right. Some areas have a strong training culture within a company. Certainly Environment and Safety as Human Resources does. Law department doesn't. Finance probably doesn't, that's where you start nickel and diming over, really has a lot to do with where you are placed in the organization.

Particularly on the good centralized stuff. Sending a guy off for a few months to management school down at UVA. That's a tough one in some areas and an absolute easy one in others. Obviously, nobody bitches when I get all the guards together and they do CPR. That's an easy one.

Respondent three:

You know, could be big, I think that really depends on the organization. It also depends a little bit on the person at the top and that person's ability to negotiate so to speak with his or her boss in the organization which they reside, in order to get the appropriate money for the training. So, and I think it really, in that regard, you know, it could have a positive or negative effect depending on one's ability to be able to do that. I know that based on this organization, my organization here, I report to the executive vice president of Human Resources. And, I feel, in this particular company, in this particular time, this is where I should report. I think at some point in time I'll report to the probably to a president or somebody under the CEO. We don't have anybody in that position at this particular point. And, you know once the investigations lead to the Head of Facilities, you know they

realized that I shouldn't be there. And, HR was very reluctant to allow us to get involved in investigations because we worked for a department outside of HR. OK, so you have basically a property, confidentiality issue by being outside the HR organization. So then finally I moved into the HR organization and basically took over investigations and then we started going backgrounds because we weren't even doing background investigations back in '92. We started doing backgrounds. So we were able to really help them get involved in these types of activities that they wouldn't let anybody do outside of the HR organization.

Respondent four:

Well I think that the reporting relationship of the security function and the level of which it reports is important to underscore training needs. I think it makes it easier to sometimes, to get that funding.

In our case we report to the office of general counsel. Which I think is absolutely the right place for any corporate security organization to report. It's the optimal place. For example, the prescription drug marketing act and the daily interaction with our regulatory attorneys as you know, do these investigations on a daily basis around the country. And I wouldn't describe it as formal classroom training; it certainly is facilitated by the fact that the legal function as well as the goal in security group are both housed with the office of general counsel. So the reporting relationship and where the organization is located is enabled or facilitated by you know the, that reporting relationship.

Because there's an understanding and appreciation from the legal side of the house as to what is needed to, for my staff to be able to do their job and do it well. Because they see the work product. They're working with us hand in hand. Those, in my view, I think are mistakes. The symbiotic working relationship and functional alignment of the corporate security function with the legal functions in my view are unmistakable. It's just, it, one supports the other.

Respondent five:

My opinion is the placement is more, rather than getting into the terminology of legal or HR or tech ops or admin services, what's important about the placement is the person it reports to. Not whether that person is the general counsel or the head of HR. What's important is that it be a well-established successful executive who's not looking to use every possible thing under his banner to call himself to the next promotion. And therefore brings calm, oversight with a high degree of confidentiality. What you like to avoid is somebody new to the company, someone who doesn't have the track record of experience within the company. Someone who's looking to make a name for themselves to get to the next level and would use security issues to do that if he thought it could possibly benefit him. So I'm more inclined to not where I reported as long as it was the right person. Which is probably different from what everybody else said?

Respondent six:

Well, it's I think it's critically important. I think that the placement of security in an organization has a direct bearing on the way security is viewed in the company. The importance that a company places on security and that perception and that reality trickles down to the training aspect of it. If senior management truly believes that security is important, they place it at a high level in the company. They ensure that the head of security has direct access to senior leadership and they ensure that security has the necessary resources to do their job. As you and I just suggested, the training aspect, training's a resource. It's a resource like guns and bullets and camera and video tapes are resources. A lot of companies don't recognize that. A lot of companies' bury security beneath the facilities manager or the HR manager or something like that. In my opinion in most major companies, security should have a much higher profile. I think where a company places it is a statement of the importance they attach to it and the importance they attach to it determines how much money and how important they see training.

You know you bury the function under a mid level manager and that person is more likely not to appreciate the importance of security. It's just another function in a vast portfolio of things the guy's responsible for. He might be responsible for the corporate fleet, the company store, the cafeteria service and oh, by the way, security also. And, when that guy runs into a budget crunch he's going to look at security as the least important thing in his portfolio and training is probably the least important thing in security. So, it's bound

to get axed. I think where the function is placed is critically important to the kind of training that can be expected.

Respondent seven:

I think it can affect it considerably if your department or your function is not integrated or seen as part of the business, the operations. Case in point, where I was at previously security was part of the safety, oh no, we aligned ourselves with the safety and risk management group so they were already integrated in the operation and dealt with and reached out to every single employee in the organization. Now if we were just from corporate, trying to break into that, that whole idea of training someone at a XXXXX level, we would have never accomplished that. So you have to know your organization and understand and really get yourself into those avenues where training's already occurring. You know what I'm saying? So you just take the security piece and you just attach it to what people are already engaged in.

It's a great idea to try and watch these things and to have dreams of grandeur but it's really harder, it's much easier if someone's already greased the skids so to speak. And you can just attach yourself to what's already been done. I've found that to be the most successful way to do it.

With metrics involved some key pieces you have to have a way to again, like your retention piece which requires metrics, you have to be able to show people in retaining a solution. It's great to even then attach that to actual results of like reporting, reporting incidents could be a metrics, there's a whole different metrics.

Respondent eight:

Ah yes. It's essential that the corporate security director or VP reports to a board member. Because that gives them the authority and the recognition within the company. It elevates the security function to a higher level which concentrates the mind of the individuals within the company no matter where they are that security is important. It's a high level board issue and in my experience having been previously with HR, finance and legal, the optimum department of the security organization is within legal.

Respondent nine:

You know we, the programs that we run for professional development and personal development are mirrored throughout the corporation, through the performance management process that covers is cross functional.

Oh yes. I think a lot of us have bench marked with each other on where security falls within the structure of the company. There have been a myriad of reporting relationships; some in facilities, some in legal, some in HR. The development of the company and individuals who have these functional areas have big barring on how effective the security is going to be within the corporation.

Because they would have their own functional initiatives in this regard. Then you would be absorbed into that philosophy which may or may not be helpful to you in the security capacity. And that can be a problem or a blessing. Most people that report to an HR function have had difficulty because it basically does not have a lot of synergy with the security group. And, that's been my finding. Those that have reported to a legal function

seem to fair better within the corporate function because of internal programs already existing in those functional areas.

Question Six: Question omitted prior to interview. (How does the placement of training within the organization effect training security personnel?)

Question Seven: What do you perceive to be barriers to setting up training for security personnel?

Respondent one:

Well, one is always budget. Secondly, identifying the training that's needed. That's, if you're relatively successful at what you do you have a tendency, like we do, that hey, you know we're beyond the point of needing training. That you don't assimilate on your own and each individual... But identifying what training is needed is a major issue. If my guys are falling down on basic interrogation or interview techniques, then I need to be attuned to that and say ok, maybe you guys need to take a couple of these courses that are out there. What ever it is, if it's like, they can't... analytical skills are weak, then I might direct them here at a course at Rutgers or something where they have to do statistics or analysis of functions. The barrier is you have to have the time to identify weaknesses but it has to be significant weaknesses when you have a small group like this cause you don't have the luxury of being able to take a couple guys and being able to send them to a course for three weeks or something or other.

Because it affects all the other guys.

Well you heard the story at XXX. Two or three years ago. XXX was overseas and if you've been to the offices, you know you walk in and go to the girl and there's a bank of elevators, she gives you a badge to put on your lapel. You go over to the elevators and that's where the security guards are. They clear you into the elevator. You get on the elevator, you can take off your sticky badge and no one gives a sh** from that point on, it always drives me up the wall but, a bunch of animal rights people, somehow got past the guards and they get up to the executive floor at noontime on a Tuesday or Wednesday, I forget which. They went up running through the executive floor screaming and yelling and throwing stuff around and grabbing papers off of desks, the usual animal activists bit. A couple of the executives that were there immediately picked up the phone and called and low and behold, everybody was out to lunch.

Worst day of his life. But you know, when they have trouble, they call you. You hopefully will have someone there to answer the phones. So now they have rotating shifts.

