ASIS INTERNATIONAL
Advancing Security Worldwide™

# Proceedings of the 2002 Academic/ Practitioner Symposium

Held on the Campus of
The University of Cincinnati
Cincinnati, Ohio
May 29-31, 2002

Proceedings of the 2002 Academic/Practitioner Symposium

ASIS


# Proceedings of the 2002 Academic/ Practitioner Symposium

**HELD ON THE CAMPUS OF**

**THE UNIVERSITY OF CINCINNATI**
**CINCINNATI, OHIO**
**MAY 29-31, 2002**

Cover photo by Lisa Ventre, University of Cincinnati

# Table Of Contents

**Appendix**

# INTRODUCTION TO THE 2002 SYMPOSIUM PROCEEDINGS

David H. Gilmore, CPP
Chairman, ASIS Academic/Practitioner Symposium

The ASIS Academic/Practitioner Symposium is a forum for promoting continuing communication and dialogue between security academicians and security practitioners. Prior to 1997, this forum did not exist at the national level. Since then, selected academicians and practitioners from all over the United States and Great Britain have been invited to come together annually for an intensive, multi-day program of plenary sessions, guest speakers, and breakout sessions. In each case, the purpose has been to bring to bear the experience and expertise of the participants to gain a consensus regarding the field of security and to develop educational programs at the baccalaureate and graduate levels that respond to cutting-edge issues in security.

Each year, participants have endeavored to build upon the work done at previous Symposiums. As a result of the first five Symposiums, the participants have, among other products and initiatives:

- Developed the instructor course outline for an introductory course in Business and Organizational Security Management for business students. The groundwork was laid in the first Symposium.

- Developed the instructor course outline for an upper level undergraduate course in Risk Management for Security Professionals. The preliminary work was done at the second Symposium.

- Initiated an on-going Security Education and Career Study designed to gather data on entry level security management positions and the factors used in filling those positions. This study emerged from the work done on-site during the third Symposium.

- Developed a consensus-based model containing the core elements of the security field. The model was developed as the result of a pre-arrival survey for the third Symposium, on-site work at the third Symposium and a pre-arrival survey for the fourth Symposium.

- Developed undergraduate and graduate curriculum models, based on the security model that was previously developed through the Symposium process. These curriculum models were created at the fourth Symposium.

- Developed preliminary qualitative and quantitative criteria that could potentially be used by ASIS in accrediting undergraduate and graduate security education programs. These criteria were developed at the fifth Symposium.

These Proceedings reflect the products of the 6th Annual Symposium that was held at the University of Cincinnati in May 2002. A lot had happened since the 2001 Symposium, held in August 2001 at the University of Maryland University College. The attacks of September 11 and the anthrax incidents put security into the spotlight and increased the public's awareness of security. Many would agree those events also increased the public's expectations of security. The public expected law enforcement and public and private security to protect them from a widening range of threats. Homeland security, aviation security, and protection against weapons of mass destruction (WMD) took on a priority and an urgency that we hadn't seen before. Those of us involved with security education need to ensure that we are developing courses and curricula that respond to the needs, requirements, and expectations that derive from this new environment in which we find ourselves. The 2002 Symposium provided an opportunity to determine if we were doing that.

In Cincinnati, we defined those core competencies that we expect individuals to have when they successfully complete undergraduate and graduate security education programs. The identification of core competencies is a necessary part of the accreditation process. In addition, the development of core competencies enabled us to validate the curriculum models that were developed in Norman, Oklahoma, at the 2000 Symposium.

All of the Symposiums and all of the products that have emerged from them have been predicated on the following precepts that set apart what we are doing from the efforts of those who have gone before:

- That security is a business function and is not a subset or spin-off of the criminal justice system.

- That Business and Organizational Security Management is a discrete field of academic study, separate and apart from criminal justice and police science.

- That within the academic community programs in Business and Organizational Security Management are ideally situated within the college or school of business administration, rather than in the criminal justice department.

- That if such an organizational alignment is not feasible, programs in Business and Organizational Security Management should, at the least, be interdisciplinary and should incorporateappropriate business theory and concepts.

Since 1997, the ASIS Academic/Practitioner Symposium has been, and continues to be, a forum in which dedicated and determined security academicians and practitioners give of their time, energy, experience and expertise to explore and debate pressing issues in security education. We use this important forum to look not only at where we are in security education, but also where we need to go in order to respond to the challenges confronting security education in the 21st Century.

# Setting The Stage For The Symposium

# Day 1

## Setting the Stage for the Task Groups

### Plenary Session #1: Welcoming Remarks and Symposium Overview

**David H. Gilmore, CPP**
Chairman, Academic/Practitioner Symposium
Moderator

David Gilmore welcomed the participants to the 6th Annual ASIS Academic/ Practitioner Symposium. After thanking various individuals who helped organize and run the Symposium, he also introduced the leaders for this year's breakout groups: Dr. Jim McClanahan and Mike Magill for the undergraduate groups, and Kevin Peterson, CPP, and Dr. Eva Vincze for the graduates.

Breaking slightly from past routine, Gilmore next introduced Daniel Kropp, CPP, Vice President, and President-elect of ASIS International .

**Daniel Kropp, CPP**
President-Elect of ASIS International

In his opening remarks, Daniel Kropp stated that "much credit for the direction we'll be taking next year" goes to the participants of these symposia. He stressed that this sustained effort has been possible because the organizers and participants have understood from the start that they would "be in it for the "long haul."

Likewise, ASIS has had its long-range strategic plan, which looks at not only the following year, but also where ASIS would like to be in the next five, ten, and twenty years. A Strategic Planning Committee reviews the plan every year and "tweaks (it) as necessary" but members have remained true to the plan as initially written. Kropp himself, a member of the committee for the past four years, shared that "I have bought into it. I have invested into it. I believe that what we are doing is the right thing." President elect Kropp stated that there "won't be a whole lot of sexy change" next year. Rather, he anticipates "you're going to see the course moving ahead the way we have planned the course to go."

He continued by describing six critical initiatives that the Strategic Planning Committee identified for next year.

1. "The first one was thrust upon us…homeland security." At the moment, ASIS is not a "completely invested partner" but according to Kropp "…they know we are here. They believe in our strength. They believe in our commitment and dedication and they have guaranteed us that we will have a place…"

2. Marketing—the effort will focus on not only ASIS, but also on the security industry itself. Kropp suggested that "we never took the opportunity to step out and let business and government know what we know." But "they are now ready to listen. They are listening." He believes the opportunity is there and that the industry should take advantage of it before the window closes again.

3. Identify volunteer leaders. Kropp qualified this by explaining the organization needs to "identify the issues that motivate or de-motivate volunteer leaders, especially at the chapter level. The last three initiatives are ones that Kropp believes are "near and dear to this group."

4. First, the Society would be continuing the Standards and Guidelines Commission. Don Walker, a past president of the Society, and Chad Callaghan, a former board member, are co-chairing the Commission. Kropp also announced that while "it hasn't hit the streets yet" the group has approved a Risk Assessment Guideline. While ASIS is not licensed to "write standards in the legal term" the guideline does have ASIS's blessing on how to conduct risk assessments. The Commission is also near completing the standards and guidelines that should be associated with the position of "Chief Security Officer." Kropp referred the audience to an article in the *New York Times*, where "chief security officer" appears to be the "title of the future." Accordingly, Kropp stated, "if someone doesn't come in and say this is really what you need to know and what you need to be for this position," in five years there will be such disparity that no one will really know what a chief security officer is. In addition, the Commission is working on other standards and guidelines and will release them as they are completed.

5. The final two initiatives deal with the Foundation and with education and research. Kropp stated that while there has been a strong emphasis on the "body of knowledge…and giving our people an academic foundation," efforts on conducting research have been lacking. Therefore, ASIS will be concentrating more on "academic research in the security industry."

6. Lastly, but the one where "this group really comes in," is the continuing effort and focus on "educating business people about security and educating security people about business." Kropp emphasized that they need the "future CFOs and CEOs to understand what security is all about."

Kropp concluded his remarks by telling the group how he will be the first ASIS president "who doesn't have the law enforcement or government or criminal justice background in any way, shape, or form." He believes that in the near-term, the Board of Directors and future presidents will "resemble more our historical presidents." But he looks forward to the day, perhaps 20 years from now, when he reads in *Security Management* magazine about an ASIS president who says, "'I majored in security management … I always wanted to work in this industry and now I am here.'"

In this same vein, he reinforced the importance of their work to the group. And although "some of the impact won't really be felt in our Society for 20 years," Kropp thanked them in advance for all their effort, time, and personal sacrifices in helping ASIS.

Gilmore took advantage of a short interval between presentations to open the floor for a few questions.

**Question/Comment:**

Richard Hollinger from the University of Florida has been conducting research over the years for the National Retail Foundation into retail theft and it "has had its struggles." The questioner wondered whether ASIS would be interested in supporting this type of research.

**Answer:** Kropp briefly answered that while he hasn't approached the Board about this, it has been something he's thought about, with the intention of reaching out to companies for organizational and financial support.

Dr. Robert McCrie, CPP, added that he had heard Dr. Hollinger himself state that since no one supported the research, it didn't have the value it should have. McCrie suggested that if the members of an industry, in this case the retailers, "drive this issue and believe that that type of research needs to be done, our Foundation would support it.