Absolutely, whether it's something practical like that or something that's completely bizarre and there's no place else to report to, it's going to be in your lap no matter what it is. If it's an owl caught in the atrium somewhere, it's going to come to you. We don't have responsibility here for security in the complex, but when some executive calls from the tower, I just can't blow him off and say it's not responsibility. So I would channel it to the right place. And, we don't manage guard forces but we do offer security surveys. So you're right, we can't really, you could try to separate it but it's still going to come into your lap no matter what happens.

Most companies just go for cost and the lowest bidder and you get what you pay for. Our guards here are probably paid higher than probably any place else in the company because we demand a higher quality and it really pays off, I think.

Respondent two:

Well, the first barrier is work load and time available. In other words, most of us in security are so thin; the ability to take time off or to build training into a work day is very difficult. So I guess there's a queasier financial piece there that's the biggest barrier. And the second barrier is, the quality control of the actual training itself. Picking the right courses, getting the right people to do it. There's so much junk out there. There's so much films and stuff that, everything from ASIS to some lease guys out in California that make their living training everybody. They'll train security guys; they'll train nurses of who take of drivers and stuff. On the other hand, when you hit it right, it just, it really changes a guy's life.

No these guys were... First thing they did the first day, they met them in the hotel and they started the first stages doing counter surveillance routes, route selection, choke points, most likely to get ambushed. The second day, and just one-on-one, or two-on-one actually. Second day, they went out and did the driving. The cost was a couple grand. If it was $2,000, I'd be surprised. It was very, very reasonable. Very, very professionally done.

My drivers, the first time they did it, they thought they knew what they were doing and they first of all, they panicked, and they literally broke into a sweat and froze. Went completely off the track when somebody started shooting at them.

Respondent three:

Barriers? Well certainly you know getting the budget to do it. That is an issue because like I said before, you know, you have to do it while they're on post or you have to do it, bring them in to do it and then that's going to cost you overtime. You know, there's no getting around that so obviously if you can't get the budget, then you have to come up with innovative ways to do it on post. But I think, obviously on post getting, getting an adequate budget to handle the level of security, the level of training that you want have for your organization is certainly a potential barrier. Cooperation by the, if you don't have the right level of supervision, in other words, if you don't have people that know how to supervise or manage, then you could possibly have a barrier to affect the learning because you don't have people who could answer questions. You don't have people that care; you don't have people that, you know, want to or are looking out for the security officers to ensure that they are providing the level of service that the customer wants. Sometimes that can be a barrier and again, that goes back to my reasons for not having, you know, glorified security officers, supervisors. Or, you know heroes because they've done a great job because they were a patrol officer for so long, they've done such a great job of promoting the supervisor and so on. But that could definitely be a deterrent or a hindrance to your training program.

That helps people understand why it's important.

Respondent four:

Budget yes that would be one. And I would say the other one goes back to a perhaps, imbedded in a lack of client-oriented service. Whereby the line organizations that you're supporting whether they be in our case, sales and marketing, manufacturing, research, if they don't understand your role, or if they're not satisfied with your role, they may not necessarily see the need for training. You know, despite how the function has changed and evolved over the 25 odd years that I've been in this business, there are still some of those archaic long-held views that security is the guard at the gate.

Respondent five:

Well barriers would be a lack of understanding by high levels of executives of the value that a modern professional security program can bring.

You know an example, you know with XXX. For years XXX was one of the top companies in the United States. But it had an inferior low level unsuccessful security program. It's probably one of the few areas where it wasn't one of the world class programs within the industry or within all businesses. It just didn't make any sense. It held some programs back. So, you know, not viewing security as a value added activity... Another drawback is looking to it as locks, guards, alarms, and period. And not recognizing the investigative, the intelligence due diligence sides can be extremely valuable and perhaps more valuable.

Respondent six:

I think senior management buys into security as an important role and senior management reluctance... I think if senior management doesn't appreciate the importance of security, they're going to be less likely to be supportive in setting up a good comprehensive and sometimes expensive training program. So it's management's perception of the importance of security that could be a barrier. The head of security's outlook about training could be a barrier some people who head up security organizations want to make sure that they always know more than the people that work for them so they don't want to train these guys too much you know? My perception has always been that I want everybody who works for me to know more about what he's responsible for than I do because if he know less than what I know about his responsibility I don't need him. So you know I think the senior security officers understanding that the better trained and the better equipped that people are to perform the better he's going to look and the more secure the company's going to be. Senior management's attitude toward security and security director's attitude toward training could be barriers or they could be enablers. If they go the other way. And money.

Respondent seven:

Again, having learned from mistakes I think we mentioned some of the lack of planning and scope, not having a clear understanding of the end result; it's not so much content. You know we, we're pretty good I think, we knew up front but putting it into a deliverable format is where, it's the old making information understandable for non

security professionals. You really have to break it down to basic elements of what it is that we do. I think another barrier is just not understanding your organization and you've got to understand your organization and culture.

Which means it takes time. Which means you can't just walk in the door and start to roll something out. This takes patience and persistence. Almost to the point where you're better off not doing anything for a period of time, till you understand.

Yes. Yes. Move cautiously. You know, proceed with caution.

Respondent eight:

People are naturally reluctant to engage in security training because it's not the core activity. The core activity is in selling the product, manufacturing the product, and research; therefore there are natural barriers because they see it as a hindrance to achieving their own goals and objectives. To overcome that you have to buy in support from the top. Actually. conservative and collaborative way impress upon the prospective audience of the need to secure our people and our assets. Because it adds value to the business.

Otherwise management time would be expended in dealing with security problems which could have been avoided.

Respondent nine:

Clearly, based on the programs that they've already had ongoing in the function and the synergy of your group to theirs.

I think just funding. I mean, I go back to that. If I'm limited on my funding, I'm going to have to review what programs we run with and re-prioritize based on what we want and what we are going to be able to do. Based on the allocated funding.

So to me funding is a critical part of. It seems to me in good prosperity times, you have abundant training programs but when people are running tight in the industry, you have to cut back and you're looking at any possible cutbacks you can make across the board. Training unfortunately falls under that knife with everybody else.

In fact, you'll pay for that one or two years down the road on core competency or growth. Professional growth the individuals you have leading the units.

Preparedness suffers without funding for training in my opinion. At least in our culture, the whole reason security is proprietary with, well we have some contract people, but the reason we still have proprietary people running the security function is to make sure we have adequate, actually feed preparedness levels that we've established. And you know that's a myriad of things for natural disasters, chemical spills, you know the whole gamut.

Question Eight: What practices are ineffective in setting up successfully run security departments?

Respondent one:

I think it's the central authoritarian, you know, very rigid hierarchy of taking orders where the regional people, or even your own divisional security people, can't run their own businesses. Everything has to be centrally authorized. We're, this is why we are successful. We feel it's caused because they are a decentralized company. It's a mutual fund of

companies. So there are security people who report to their companies who have no relationship with us. There's no dotted line, they don't report to me. There are five or six of them here in the company. And they take care of their own companies. They keep me advised because we have this informal relationship of what's going on of significance and if they get into a problem area where they need some assistance or some help or some advice then they come to us and we work together on it.

For my company, for this company, with a very decentralized structure, that's the only way it could work. Now, the safety department who sits right next door to me, they have a very rigid, hierarchical structure. They have regional safety people all over the friggin' world. I mean, you probably have the same thing. They got like a hundred and something people because safety is such a big issue in the manufacturing process between using chemicals. But the VP runs it with an iron hand. He has deputies here in corporate that run every aspect of the safety program overseas. Now it may work for him but they don't have a lot of flexibility and it's the government model. Everyone kind of kisses up. Whereas, our people have a great deal of independence. I now have a guy on the west cost. New company. We bought them two years ago. Investigating an $800,000 embezzlement going on on a purchase card. Woman bought horses and every other damn thing. We're about to seize her house but, he's running that. He doesn't report to me. He has somebody from internal audit participating and that's kind. Explaining what happened in the event we ran across it again. It was some areas where we could have different ideas. We could have done something differently and that was very beneficial to all of us. But, he's in charge of

it, he runs it, he gets the blame, he gets the fame. And, we kind of blessed it and said, you've done a hell of a job. He's thought about doing this, and he doesn't even think about it. It's informal, informal, not a direct hierarchy structure and for me that works. But then again, depends on the culture of the company.