**Question/Comment:**

How has the name change been received?

**Answer:** In January 2001, the Board of Directors voted to change the name of the society to ASIS International—they have done away with American Society for Industrial Security. While some believe that the name was changed "to placate our international members," this was not the case. In fact, over the years, the Society had "heard as many grumbles…about the word industrial" as about American. The new marketing for the name change will roll out the last quarter of 2002.

At this point, Gilmore introduced Dr. Lawrence Johnson, Dean of the College of Education of the host University of Cincinnati, who welcomed the attendees to the University and encouraged them to explore the sights, sounds, and restaurants of Cincinnati.

**Lawrence J. Johnson, Ph. D.**
Dean, College of Education, University of Cincinnati

### Welcoming Remarks

Johnson expressed his pride in the university's criminal justice program and wondered if they thought it odd that it should reside in the College of Education. This reflects his personal commitment to building strong communities and his belief that "you cannot have a healthy community without a good school system, without great recreational opportunities, without security, and we really have to get to the place where we're all working together to do this and make safe environments." He welcomed them once again and turned the podium back to Gilmore**.**

Gilmore moved forward with an overview of the Symposium, mainly for the benefit of attendees who had not attended any of the prior symposia.

**David H. Gilmore, CPP**
Chairman, Academic/Practitioner Symposium
Moderator

## Symposium Overview

"The goal all along of the Symposium is communication." With this statement, Gilmore described the ongoing process they have been using to achieve the underlying purpose of the Symposium: to establish the idea—in the minds of both the academic and business communities—that security is a business function, and not an element of criminal justice.

Indeed, Gilmore stressed that security is not only a business function, but that it is more—a "distinct field of study." Accordingly, ASIS International has had two goals—"…educate security people about business…(and)…educate other business students beyond security about the world of security."

While the strategic academic goals remain unchanged, one of the objectives for this year would be to validate the curriculum models developed at the 2000 symposium held in Norman, Oklahoma. While he believes that ASIS "is the appropriate one to be an accrediting body for security education programs," Gilmore stated that they would save this topic for a later time.

In the meantime, he provided the group with a short recap of what was accomplished at the previous symposia:

- Tentative introductory courses—the idea being to develop a course in business security for business students.

- Description of the security field—an 18-point "security model." Gilmore acknowledged that it was "like a Christmas tree—people kept hanging stuff on it," and that at some point in the future, it would be reviewed and probably condensed to reflect "the core elements of security."

- At two other symposia, the groups developed the foundation for the current Body of Knowledge taskforce and the Security Education and Career study. Referring back to the Oklahoma symposium, Gilmore described how the groups developed two curriculum models—an 18-credit hour concentration or "minor in Business and Organizational Security Management" for an undergraduate program, and a 21-credit hour program for the graduate level. Participants were asked to develop a title, catalog description, objectives, and rationale for each course.

- Last year's symposium focused on accreditation. In examining this topic, attendees concentrated more on the structure of the program, less on course content issues.

This year, participants had three goals.

1. Develop those core competencies or program objectives that the individuals coming out of both the undergraduate and graduate programs should have. In other words, "what is it that we want them to know? What is it that we want them to be able to do at the end of the program?"

   Gilmore further explained that "right now, we do not have a consensus in the security education field as to what graduates ought to know…" By way of example, he pointed out that no matter where people get their degree in accounting, there is a common expectation of what they should know and what they should be capable of. This expectation does not currently exist for the field of security education.

2. Validate these core competencies against the curriculum models developed in Oklahoma.

3. Validate the curriculum models in light of the events of September 11, 2001.

When developing the core competencies, participants were instructed that they should "look at this from the eyes of the prospective employer." Gilmore shared that in his opinion, the reason why so many security education programs fail is because they are developed without considering the ultimate end user—the employer.

Accordingly, the practitioners attending this year's event would play a vital role in providing the employers' point of view. This dialogue would be of tremendous help to the academicians who "would say, okay, this is the best way to deliver" it.

Gilmore requested that the groups limit the number of core competencies to twelve, mainly because it would be rather unrealistic for a program to achieve any more than that.

He made two other requests of the groups:

- For those working on the undergraduate groups, they should assume that for the foreseeable future, the student would not be pursuing a graduate degree.

- As for those members of the graduate groups, they should assume the student does not have an undergraduate degree in security.

He reiterated that communication—the exchange of ideas, perspectives, and experience—was the goal of the symposium.

Once again, an interval between speakers permitted a brief question and answer session.

**Question/Comment:**

In developing the core competencies, should we address the vehicles for testing as well?