In this company, if someone tried to do that in this company, they'd have their legs cut out from under them. My general counsel has told me that on a number of occasions. He said you know, you adjusted to the culture of the company and you get the businesses out beyond what we hope for and you do it in a way that fits in well with this company. You have direct access to the CEO, you know, I talk to him practically on a daily basis. I eat with him, I travel with him, other companies, that's not the case cause it's a different culture. And, you have to adjust your model to that culture.

Respondent two:

The boiler plate programs that you can buy tend not to be relevant, they're so generalized, I guess you can find ways to spend money on a boiler plate and end up with nothing that is specifically useful to your organization and you loose the attention of your guys. So, not having something that is very work-specific to the guys' work, for instance, there is a whole different set between teaching a guy to how to do an interview and interrogation at Reed and we do that or sending out a bunch of guards to learn how to do CPR. The skills that some of the issues are the same, in other words the team building, the systemization of skills but it has to be very specific to the job and to the mission. Specificity is a big issue.

Respondent three:

Well, no. I think the biggest problem is, is the fact that we don't train them. We don't tell them, you bring somebody in for a temporary assignment and basically you just put them on that assignment with very little information. Not enough information to do, you know, a professional job. As a result, they don't look professional. Basically, you just put them out there and expect them to understand what they're supposed to do and do it appropriately. I think the lack of training, the lack of the subject that we're talking about here, is one of the biggest mistakes that we make.

Yes, now I see what you're talking about. These self tests... Well one of the things that we require is for the training to be customized. One of the things that a lot of what people do is rely on PSTM tests, tapes, and all that kind of stuff that are very, very general in nature and sometimes don't even apply to your organization. I think it's a matter of, you know, if you want that professionalism and credibility and you want that confidence in the security officer you've got to teach them things that they're going to encounter at your organization and how to handle them. You know, for example, if we have hazardous material on site, then we need to teach them how to approach that situation, how to respond to that situation vs. just telling them how to use a fire extinguisher. So we've got to get down into the detail of what may happen at that particular site and teach them how to respond to that. Again, that level of self confidence is needed when you respond to a situation like that. So you don't get yourself in trouble. They can get injured, they could get hurt, they could have somebody else hurt. They need to know what to do so it's very

important to tailor it and to customize it to your site and I think that's one of the issues that a lot of people don't do. A lot of people rely on these very general systems for training if they do any training at all. And, the security officers can't relate to them. I don't really care for that unless there's some opportunity for interaction after it. In other words, we may design a tape and we may have a tape that's applicable to our site but then you have to have supervisor or somebody there to be able to answer questions. So, if the officer has a question, they can answer it. Or actually ask the officer a few questions on whether or not they comprehend and understand their responsibilities associated with that particular accident or incident.

Yes, so I think too many times we give them a tape, go in there and say take 20 minutes and learn this and check your name off that you've had this training. It just, that's pretty much ineffective.

Of course what you have is the, there isn't a push. I see is part of the issue. There isn't a push on the contract security company to do that. Because, they don't want to say, well you need this amount of training and by the way, it's going to cost you this, so when you hear presentations, you've probably heard these many times and you hear proposals from security companies, they talk about this magnificent training program that they have but they never talk about how much it's going to cost you. And if you just go by what they say, wow, we have this tremendous training program, and you don't address it, it's not in the proposal.

Respondent four:

It would be designing or promoting funding training that is irrelevant to the business. I'll give you a very crude example. Nobody on my staff, nobody in this company carries a gun. Firearms training for someone on my staff, because that's something that they wanted to do and something that they've requested; completely irrelevant to the business.

That's an extreme example.

Not that comes to my mind. I think it's a basic principle that you would build a training program to support the needs of the business.

Respondent five:

Oh. Um. One practice would be to concentrate solely on security and not on business issues. Which is obvious from some of the other things that I've said. Um. One practice would be to have someone, you know, strictly focused on the immediate issues that are impacting his local assignment area and not give him a broader, more global perspective of the issues facing the industry.

I mean obviously, one is going to be focused on for example guards and alarms cause that makes up 50-60% of his business, what he does for the company. But he also needs to take the macro view. The guards, alarms, and such, visiting center, that's a micro view. But he also has to be able to take that macro view to be able to support let's say the company efforts against counterfeiting without actually having a counterfeit case to work themselves.

I think those are general principles that I have of things that are uneffect-ineffective, I think everything else I could say would be kind of linked to them.

You know, assuming you have quality people. If you've got idiots then... One of the principles of ineffective is having the wrong people.

Respondent six:

What I would tell you is that anything that's not relevant to the job is ineffective. You know some people set up, you know new employee orientation programs or security training programs or whatever and they spend a lot of time talking about things that don't relate to the job. Don't relate to the roles and responsibilities.

Respondent seven:

I think what, when you see training defeated is so often in delivery expectations. In other words, we think that face-to-face type of training is the only way we can train people. We have, there's a misconception that there's one form or one medium of training is going to do it.

Yes. It just has to be... There's an expectation that you sit in a classroom for eight hours and you read the material and you walk out understanding and retaining all. It just doesn't work that way. There needs to be a variety of ways that you're trying to get information to people whether it be, it could be video, it could be face to face, it could be a virtual reality. We do some of that and some of our training for security persons... And it could be situational analysis. There's a variety of different ways that you can present material with the hope of having them retain that information.

Because people are going to take in information…

Respondent eight:

Simply just disseminating a program for local tuition without the guidance and support from the corporate center. The message seems to have more bearing and weight if it's delivered by somebody from the corporate headquarters.

Respondent nine:

Well this may sound, this may come off bad. I truly believe in benchmarking with real experts. I don't believe in benchmarking or relying on data from people that are largely academic. I don't know how to say that any other way than just say it that way. I, we deal, I'm sure in your position the same way, I deal with a lot of phone calls from academics whom we help but sometimes we'll have experts on how security should be configured or how programs should be run and these are not by practitioners so I try the nonpractitioners, I haven't found provide particularly good data. I don't know any other way to say it but to say it like that.

Question Nine: How does the training of security personnel for the ethical pharmaceutical industry differ from the training of the other industries?

Respondent one:

I don't see where it would be significantly different. I honestly don't. I mean the ability to get and gather information, analyze, prioritize, and resolve, come to know where you're going and come up with a way of getting there that's effective and cost effective and with positive results. Whether it's pharmaceutical business or whether it's any other

business and there are some businesses I think where there's different competencies that are more important than others. If you're in the oil patch and your running security for a site in Algeria, you've got to be a little more in depth at paramilitary role than most security people. Communication issues that you have, kidnapped may be some different companies have certain select businesses but I wouldn't see much difference between pharmaceutical or financial. We talk and exchange information on the same issues, with some exceptions, I think it is the same basic training that you're interested in is to help your people do their job better which is interview skills, analytical skills, certainly computer skills.

If I had the luxury of a larger organization, then my druthers would be, I would say, ok Andy, your ability to prioritize your work is your biggest weakness. You run helter skelter, you don't prioritize very well, I would like to have you take this course on prioritizing things.

Respondent two:

It doesn't. The skill sets are the same, the values, the team building, the consistency program. All of that. Whether you're doing it's was wax or at a pharmaceutical company. The one I guess I'd say this. Because of the heavier regulatory oversight, there has to be a much little bit higher sense of legal good practice. I guess there's a more *sensitive* industry.

Respondent three:

You know, may be some of the individual training is different. For example, you would be trained in GMP? Practices and you know you have to understand that you know,

your animal facility and you know, you have to understand how important manufacturing is and so on and so forth but again it's just a matter of that's more customized, that's more specific to the industry. In general, in general, I don't think the training should be any different. I don't think it's any less important or any more important that any other industry. It's a matter of providing quality security services. I think that's what training should be all about. To ensure, to help assist the security officer to have a high level of confidence, act professionally, be credible, be knowledgeable, that's what training's all about regardless of what industry it is. If you have that, then you are on your way to being able to provide quality services.

Respondent four:

I would say that it really shouldn't differ much, as much as that training which is particularly associated or focused on aspects of the pharmaceutical industry. It's actually very similar. It's encouraging the same certifications. Whether that be CISSP, CPP out of ASIS, CFE but drawing it to the pharmaceutical industry, it requires an understanding if you're supporting the manufacturing division of GMP. You know, Group Manufacturing Practices. Understanding of PDMA if you're supporting U.S. Human Health that markets themselves direct here in the United States. So, I think some of the most important training that people can have that are supporting the ethical pharmaceutical industry are courses maybe even internal courses, courses like you know manufacturing 101 that some companies offer. Research 101, Sales and Marketing 101. Really getting that basic

understanding of what these organizations are doing, how they function, and then you build on that with the on-the-job training and the relationships that you build.

You know, the old view of the corporate security professional was you know, we were company cops. That's so out-dated and so doesn't work. That, anybody still in that model is breeding failure. And, you know, I think that. I think that there are more than a few corporate security organizations based on the people who head them and their personalities and their long successful careers in government service, they have a hard time making the transition over to the corporate world and realizing that they're working on a business model as opposed to a law enforcement or government service model.

The security function is no different than the human resources, the legal, the finance, whatever other corporate staff groups there are, we're all individually looking and supporting the business with our own respective areas of expertise. So that too is a perhaps a different view than the old colloquial one that has been held, you guys are the security guys and we know where to get in touch with you when we have a problem. That model really doesn't work. You've got to be viewed as an extended number of whatever, extended number of the management team to whatever group or clients you're supporting.

And you've got to be willing when you look at whatever business issue it that is out there that you can add insight as a security professional because I can promise you the line manager is not, does not, have a trained eye to see the issues that you might be able to see. The same as with HR or Legal, it's just a different training and it's you're part of the business. You've got to be part of the business. This all does go back to training. It's why I

really don't recruit folks over sort of 40 years old to bring into the organization because I want them young and I want to be able to develop them on the job to make them corporate security professionals. I don't want to bring somebody in at age 50. And I'm not saying this is the only model, I'm being very general but I want to bring people in that I can shape and mold and who are bright people with some security intelligence experience in a public organization. I think that's important to see that side of things and to have gotten that experience. But, I don't think your best corporate security professionals are the ones who have had 30 year careers and then make the switch to the private sector. I want somebody that's got 5 to 10 years on that side. And you know, whether I'm recruiting in Asia, Europe, North America, Latin America, I'm looking for that model because it's my own experience as to...there's going to be a certain profile. Interesting story I, when I was recruiting for...I think the best general training is the on-the-job training that you supplement with particular areas of expertise, whether that be interview techniques, PDMA, language, whatever is needed to make you the best security professional who supports your clients that your assigned.

Respondent five:

Well, like most industries, the pharmaceutical industry has issues and problems that are shared with other industries. You know, you've got to have controls, you've got to have policies, you've got a control access, you have to have alarms, you have to do due diligence, you have to, you know, background checks on potential employees, you have

thefts, you have frauds, internal and external. All these things are shared by major business corporations.

Is that we have a unique set of issues, a unique set of problems that to a certain extent are different and that obviously involves the counterfeiting of medicines, the illegal diversion of products, the protection and control in tracking control substances. The extremely important issue of information security since the entire lifeblood of the company is based upon research and on patents and on intellectual property and trademarks. So these are all to one degree or another somewhat unique. You have some auto company, you know might have counterfeit brakes floating around out there but that's really different. They wear out quicker but that's really quite a bit different from taking a counterfeit pill. You also have the strict regulations that other companies don't have between the FDA and the DEA and the United States and from the Medicine Control Unit in Great Britain and other health and regulatory authorities across the globe, you have very, very tight restrictions placed upon the industry.

Yes but I think, almost any industry could say well, here's a list of things we share with everybody in business and here's a list of things that's unique to us. I'm sure the steel industry could come up with a little list of what makes them unique and you know Boeing could probably come up with a list of things that make them unique. Each industry has its own unique set of its own issues and problems. And then some companies might have their own set based upon where they are located. So, but each industry has its own set and I think each company probably has its own set.

Respondent six:

In my experience, it is broader and more complex because we have more responsibility and let me explain that this way. We manufacture product so we have to have security standards for the manufacturing of product, we distribute product so we have to have supply chain security standards. Our products are all based on patents and intellectual properties so we have to have people that understand intellectual property and know how to investigate people who would steal intellectual property. In other words, violate our patents and counterfeit our products. We have in that same area, a lot of our proprietary information networked into a proprietary computer network. We have to have people involved in the security operation who know technology and know computer forensics and that sort of thing. We have the same issues of violence in the workplace and theft and whatnots that other companies have to we have to have people who know and understand how to deal with those issues. So, we run an operation that's responsible for all of those aspects of security. We have some people that are responsible for discreet little parts of that who receive expert training in their area of responsibility. We have other people who are kind of generalists who do, who have responsibilities in more than one area. So they get training in more than one area. Keeping those people current and keeping them motivated is an HR challenge, a budgetary challenge, a motivation challenge, and I think when you look at training in the pharmaceutical industry across the board, it's probably one of the most demanding industries in that regard and we probably spend more money on it than a lot of other companies spend. That's a long-winded answer.

Currently serving in that role. So gee, it's about what you think about this topic. And that's going to be the really interesting aspect of me sitting down and looking at it. Your colleagues sometimes were close to what you're saying and sometimes they're not but it really does help to answer what is it that you're thinking about for this particular issue.

Respondent seven:

I think there may be similarities with other industries but just some really unique things have popped up for me. Keep in mind I've only been in the industry now for 18 months. I am still learning literally every day more about this industry, more about the organization I'm a part of. So I'm sure you may get better answers from some other people who've been in the industry longer. But what I can tell you is first thing that comes to mind is the training of nonemployees. Specifically law enforcement. It's important for us to have law enforcement understand some of our biggest threats are counterfeiting, diversion, that's pretty critical. Where, maybe in some other industries, that's not so true. That may not be as big a deal. So that affects training. We literally need to train law enforcement. Which could be a foreign concept if you're not interested in the topic. Training law enforcement boy. But you get into some of the intellectual people that, or intellectual property's a big deal. Like the movie industry. Pharmaceutical industry, you know, intellectual property are life blood.

Really the one thing that comes to mind is the importance of here, you're interviewing all ten of these people, I think we're going to be far more successful by

banding together and perhaps looking at some of these issues even like training in a more standardized way. There's a way that we can share more information across the board, it's really going to help us. It's going to help us tremendously.

Respondent eight:

Well having been in the finance industry previously to joining the pharmaceutical industry, I can only use my own experience in that within the pharmaceutical industry, it tends to be more fluffy. More based on a cultural philosophy to try and encourage philosophy of good security which is not prescriptive. Within the financial sector, training was very much by rote. This is the procedure; this is what you will do. Do not deviate from the procedure. Very heavily regulated I would say.

Less prescriptive.

Respondent nine:

Well, I wouldn't know if I'd be able to answer that.

I, I, just quite frankly am very reluctant to guess. I feel really out of the loop on what some other industries may do.

Summary

This chapter captured the transcribed responses from the nine respondents to the seven research questions asked of them. These responses will be analyzed and conclusions will be reported in Chapter V of this study.

Chapter V

Summary and Discussion

Introduction

The purpose of this study was to answer the question: What are the elements of a successful training model, as perceived by global corporate security heads working in the ethical pharmaceutical industry?

The literature review for this study revealed that research on security training is neither comprehensive nor plentiful. In addition, heads of global security organizations have not been queried about their perceptions on what elements make for successful security training. Since these individuals play a key role in their organization's function and direction, their perceptions on this topic are quite important.

Open-ended interview questions pertaining to various elements of security training were utilized to gain an insight into the various respondents' perceptions. Nine out of the ten individuals asked to participate in this study voluntarily agreed to be interviewed. Interviews ranged from thirty minutes to sixty minutes in length and were conducted in person or by telephone, depending upon each respondent's preference.

Key elements gleaned from participants' responses are presented after each research question. Following the *Summary of Study* are the *Discussions and Recommendations.*

Summary of Study

Following is a summary of the seven study questions (see Also Appendix E):

Research Question One

What is your definition of successful security training? In general, the participants' responses were extremely varied. Some of the respondents felt that their answers applied only to individuals performing professional proprietary duties for the company and did not include contract security staff or contract security officers. Other respondents believed that it was important to include all levels of staff including contract security personnel. Some respondents were specific in their answers while others chose to speak in more general terms.