**Answer:** While time will probably not permit them to address this aspect, if they have time they are free to pursue it. In reality, they expect that this will be a project in itself.

**Question/Comment:**

Regarding the perspective of the employer, which employer? There is the industrial employer and then there is the security industry itself. The industrial employer would seem to require a specialist, while the security industry would have more use for generalists. How do we resolve this?

**Answer:** While there isn't time to address this question in the depth it deserves, Kropp answered that the programs would have to somehow address the needs of all employers. He did think, however, that there shouldn't be a "chocolate and vanilla" version where undergraduates would have a choice of one program that is proprietary and one that is for contract security.

**Question/Comment:**

Can the CPP program be used to validate the security education program?

**Answer:** No, because the CPP currently is not an academically based program. And in reality, someone coming out of a degreed program might not necessarily be able to pass the CPP exam because they wouldn't know the "nuts and bolts" of physical security.

**Question/Comment:**

Wouldn't this be confusing to the business community?

**Answer:** Quite possibly, but Gilmore pointed out that if someone gets an accounting degree, that doesn't necessarily qualify him or her for a CPA. If one gets a law degree, he's not automatically able to pass the bar exam.

Another speaker brings up the possible dilemma an employer would face if he had to choose between one candidate who had a CPP and another candidate with a major in security management.

Time runs out for further discussion on this topic and the group takes a short break before the presentation from John Tippit, CPP**.**

# TASK BACKGROUND AND PARAMETERS

During the 2000 Symposium in Norman, Oklahoma, we developed undergraduate and graduate curriculum models in Business and Organizational Security Management, summaries of which are attached. The tasks and parameters at that Symposium were as follows:

- **Undergraduate Groups:**

Develop six courses, [18 credits] to form the basis of a minor, area of concentration or option in Business and Organizational Security Management.

- **Graduate Groups:**

1. Develop seven courses [21 credits] to form the core for a 36-credit degree in Business and Organizational Security Management.

2. Assume that degree candidates do not have an undergraduate degree in security management.

- **All Groups:**

1. Use the revised security model [attached for your reference]as a baseline in developing courses. Each core element should be accounted for in one of the courses that is developed unless the group determines the core element is not appropriate for study at that level.

2. Prepare a course worksheet for each proposed course, to include:

   a. Course title
   b. Catalog description
   c. Course objectives
   d. Rationale for course

3. ASIS has developed an instructor outline for a three-credit upper level undergraduate course in Risk Management. Each group will be provided with a summary of that course outline for the group's consideration.

4. Assume that the undergraduate and graduate degrees in Business and Organizational Security Management will be offered through an institution's college/school of business administration.

5. If time permits after you have completed the primary task outlined above, identify those non-security business courses that you feel should be part of a degree program in Busi ness and Organizational Security Management. Each group should identify not more than three such courses. You need only develop the name and catalog description for each course.

During last year's Symposium at College Park, Maryland, we developed proposed criteria for use by ASIS in the future accreditation of security education programs. The tasks and parameters at that Symposium were as follows:

- **Undergraduate Groups**—develop qualitative and quantitative criteria for the accreditation of undergraduate security education programs. For purposes of the task assignment, assume the institution has no graduate security education program.

- **Graduate Groups**—develop qualitative and quantitative criteria for the accreditation of graduate security education programs. For purposes of the task assignment, assume the institution has no undergraduate security education program.

- **All Groups**—

1. The primary objective of ASIS accreditation will be to promote ASIS's business security initiative. That initiative is predicated on the following concepts:

   a. That security is a business function and is not a subset or spin-off of the criminal justice system.

   b That Business and Organizational Security Management is a distinct field of academic study, separate and apart from criminal justice, administration of justice, criminology and police science.

   c. That within the academic community, Business and Organizational Security Management curricula should be interdisciplinary and should include appropriate course work in business concepts, methods, and practices in addition to security-specific courses.

2. ASIS will be the accrediting body and there will be no third party involvement in the accrediting process.

3. ASIS will establish the accreditation policies, procedures, and criteria. Accordingly, the output of this Symposium will be advisory in nature.

4. ASIS accreditation will be limited to four-year and graduate programs at institutions that are fully accredited by a national or regional accrediting body. Community colleges, junior colleges and other two-year programs will not be eligible for ASIS accreditation.

5. ASIS accreditation will be limited to security education programs with a clearly-defined major, minor, area of concentration, or option in business and organizational security management or a related security field, (i.e., asset protection or loss prevention).

6. The 18 point security model and the undergraduate and graduate curriculum models developed by previous Symposiums are to be used as baselines for any criteria related to the security-specific part of the curriculum.

This year, as in the past, we will draw upon the work done in previous Symposiums. In addition, following past practice, you have been divided into undergraduate and graduate breakout groups.