Respondent One believes that training should involve all elements that impact the business.

Respondent Two indicated that training should be relevant and cost effective while addressing skills, leadership, and team building.

Respondent Three was of the mind that training should address customer service issues along with developing professional appearance. This respondent felt very strongly that contract security personnel be included in any training programs being developed.

Respondent Four defined successful security training as training that leads one to continue a professional development of staff members. In addition, Respondent Four was of the belief that the training should be strategic and that it should be limited to professional staff only.

Respondent Five indicated that training should involve high potential, experienced individuals concerning specific business issues of the particular industry so that they can be

applied to desired investigative, law enforcement, and intelligence experience. He further believes that the training should be value added and that the training be directed only towards professional security staff, not to include security officers.

Respondent Six felt that training should be different depending on the level in the organization and that training is a resource just like guns and barriers.. Furthermore, training should be on a continuum.

Respondent Seven indicated that training should be results-orientated on the part of the recipient regardless of the level.

Respondent Eight felt the training should deliver and communicate key messages and it should shape the culture within the organization. In addition, it should convey policy, procedures, and standards.

Respondent Nine indicated that training should revisit standards and that it involve a two-fold process that allows the individual to feel good about the training and that leads to an effective action.

Research Question Two

From your perception, what are the elements of a successful training model to optimize the training of security personnel? Question was omitted prior to the interview.

Research Question Three

What do you perceive to be the ideal best practices for a global corporate security training program? Responses to this question were also varied. Several of the respondents indicated that incorporating business related issues into training was a key element.

Respondent One was of the belief that the use of a regional model would work best due to the fact that different regions of the world are impacted by different issues. In addition, Respondent One indicated that latitude should be given for changes in the different regions and that the policies do not drive the training.

Respondent Two felt that the team should be trained in one methodology and that it would help in developing trust amongst the team.

Respondent Three was in favor of customer service-focused training where the staff is trained to understand what is expected of them.

Respondent Four indicated that the training should be designed so that trainees understand that business and training incorporate language skills and that training be individualized to reflect different businesses that security would be supporting.

Respondent Five felt that training should be a formalized program during which time professional security personnel have the opportunity to also become businessmen.

Respondent Five believes that training should blend security expertise with business issues and that operating as a *silo* be avoided. Respondent Five also stated that training should include working as a team across the globe and that company culture be supported.

Respondent Six indicated that the best practices should entail management and leadership courses and that the individuals being trained know their responsibilities.

Respondent Seven believes that understanding the business as well as working on issues of re-training and staying current be incorporated into best practices.

Respondent Eight indicated that the use of various techniques to deliver training be included. Such techniques would include classrooms, interactive software packages, breakouts, and on-the-job training. Respondent Eight also said that security staff should engage in projects that help them explore issues of the business with guidance from individuals who are knowledgeable about it.

Respondent Nine indicated that networking to achieve important information be utilized as well as using graphics and instilling the company culture into the training.

Research Question Four

What impact does budget have on training security personnel? The respondents were unanimous in stating that budget had a huge impact on training security personnel. Adjectives such as, Monumental, Significant, Huge, and Very Big were used to underscore how strongly the respondents felt. All nine respondents stated that budgetary decisions about training is a key element in the success or failure of the security organization. Respondents indicated that in administering a budget, one should keep in mind that training is an important element and should not be one of the first things to be reduced when cutting the corporate budget. Furthermore, they indicated that the return on investment for providing adequate training for personnel should be taken into consideration.

Research Question Five

How does the placement of security within the organization effect training security personnel? Responses to this question were unanimous in that all respondents felt that the placement within the organization was extremely important. All of the respondents indicated that placement of the security organization should be at a high level within the company.

Research Question Six

How does the placement of training within the organization effect training security personnel? *Question was omitted prior to the interview.*

Research Question Seven

What do you perceive to be barriers to setting up training for security personnel? Respondents Four, Five, Six, and Nine all felt that reporting to a manager or organization that did not understand the security mission was a very big barrier. In addition, they considered support from senior management or lack thereof as a key element in security training. Respondents One and Three indicated that the administration of the security budget was a key barrier to setting up training. Respondent Two indicated that the workload and lack of time for training was a key barrier. Respondent Seven indicated that a lack of planning and not having an understanding of the importance of training was a barrier. Respondent Eight indicated that training not being viewed as a core activity with proper corporate support was a barrier.

Research Question Eight

What practices are ineffective in setting up successfully run security departments? Respondents Two, Three, Four, Five, Six, Seven and Eight all indicated that the use of boiler plate or training that is not individually designed to the business unit constitute an ineffective training practice. Respondent One indicated that training that is informal and is not directed towards corporate culture is an ineffective practice. Respondent Nine indicated that the lack of benchmarking with other organizations and real experts was an ineffective approach.

Research Question Nine

How does the training of security personnel for the ethical pharmaceutical industry differ from the training of other security personnel? Participants' responses to this question were evenly divided with four indicating that there was some difference in the training for the ethical pharmaceutical industry and the other four respondents indicated that there should not or was not any difference. One of the respondents, Respondent Nine, indicated that since he did not work in any other industry, he didn't really know and was not in a position to comment.

Discussion

This research focused primarily on analyzing participants' responses to seven research questions and to a lesser degree on information gleaned from the Demographic Survey Form.

Analysis of the Demographic Survey Form revealed that all nine respondents were white males, ranging in age from their early 40s to their early 60s. The level of education ranged from bachelor's degree to master's degree and all had at least 20 years of supervisory experience. The fact that nine out of ten individuals solicited to participate in this study reveals that there is a significant interest in this topic.

By far, Research Question Four, "What impact does budget have on training security personnel?" was found to be the most important element affecting security training. Individuals responsible for administering security budgets should keep in mind the importance of training and not allow this line item to be one of the first to be reduced when budget cuts are requested. As Respondent Six indicated, "training is a resource just like guns, barriers, etc., and should not be summarily dismissed." Harowitz (1997) captured similar comments about the handling of budgets, and the impact that budget has on training. According to Harowitz (1997), the Security Management and Pinkertons, Inc. survey reported budget as a key element. Also, Roth (2001) and Ledoux (1995) detail the importance of costs, as well as discuss how security managers actually spend budgeted money.

Incorporating business elements and courses into formalized training was also a key issue and articulated as a "best practice" by the majority of Respondents. However, the Respondents were not in agreement as to what should be covered. Similarly, Nalla, *et al.* (1995) conducted a survey to determine which topics security managers thought most

deserved emphasis in graduate education. Those who responded called for a variety of courses more typically found in a business curriculum.

> ...business skills, with courses such as motivation techniques, negotiation skills, employee training; security/ethics, with courses such as intelligence gathering, privacy issues and ethics, security administration, and operations security; and communications, with courses such as computer preparation, public relations and the media, public speaking, and writing (p. 95).

Morley, Vogel, and Huegel (1993) also surveyed security professionals about their needs for post-secondary education, including inquiry about preferred methodologies. Their stated purposes were to identify the priorities placed on certain courses by security professionals in terms of their personal and professional development and to describe which educational methodologies were most attractive to them (within certain budgetary and technological parameters). Their sample consisted of members of ASIS in the contiguous United States, about whom certain demographic information was also collected. The survey asked the group to rank a list of courses typically found in a general college curriculum according to their importance in the education of security professionals. Most important for this group were courses in management, English, and speech communications. The researchers' results varied widely, but they believe that this in itself was a relevant finding, commenting: "It may be that the field of private security is so diversified, and in such a state of flux, that developing a concise core curriculum is fraught with difficulty" (p. 126).

Placement in the organization according to the Respondents plays an "important" role. Some Respondents felt that it is not the function that you reported to but the person you reported to that was more important. Dalton (2001) contends that "the issue is not where security should report but what its function within the organization should be" (p. 1). Harowitz (1997) offers an example from the multinational pharmaceutical industry, citing the case of a new assistant vice president of security who made it a top priority to convene a meeting with senior management to obtain support for making security integral to the organization. Once he had their support, he met with his internal customers, the department managers, to increase their awareness of security concerns in their areas. He followed the same process with the members of his own team, meeting with them off-site, bringing in a consultant to help map out goals, and in general solidifying the department's mission. As the new vice president put it, "My idea was to start at ground zero and ask ourselves, what do we do, who are we, who are our customers?" (p. 5).

Relying on standardized training was discouraged by the Respondents, as it does not allow for variations in corporate culture or individualized business needs. This is supported by Goodboe (1995). Goodboe (1995), when he was vice president for training at the Wackenhut Training Institute (a major provider of security services and training), advocated the use of adult learning principles (*andragogy*) in the design and implementation of security officer training. The Institute surveyed nearly 600 field security employees to determine which training and education methods they preferred and found that their results were similar to those in earlier research among both police and industrial

security personnel, in characterizing people drawn to law enforcement and security as "traditional and conservative," with a tendency to "hold onto old ways of teaching and learning" (p. 2).

Consistent with the conceptual framework of adult learning, the security personnel that Goodboe (1995) surveyed were strongly in favor of training methods that made cause and effect relationships clear, that explained why they were learning certain material, and that described concretely the application of what they were learning to their work. They also approved hands-on learning experiences. While there was some recognition among them "that the traditional 'I'll talk, you listen' lecture method [was] still applicable in some contexts" (p. 3), they were not convinced that it was the most effective training method for security personnel.

Respondents were not in agreement as to what levels within the organization should be included in training. Some of the respondents were of the belief that only "professional proprietary security staff" have focused training while other respondents felt that both proprietary and contract security staff should be included. Harowitz (1997) and Ledoux (1995) found similar disagreement about contract staff and proprietary staff.

Training differences between security personnel working in the pharmaceutical industry and other industries were mentioned by only four of the nine respondents. Four respondents felt that there was no difference in training. This split in opinion causes ambiguity as to whether the pharmaceutical industry needs or requires different training.

Recommendations

The following elements are recommended for inclusion when individuals heading security organizations are planning security training:

1. Budget: Cost center managers should keep in mind the importance of training. Summarily cutting money for training, or worse yet, not budgeting for training, could lead to members of the organization not receiving needed training.
2. Inclusion of business topics: Training for security personnel should include various business topics germane to the industry in which security staff are working.
3. Incorporation of various learning techniques: All of the nine respondents were of the opinion that various learning techniques should be adopted. The use of videos was viewed as something that is just one element of training and should not be the only method utilized.
4. Organizational inclusion: Regardless of the level in the security organization, all individuals should receive training that allows them to understand what they are expected to do.

Recommendations for Future Research

The investigator recommends that future research address or might include the following?

1. Survey security officers of ethnical pharmaceutical companies--both employees and contract employees--to find out how prepared they feel they are, what they feel they

don't know, what gaps they see in security, and what security breaches they have seen that could have been avoided had proper training been provided.

2. Study the relationship between employee morale of security officers and the level of training they have received. (Relate moral to job effectiveness).
3. Study security personnel who have changed fields to see the extent to which on-the-job training carries over from one industry to another from their perspective as well as from the perspective of their employers.
4. Study the relationship between security officers' knowing their job responsibilities and the way in which their job fits into the goals and objectives of the whole company and the effectiveness of their work.
5. Study the relationship of corporate budgets to security effectiveness in corporations.
6. Study the correlation between placement of training in a corporation and the effectiveness of security personnel.
7. Study the relationship between the type of training received and the job responsibilities of security officers as compared with their effectiveness.

REFERENCES

American Society for Industrial Security (1997). Matrix of sessions [Electronic version]. *Security Management, 41* (7), 62. Retrieved April 20, 2002, from: MasterFILE Premier/EBSCO database.

American Society for Industrial Security *ASIS International 2001 employment survey: Not all security compensation is created equal* (2002). ASIS Security Industry Buyers Guide.

American Society for Industrial Security. (2002) *Assets protection course II: Practical applications.* Professional Development Events. Retrieved April 27, 2002, from: http://www.asisonline.org/profdev/apcii0502.html.

American Society for Industrial Security. (2002) *Assets protection course III: Functional management.* Professional Development Events. Retrieved April 27, 2002, from: http://www.asisonline.org/profdev/apciii0602.html.

American Society for Industrial Security (2002). *Managing your physical security program* Professional Development Events. Retrieved April 27, 2002, from: http://www.asisonline.org/profdev/managing0502.html.

American Society for Industrial Security (n.d.). *Professional Development* : Professional Education. Available from: http://www.asisonline.org/onllinecourses.html.

Anderson, T. (2002). Training for tense times. *Security Management Online,* March. Retrieved April 24, 2002, from: http://www.securitymanagement.com/library/001200.html.

Retrieved April 27, 2002, from: http://www.asisonline.org.

Biner, P., & Dean, R. S. (1998). Profiling the successful tele-education student. *Distance Education Report,* 1(2), 1-3.

Blanchard, K. H., & Hersey, P. (1996). Great ideas revisited [Electronic version]. *Training & Development, 50* (1), 42. Retrieved April 26, 2002, from: Academic Search Elite/EBSCO database.

Bondi, C. B. 1993). In pursuit of professionalism: The private security specialization at Pennsylvania State University. *Security Journal, 4* (1), 27-33.

Certificate in Security Management Studies (n.d.). John Jay College of Criminal Justice. Available from: http:/www.jjay.cuny.edu/securitymanagement/.

Christensen, E. W., Anakwe, U. P., & Kessler, E. H. (2001). Receptivity to distance learning: The effect of technology, reputation, constraints, and learning preferences [Electronic version]. *Journal of Research on Computing in Education, 33* (3), 263. Retrieved April 26, 2002, from: Academic Search Elite/EBSCO database.

Dalton, D. R. (2001). What should security's function be? [Electronic version]. *Security Management, 45* (7), 160. Retrieved April 10, 2002, from: Business Source Premier/EBSCO database.

Davies, S. J. (1997). Teach them well [Electronic version]. *Security Management, 41* (9), 83. Retrieved April 20, 2002, from: MasterFILE Premier/EBSCO database.

Deming, R. (1989). Mapping the discipline of security administration education. *Security Journal, 1* (1). 14-20.

Koletar (1999). Education discussed at symposium. *Security Management, 43* (9), 220 - 221.

Koletar (1999). Education discussed at symposium. [Electronic version]. *Security Management, 43* (9), 2 . Retrieved April 20, 2002, from: MasterFILE Premier/EBSCO database.

Koletar (1999). Education discussed at symposium [Electronic version]. *Security Management, 43* (9), 11. Retrieved April 20, 2002, from: MasterFILE Premier/EBSCO database

Freimuth, K. C. 1996). Checking security's customer compass [Electronic version]. *Security Management, 40* (9), 125. Retrieved April 27, 2002, from: MasterFILE Premier/EBSCO database.

Gips, M. A. (1999a). A lesson in training [Electronic version]. *Security Management, 43* (9), 29. Retrieved April 23, 2002, from: MasterFILE Premier/EBSCO database.

Gips, M. A. (1999b). A pharmacopoeia of protection [Electronic version]. *Security Management, 43* (3), 42. Retrieved April 27, 2002, from: MasterFILE Premier/EBSCO database.

Gips, M. A. (2001). Drug counterfeiting: A bitter pill [Electronic version]. *Security Management, 45* (9), 16. Retrieved April 27, 2002, from: MasterFILE Premier/EBSCO database.

Goodboe, M. E. (1995). Should security practice andragogy? [Electronic version]. *Security Management, 39* (4), 65. Retrieved April 25, 2002, from MasterFILE Premier/EBSCO database.

Grasha, A. F. (1994). A matter of style: The teacher as expert, formal authority, personal model, facilitator, and delegator [Electronic version]. *College Teaching, 42* (4), 12. Retrieved April 26, 2002, from: Academic Search Elite/EBSCO database.

Grasha, A. F., & Yangarber-Hicks, N. (2000). Integrating teaching styles and learning styles with instructional technology [Electronic version]. *College Teaching, 48* (1), 2. Retrieved April 25, 2002, from: Academic Search Elite/EBSCO database.