As we are all aware, the attacks of September 11 and the subsequent anthrax incidents have created an emphasis on homeland security, aviation security, and protection against weapons of mass destruction (WMD) that we haven't seen before. Those of us involved with security education need to ensure that we are developing courses and curricula that respond to the needs, requirements and expectations that derive from this new environment in which we find ourselves.

Therefore, in the context of that new security environment, the task for each group is to define those core competencies/program outcomes that we expect students to have when they successfully complete baccalaureate and graduate security education programs.

In developing these competencies/outcomes, groups should address the following question: What should graduates know and what should they be able to do when they complete the program, whether it be in New York, Kentucky, Arizona or Washington, DC? To ensure a consistent approach among groups, this question should address needs, requirements and expectations from the perspective of the organization that currently employs or may potentially employ the program graduate, and **not** from the perspective of a student enrolled in the program or an academician presenting the program.

Not only is the development of core competencies/program outcomes a necessary part of the accreditation process but it will also enable us to validate the curriculum models that were developed in Norman at the 2000 Symposium.

All groups should validate the Norman curriculum models from the following perspectives:

- Do the courses that were identified in 2000 correlate with the core competencies/ program outcomes that you're developing here in Cincinnati?

- Do the courses that were identified in 2000 respond to the challenges resulting from the events on and after September 11, 2001?

The additional parameters within which these tasks are to be accomplished are as follows:

- The number of core competencies/program outcomes will be limited to 12 at the undergraduate level and 12 at the graduate level. Some core competencies may apply to both undergraduate and graduate programs. In those instances, the breakout group should annotate the core competency as such.

- Undergraduate groups should assume that degree candidates will **not** pursue a graduate degree in Business and Organizational Security Management in the foreseeable future.

- Graduate groups should assume that degree candidates do **not** have an undergraduate degree in security management.

- In validating or revising the Norman curriculum models, groups will adhere to the 2000 Symposium task parameters indicated above, as they relate to the number of courses and the overall scope of the program.

If you disagree with any of these parameters, feel free to note the disagreement when making your group report. However, please **do not** change any of the parameters.

# Security Model

This model, developed by consensus by past Symposium participants, identifies 18 core elements that constitute the field of security, as follows:

Physical Security

Personnel Security

Information Systems Security

Investigations

Loss Prevention

Risk Management

Legal Aspects

Emergency/Contingency Planning

Fire Protection

Crisis Management

Disaster Management

Counterterrorism

Competitive Intelligence

Executive Protection

Violence in the Workplace

Crime Prevention [General]

Crime Prevention through Environmental Design [CPTED]

Security Architecture and Engineering

**John D. Tippit, CPP**
**President, The Tippit Group**

## Research to Support the Education and Training of the Professional Security Practitioner

Tippit placed his within the context of another research project currently underway.

He began with an explanation of the Joint Security Training Consortium and its mission. The Joint Security Training Consortium was established as a result of an Intelligence Community and Department of Defense program decision memorandum in 2001. The Consortium's purpose is to strengthen skills and career development for security professionals. Tippit stressed that this focused strictly on professionals, and therefore, did not address job categories such as guards, administrative positions, or police officers. This focus was expressly dictated by Congress that funded this program.

The Consortium was charged to develop and implement policy for core security training and professional development. Furthermore, they were to evaluate and construct security certification programs to be used by not only the intelligence and the Department of Defense communities, but also by the industrial companies that support those communities.

One of the Consortium's objectives—and this is what ties in with this year's Symposium—is that they were to concentrate on the outcomes of the training, on the core competencies. In other words, "if you learn the principles and precepts and practices of physical security as a discipline, it shouldn't make any difference whether you learn it at a university, in the commercial sector or the private sector or whether you learn it at the new CIA University or the DIA University or the DoD University system. It shouldn't make any difference."

Tippit explained that one of the first problems they observed was that when they took a practitioner out of his or her particular discipline (industry), they experienced a loss of confidence in their ability to perform in the new environment and invariably required retraining.

By way of further comparison, Tippit shared that in the past ten years there have been several top-level reviews of the national security architecture. These reviews, including a review of significant security failings going back 25 years, isolated some common elements. According to Tippit, "several of these reviews drilled down into the performance issues of security practitioners." In many cases, core security training requirements were poorly articulated; the disciplines were ill defined. There was no common policy. Not only was there a "lack of programmatic approach" but also many times, people would "set a requirement but it would be waived, disregarded or just simply not even considered…"

Tippit also drew attention to a common attitude in the security profession that once someone finishes his or her training, they stop there and consider themselves "a competent complete practitioner for the rest of your life." Tippit pointed out that this is in direct contrast to just about every other "learned profession that recognizes when you complete your education and training

you are qualified at best for an entry level position…" To advance in these professions, individuals understand that they need to acquire even more education or training.