Harowitz, S. L. (1997). *Security's positive return*. Retrieved April 20, 2002, from: http://www.securitymanagement.com/library/ooo412.html.

HealthAce Intelligence Briefing (August 19, 2003) [Electronic version]. Retrieved August 19, 2003 from: http://www.healthace.com

Intellectual property theft may cost U.S. firms $250 billion (May 5, 1998) [Electronic version]. *Enterprise/Salt Lake City, 27* (48), 11. Retrieved April 20, 2002, from: MasterFILE Premier/EBSCO database.

Jayne, B. C. (1994). The search for an honest work force [Electronic version]. *Security Management, 38* (1), 47. Retrieved April 27, 2002, from: MasterFILE Premier/EBSCO database.

Jones, J. W. (1996). Ensuring an ethical environment [Electronic version]. *Security Management, 40* (4), 23. Retrieved April 27, 2002, from: MasterFILE Premier/EBSCO database.

Kalitka, P. F. (2000). Do they know what you know? [Electronic version]. *Security Management, 44* (9), 276. Retrieved April 27, 2002, from: MasterFILE Premier/EBSCO database.

Kane, P. (2000). People skills are paramount [Electronic version]. *Security Management, 44* (8), 31. Retrieved April 23, 2002, from: MasterFILE Premier/EBSCO database.

Kane, P. (2001). Practice what you teach [Electronic version]. *Security Management, 45* (10), 55. Retrieved April 16, 2002, from: Business Source Premier/EBSCO database.

Kaupins, G. (1997). Trainer opinions of popular corporate training methods [Electronic version]. *Journal of Education for Business, 73* (1), 5. Retrieved April 23, 2002, from: MasterFILE Premier/EBSCO database.

Koletar (2002). ASIS International 2002 Education Speaker: American Society for Industrial Security. Retrieved April 20, 2002, from: http://www.asisonline.org.

Ledoux, D. T. (1995). Exploding the myths of contract security [Electronic version]. *Security Management, 39* (1), 37. Retrieved April 27, 2002, from: MasterFILE Premier/EBSCO database.

Leedy, P. D., & Ormrod, J.E. (2001). *Practical Research: Planning and Design* (7th ed.). Upper Saddle River, NJ: Merrill/Prentice Hall.

Lieb, J. A. (1991). The introduction of a private security specialization at Penn State University. *Security Journal, 2* (1), 40-43.

Marsh, H. L. (1991). Corporate/University cooperation in security education programs: A model for professionalization of security personnel. *Security Journal, 2* (3), 180-184.

McAinsh, S. (1999). The importance of being certified [Electronic version]. *International Security Review,* 109 (Mar/Apr), 24. Retrieved April 20, 2002, from: MasterFILE Premier/EBSCO database.

Millwee, S. C. (1999). How can security get inside the door? [Electronic version]. *Security Management, 43* (12), 118. Retrieved April 10, 2002, from: Business Source Premier/EBSCO database.

Mission (n.d.). John Jay College of Criminal Justice, Criminal Justice Center. Available from: http://www.jjay.cuny.edu/centersInstitutes/criminalJusticeCenter.

Morash, M., Vitoratos, B., & O'Connell, T. (n.d.). *Workplace violence programs in leading edge companies*. East Lansing, MI: School of Criminal Justice, Michigan State University. Retrieved April 20, 2002, from: http:/www.cj.mus.edu/~outreach/security/violtsum.html.

Morley, H. N., Vogel, R. E., & Huegel, B. L. (1993). The higher education dilemma for the private security professional: Delivery methodologies and core curriculum from the practitioner's perspective. *Security Journal, 4* (3), 122-127.

Nalla, M. K., Christian, K. E., Morash, M. A., & Schram, P. J. (1995). Practitioners' perceptions of graduate curriculum in security education. *Security Journal, 6,* 93-99.

Nichter, D. A. (2001). Is your VIP protected? [Electronic version]. *Security Management, 45* (5), 42. Retrieved April 20, 2002, from: MasterFILE Premier/EBSCO database.

Patton, M. Q. (1990). *Qualitative Evaluation and Research Methods*. (2nd ed.) New Park, CA: Sage Publications.

Roth, D. (2001). Someone to watch over us [Electronic version]. *Fortune, 144* (12), 216. Retrieved April 20, 2002, from: MasterFILE Premier/EBSCO database.

Rothke, B. (2001). Corporate espionage and what can be done to prevent it [Electronic version]. *Information Systems Security, 10* (5), 10. Retrieved April 10, 2002, from: MasterFILE Premier/EBSCO database.

Security Management Institute Presents the Forty-Seventh Professional Security Management *Course* (2002). John Jay College of Criminal Justice. Available from: http://www.jjay.cuny.edu/centersInstitutes/criminalJusticeCenter/course/secur_PSM.htm.

Simonsen, C. E., & Nelson, R.G. (1994). Searching for standards: The task of legislative, association, and public action—the state of Washington's experience. *Security Journal, 5* (4), 186-198.

Transportation Security Administration (TSA)- History- P.L. 107-1771 (2001) [Electronic version]. Retrieved March 6, 2003 from: http://www.tsa.gov/interweb/assetlibrary/AviationandTransportationSecurityActATSAPubliclaw 107-1771.pdf.

Vaill, P. B. (1996). *Learning as a way of being: strategies for survival in a world of permanent white water*. San Francisco, CA: Jossey-Bass. P.96

World Institute for Security Enhancement (2001). Understanding security technologies(Electronic version). Program description. Retrieved April 20, 2002, from: http://www.worldinstitute.org/wise/courses/iss/iss.html.

APPENDICES

Appendix A

Certification of Completion from National Institutes of Health

Completion Certificate

This is to certify that

Kevin Schatzle

has completed the **Human Participants Protection Education for Research Teams** online course, sponsored by the National Institutes of Health (NIH), on 01/25/2002.

This course included the following:

- key historical events and current issues that impact guidelines and legislation on human participant protection in research.
- ethical principles and guidelines that should assist in resolving the ethical issues inherent in the conduct of research with human participants.
- the use of key ethical principles and federal regulations to protect human participants at various stages in the research process.
- a description of guidelines for the protection of special populations in research.
- a definition of informed consent and components necessary for a valid consent.
- a description of the role of the IRB in the research process.
- the roles, responsibilities, and interactions of federal agencies, institutions, and researchers in conducting research with human participants.

National Institutes of Health
http://www.nih.gov

Appendix B

Letter of Solicitation

April, 2003

Dear Colleague:

My name is Kevin P. Schatzle and I am a doctoral candidate at Seton Hall University in the Department of Educational Administration and Supervision.

I am presently working on my dissertation by exploring the elements of a successful training model for security personnel as perceived by Global Security Heads working in the ethical pharmaceutical industry. The study is qualitative in nature and employs the interview process to gather data. In addition, a brief quantitative component will be used to collect demographic data. The interview process will take approximately one-half hour to complete. The demographic data collection will take less than ten minutes. Candidates for the qualitative interview process will be asked nine, open ended questions designed to probe the respondent's perceptions of the elements necessary to form a successful training model.

The purpose of this letter is to invite your participation in this study. Participation is voluntary and you may discontinue participation at anytime. Individuals working in the capacity of Global Heads of Corporate Security have been selected as my population of interest.

All participants shall remain anonymous with regard to any written or verbal presentation of the study.

All data collected for this study will be secured in locked combination safes contained in my office.

This project has been reviewed and approved by the Seton Hall University Institutional Review Board for Human Subjects Research. The IRB believes that the research procedures adequately safeguard the subject's privacy, welfare, civil liberties, and rights. The Chairperson of the IRB may be reached through the Office of Grants and Research Services. The telephone number of the Office is (973) 275-2974.

I am requesting that you complete the attached documents and return them to me within two weeks in order that data may be analyzed in a timely manner. In addition to the Demographic Survey Form, (DSF), and the Informed Consent Form, I have enclosed a self-addressed, stamped envelope to facilitate your response. Your return of the completed documents will indicate your consent to participate in the study. Your name

should not appear on any document other than the Informed Consent Form. Completing the DSF and Informed Consent Form should take no more than ten minutes.

Thank you in advance for your cooperation in this project. The results of this study, in aggregate form, will be offered and made available, upon request, to all participants.