Accordingly, Tippit explained that it became readily apparent to the Consortium that they needed to "define a security workforce that possesses the skills necessary to meet the challenges of the 21st century."

In many ways, the skills and solutions already exist today, but as Tippit remarked, "one of the first things practitioners have to learn is that we don't have the ability nor the desire to protect every asset at the same level all the time everywhere. That pre-supposes a level of control that most folks believe is unachievable and not only unachievable, but undesirable." Indeed, the concept of control and its benefits are often illusory. For example, Tippit noted that although the old Soviet Union devoted much time, money and energy into controlling the behavior of its people, not only did it break them financially, but it also experienced as high a crime rate as any democracy.

Since control didn't appear to be the answer, Tippit and his group set about developing hard data rather than "battering around a lot of personal opinions…" They have several concurrent projects underway:

- Develop a baseline definition of the security profession. In particular, "define the profession by distinct discipline, by function within those disciplines, and by task."

- Create a baseline catalog of training providers. This anticipates a future project where they hope to develop some sort of protocol for certifying or evaluating current courses.

- Compile of glossary of key security terms and definitions. This glossary is now up to 400 pages; furthermore, Tippit underscored that "we are not creating any new definitions. We are just pulling together everything that has been defined to date." While other professions have long ago resolved this problem of a common vocabulary, according to Tippit, "until it is done in this profession the concept of common training and reciprocal core competencies is going to be problematic."

- Establish "the priorities for the professional development program." This project involves examining current well-established professional development programs, specifically their core elements, their stated objectives, and how they achieve their objectives. Tippit referred to a previous study he conducted for the DoD. In this study, they first looked at every federal law or issuance that mandated security training. In all, they found 167 federal laws, presidential directives, etc., that mandated some form of training. Through the use of gap analysis, they discovered that two-thirds of the mandated training elements were not being conducted.

- Develop a baseline model training policy. Because the Consortium has no operational mission, when they complete this model, they will simply distribute it to all 32 executive agencies of the federal government. At that point, individual agencies can pick and choose elements from the policy as they wish.

At this point, Tippit came full circle back to the discussion of his current project that is attempting to arrive at a definition of the security profession. Tippit noted that in their work, they had looked at what ASIS had been doing in the symposia (specifically Oklahoma); had interviewed a European group that operates within NATO; and had talked to representatives from other countries as well, including Australia and Canada. In essence, they identified three levels of practitioners:

1. The expert or senior manager, "…those people who write standards or procedures who make a decision on levels of security.

2. The "generalist" who they find is "competent in at least four of the seven disciplines identified."

3. The entry-level specialist.

However, the problem emerged that within these levels, there was no consensus on definitions of functional roles.

Therefore, Tippit explained that "…what we tried to do is acknowledge some of the closely aligned functions that look, smell, taste and oftentimes are identified as security functions." For example, a security guard checking identification at a plant or office building performs the same function as the police officer who checks identification at City Hall. More to the point, according to Tippit, "we shouldn't have to generate a new college program" to redefine skill sets that have been proven effective through years of practice.

The Consortium's objective, then, has been to "align and define the core disciplines of security." Tippit believes there is no sense duplicating the many fine criminal justice programs or health and safety engineering programs. Going one step further, he asserted that if a person acquires a competency in a police academy, for example, "we should be able to leverage that competency" if and when that person practices outside the police profession.

Tippit went on to say that in every state but two, there are six law enforcement missions: (1) maintain order; (2) protect life and property; (3) prevent crime; (4) enforce laws; (5) detect and apprehend offenders; and (6) perform other services. He posed the question, "If you strip away from that the authority to arrest:" and other similar types of authority, "is there any of those that are not a mission of a security program?"

On the other hand, he acknowledged that a graduate of the police academy does not have the core competencies to "design, implement and execute a security program either at the federal

level or in the private sector." Therefore, he feels it best to "concentrate on the core competencies that are relevant to the security profession" and leverage the other competencies wherever they originate.

Tippit next turned their attention to seven disciplines that the group had defined to date. He observed that five have recorded histories going back 3,000 to 4,000 years including the protecting of secrets; guard functions; and establishing the trustworthiness of individuals and groups. In charting these disciplines, his group went through the federal government and its supporting industries and identified security positions as titles.

When he queried executives on these various titles—that is, what kind of abilities or competencies did they expect from someone with a particular title—their responses varied from a person who could do everything to a person who could do basically nothing.

Next his group focused on the concept of "concentrations," which have appeared in various literature as being a security discipline. They discovered that a concentration requires a "multidisciplinary competent practitioner."

Getting back to disciplines, Tippit told them that the biggest problem they've discovered is that "the people who hire security practitioners have a problem in one, knowing what to expect and two, how to measure it…what does that background mean." For no matter what position a practitioner has held, if they were to conduct a gap analysis, "you would find that there are holes."

A common frustration for the team has been the discrepancy in terminology. He explained that if one looks at three programs with the same title—for example, professional development program—oftentimes the objectives are the same but the process is wildly different among the three. His team felt that one equalizing solution might be a measurement protocol, something that across the board would define entry level competency. He referred back to the example offered earlier in the morning about a recent graduate with a degree in accounting: no director of finance would expect that person to take on a senior management position. In the same way, a degree in security management would not necessarily immediately qualify an individual for an advanced security position.

He did note that the average salary for security professionals has risen over 400% based on a study conducted by Abbott, Langer & Associates, Inc. He also referred to eight new positions created within the federal government where the starting salary is $150,000 and progresses to $250,000.

**Question/Comment:**

Is John's program strictly for government security?

**Answer:** "While the products are for government, the research is being collected from the private sector as well." Tippit observed that typically, industry turns to government for training. Moreover, at last count, there were over 13,000 individual companies cleared in the DoD program.

**Question/Comment:**

Are you finding that in your description that competencies and tasks are similar in the government enterprise sector?

**Answer:** Competencies are similar but different words are used.

**Question/Comment:**

I've spent half my life in government security and half in the private sector, and I find the taxonomy huge. For example, start with background investigation data.

**Answer:** "I agree. I guess the best way to characterize it from our point of view—the private sector doesn't view in general the same threat level that government operations imposed on it…but I suggest that there is no practice the government uses, save the crypto area, that is not available to the private sector if they were to choose their assets at the same level."

**Question/Comment:**

How about the pre-employment screen?

**Answer:** "They (private industry) have a different legal landscape that they have to deal with and as you know that varies from state to state." Tippit took a few minutes to describe a study he conducted a few years ago at the Personnel Security Research Center, an organization within the DoD that develops the definitions and requirements used for government background screening. After studying the private sector, that is, "a non-regulatory based…we found programs in the private sector that were actually superior to the clearance program the government has."

# 2002 Symposium Overview: Power Point Presentation

**David H. Gilmore, CPP**
Chairman, Academic/Practitioner Symposium
Moderator

## 2002 SYMPOSIUM OVERVIEW

DAVID H. GILMORE, CPP
CHAIRMAN, ACADEMIC/PRACTITIONER SYMPOSIUM

## SYMPOSIUM OVERVIEW

- The goal is to establish continuing communication and liaison between the academic community and security practitioners.
- The Symposium involves an on-going process and a long-term commitment.
- The focus and agenda will change depending on the issues in security education that need to be addressed.

## FOUNDATIONS OF BUSINESS SECURITY INITIATIVE

- Security is a business function and is not a subset of the criminal justice system.
- Business and Organizational Security Management is a distinct field of academic study, separate and apart from administration of justice, criminal justice and police science.
- Business and Organizational Security Management curricula should be interdisciplinary.

## GOALS OF BUSINESS SECURITY INITIATIVE

- Increase the business student's understanding of security as a business function.
- Increase the security student's understanding of other business functions and of security's relationship to those functions.

## STRATEGIC ACADEMIC GOALS

- Promote business security initiative.
- Encourage development of Business and Organizational Security Management as a distinct field of study.
- Offer curriculum models and courses to colleges and universities.
- Accredit security education programs.

## 1997-1999 SYMPOSIUM RESULTS I

- Developed the framework for an introductory course in business security for security students.
- Developed preliminary outlines for follow-on courses in Risk Assessment and Legal Aspects.
- Developed a description of the security field for use as a baseline in future security education developmental efforts.

## 1997-1999 SYMPOSIUM RESULTS II

- Spin-offs:
  - ✓ Body of Knowledge Task Force
  - ✓ Security Education and Career Study

## 2000 SYMPOSIUM RESULTS

- Developed an 18 credit undergraduate curriculum model as the basis for a minor, area of concentration or option in Business and Organizational Security Management.
- Developed an 21 credit graduate curriculum model as the core for a 36 credit degree in Business and Organizational Security Management.

## 2001 SYMPOSIUM RESULTS

- Developed proposed qualitative and quantitative criteria for use by ASIS in accrediting baccalaureate and graduate security education programs.
- Oriented Symposium attendees regarding the ASIS Professional Certification Board's Role Delineation Study.