Very truly yours,

Kevin P. Schatzle

Kevin P. Schatzle
Director Corporate Security
Office # 862-778-6301

Appendix C

Informed Consent

SETON HALL UNIVERSITY
1 8 5 6

INFORMED CONSENT FORM

(Format pursuant to Seton Hall University IRB requirements.)

To: Kevin P. Schatzle

Affiliation:

I, agree to be a voluntary participant in a dissertation project being conducted by Kevin P. Schatzle, who is a doctoral candidate at Seton Hall University in the Department of Educational Administration and Supervision.

Purpose of the Research:
The research project is entitled "The Elements of a Successful Training Model as Perceived by Global Heads of Corporate Security Working in the Ethical Pharmaceutical Industry." This study explores the perceptions of individuals working as global heads of corporate security.

Description of Procedures:
I agree to devote approximately one-half hour of my time as a participant in the interview process at a time and date mutually agreeable to both parties. I am aware that the interview will consist of nine open-ended questions designed to probe my perceptions of the elements necessary for a successful training program for security personnel.

Statement of Voluntary Participation:
I understand that I may be selected to participate in an interview with the researcher, that my participation is completely voluntary and that I may withdraw from participation at any time.

Anonymity:
I also understand that any information I provide can be reviewed by me and shall be reported anonymously in any written or verbal presentation of the dissertation. My anonymity will be secured by use of a coding system.

Data Security:
Data that is collected will be secured in locked combination safes kept in an alarmed office environment.

Confidentiality:
All personal information collected will be treated confidentially and will be accessed only by the researcher.

College of Education and Human Services
Department of Education Leadership, Management and Policy
(Formerly Department of Educational Administration and Supervision)
Tel. 973.761.9397
400 South Orange Avenue • South Orange, New Jersey 07079-2685

SETON HALL UNIVERSITY
1856

No Anticipated Risks:
I understand that there are no anticipated risks associated with my participation in this study.

Benefits to Subjects or Others:
I understand that my participation in this study may aid security practitioners in accessing the necessary elements for successful training of security personnel.

No Undue Stress:
I understand that I will not be placed under any undue stress during my participation.

No Alternative Procedures:
I understand that there are no alternative procedures or courses of treatment involved in this study.

Researcher Contact Information:
I can contact researcher, Kevin P. Schatzle, at telephone number 862-778-6301 or 180 Park Avenue, Building 105-Room 3E191, Florham Park, New Jersey, 07932.

Audio Tape Handling:
I understand that the interview will be tape recorded for reference purposes only, and that statements made during this interview may be included in the text of the dissertation. In addition, any portion of the taped session or all of it will be destroyed upon my request. Data collected will be kept for three years after the completion of the study. I understand that the results of the study in aggregate form will be made available to me upon request.

Copy of Informed Consent:
I understand that I will be given a copy of this Informed Consent Form after it is signed by me.

APPROVED
MAY 13 2003
IRB
SETON HALL UNIVERSITY

College of Education and Human Services
Department of Education Leadership, Management and Policy
(Formerly Department of Educational Administration and Supervision)
Tel. 973.761.9397
400 South Orange Avenue • South Orange, New Jersey 07079-2685

SETON HALL UNIVERSITY
1 8 5 6

Interview Preference:

I would prefer an interview: In person ____
Telephone ____
( ) -

Interview Preferences Dates: _____
Days: _____
Times: _____
Location: _____

IRB Statement:
This project has been reviewed and approved by the Seton Hall University Institutional Review Board (IRB) for Human Subjects Research. The IRB believes that the research procedures adequately safeguard the subject's privacy, welfare, civil liberties, and rights. The Chairperson of the IRB may be reached through the Office of Grants and Research Services. The telephone number of the Office is 973-275-2974.

I have read the material above, and any questions I asked have been answered to my satisfaction. I agree to participate in this activity, realizing that I may withdraw without prejudice at any time.

_____ _____
Subject or Authorized Representative Date

APPROVED
MAY 13 2003
IRB
SETON HALL UNIVERSITY

College of Education and Human Services
Department of Education Leadership, Management and Policy
(Formerly Department of Educational Administration and Supervision)
Tel. 973.761.9397
400 South Orange Avenue • South Orange, New Jersey 07079-2685

Appendix D

Demographic Survey Form

Demographic Survey Form

Age:

Race:

Experience:

Supervisory Years:

Education Level:

Researcher: Kevin P. Schatzle

Appendix E

Key Elements Matrix

Researcher: Kevin P. Schatzle

Title: What are the Elements of a Successful Training Model as Perceived by Global Corporate Security Heads Working in the Ethical Pharmaceutical Industry?

Key Elements from Respondents

	Respondent 1	Respondent 2	Respondent 3	Respondent 4	Respondent 5	Respondent 6	Respondent 7	Respondent 8	Respondent 9
What is your definition of successful security training?	Impact the business function	Relevant & cost effective skills, leadership, team building	Customer service include contract staff	Professional development include professional staff only	High potential individuals. Business issues include professional staff only	Be different depending on level done or a continuum	Results oriented	Communicate key messages should shape culture. Convey policy	Standards be revisited. Two fold process: Feel good & effective action
What do you perceive to be the ideal best practices for a global corporate security training program?	Regional model best. Latitude given to differences in regions	Train in one methodology	Customer service focused training	Understand the business. Incorporate language skills	Formalized training program. Blend security with business	Management and leadership courses	Understand the business	Use various techniques. Engage in projects	Networking
What impact does budget have on training security personnel?	Has big impact	Monumental	Important	Significant impact	Big	Very big	Big	Huge	Significant

Researcher: Kevin P. Schatzle

Title: What are the Elements of a Successful Training Model as Perceived by Global Corporate Security Heads Working in the Ethical Pharmaceutical Industry?

Key Elements from Respondents

How does the placement within the organization effect training security personnel?	Very, very important	Has a lot to do with success	Big, could have a positive or negative effect depending on person	Important	Important	Key	Important as placement could be effected considerably	Key element	Very important
What do you perceive to be barriers to setting up training for security personnel?	Administration of budgets is key. Time	Work load, lack of time	Administration of budget	Misplacement of the organization	Lack of understanding security function	Must have senior management support proper placement	Lack of planning, not understanding importance of training	Training not being viewed is core activity	Proper reporting relationship
What practices are ineffective in setting up successfully fun security department s>	Informal not directed at corporate culture	Boiler plate training	Training not tailored to culture and environment	Training that does not support business unit	training not adapted to business unit	Boiler plate not relevant to actual job	Not using varied techniques	Not specific to business	Benchmarking or lack thereof

Researcher: Kevin P. Schatzle

Title: What are the Elements of a Successful Training Model as Perceived by Global Corporate Security Heads Working in the Ethical Pharmaceutical Industry?

Key Elements from Respondents

How does the training of security personnel for ethical pharmaceutical industry differ from the training of other security personnel?	Not significantly different	Training does not differ. Skill sets are the same	Some training may be different	Training should not differ	Some industries are a little different but not much	Training more broader and complex	There is a difference	There is a difference	Does not know. Not in position to comment

Researcher: Kevin P. Schatzle

Title: What are the Elements of a Successful Training Model as Perceived by Global Corporate Security Heads Working in the Ethical Pharmaceutical Industry?

Key Elements from Respondents

	Respondent 1	Respondent 2	Respondent 3	Respondent 4	Respondent 5	Respondent 6	Respondent 7	Respondent 8	Respondent 9
What is your definition of successful security training?	Impact the business function	Relevant & cost effective skills, leadership, team building	Customer service include contract staff	Professional development include professional staff only	High potential individuals. Business issues include professional staff only	Be different depending on level done or a continuum	Results oriented	Communicate key messages should shape culture. Convey policy	Standards be revisited. Two fold process: Feel good & effective action
What do you perceive to be the ideal best practices for a global corporate security training program?	Regional model best. Latitude given to differences in regions	Train in one methodology	Customer service focused training	Understand the business. Incorporate language skills	Formalized training program. Blend security with business	Management and leadership courses	Understand the business	Use various techniques. Engage in projects	Networking
What impact does budget have on training security personnel?	Has big impact	Monumental	Important	Significant impact	Big	Very big	Big	Huge	Significant