## SECURITY MODEL ELEMENTS I

- Physical security
- Personnel security
- Information systems security
- Investigations
- Loss prevention
- Risk management
- Legal aspects
- Emergency/contingency planning
- Fire protection

## SECURITY MODEL ELEMENTS II

- Crisis management
- Disaster management
- Counterterrorism
- Competitive intelligence
- Executive protection
- Violence in the workplace
- Crime prevention (general)
- Crime prevention through environmental design
- Security architecture and engineering

## 2002 SYMPOSIUM TASKS

- Define those core competencies that students should have when they complete baccalaureate and graduate security education programs.
- Validate the curriculum models that were developed in 2000 in light of the core competencies that are developed this year.

2002

## TASK PARAMETERS

- Develop core competencies/program outcomes in light of the new security environment that exists post-09/11.
- In developing competencies, address needs, requirements and expectations from the perspective of the current or prospective employer, not the student in the program or the academician presenting the program.

2002

## TASK PARAMETERS

- Limit the core competencies to 12 at the undergraduate level and 12 at the graduate level.
- Identify core competencies that apply to both undergraduate and graduate programs.
- In validating the 2000 curriculum models, adhere to the task parameters that applied to the 2000 Symposium.

2002

## SYMPOSIUM GOALS

**Communication**

**Discussion**

Debate

Consensus

## Plenary Session #2: Update on Symposium Projects and New Initiatives

**Carl Richards, Ph.D.**
Vice Chairman, Academic/Practitioner Symposium
Moderator

Dr. Richards' presentation focused on the recently completed career study commissioned and implemented by the ASIS Council on Academic Programs in Colleges and Universities.

The intent of the study was to find out, if the respondents hire graduates with a degree other than security management, why do they do so? Are they not aware the degree exists? Or is it a case that it doesn't meet their needs. The group attempted to be as rigorous and scientific as possible in constructing the questionnaire, and eventually sent the survey to 1397 businesses and organizations in basically seven industry sectors: educational institutions; healthcare; hospitality industry; information technology; retail; telecommunications; and transportation.

Regarding the survey instrument itself, three questions—3, 4, and 5—were written to gain quantifiable information. The last was written to elicit comments.

One hundred and five surveys were returned for an 8% return, which was sufficient to make some generalizations.

Question #4 dealt with the relative weight that security education and experience carry in the hiring decision for all security positions. The following elements form the basis of the question:

- Security background Security background plus security degree
- Security degree but no security experience
- Business or other degree but no security experience
- Business or other degree with security experience
- College education only in a subject other than business or security
- Law enforcement experience at all three levels Military police

When the results were tabulated, 17% of the respondents suggested that a security background was most important. This element was followed by law enforcement with 16% of the respondents while law Enforcement Experience at all three levels compiled 15% of the responses.

Dr. Richards observed that having experience seems to carry more weight in the hiring decision. Different industries seem to mirror these same results. For example:

Educational institutions: 17% rate security background first, 15% rate law enforcement first, and 14% rate background with degree first.

Healthcare: 20% want a security background, 16% each for law enforcement and background with a degree.

Retail: 20% rate security background first, 19% rate background and degree first, and 14% rate law enforcement first.

Transportation: 18% want security background, 13% want background with degree, and 17% want law enforcement.

Question #5 asked what kinds of competencies organizations looked for in non-management positions. Following are the elements that were considered:

- Security technologies systems
- Investigations
- Computer and information security
- International security
- Legal issues
- Risk assessment
- Personal integrity and protection
- Other

One attribute, Investigations, received support from 19% of the respondents. Both Security Technology Systems and Personal Integrity and Protection received support from 18% of the respondents. These three attributes were followed by Risk Assessment with support from 13% of the respondents.

In response to a question from the audience, Dr. Richards defined personal integrity as having "honesty…good ethics…someone who is willing to do what has to be done and they take their job seriously."

Question #6 asked what kinds of competencies were important for a management position. Following are the elements that were considered: Extensive security experience,

- Business experience, 10 year plus
- Innovator
- Leader
- Inter-personal skills
- Mentor
- Technician
- Manager
- Others

Results from this question seemed to fall with what would be perceived as a normal pattern of attributes for a manager. Interpersonal Skills garnered 18% support from respondents while Extensive Security Experience gained 16% and that was followed closely by the Leader attribute with 15% of respondent support. The Manager attribute followed with 13%.
Before getting into the respective ratings, Dr. Richards dwelt on the concept of "the age old idea about what a manager is…" He isolated three attributes: (1) technical skills; (2) interpersonal skills; (3) conceptual skills.

Breaking down the responses by industry, one finds:

Educational institutions: 13% rate security experience first, 16% rate managerial experience first, 19% rate interpersonal skills first, and 14% rate leadership first.

Healthcare: 18% want a security experience, only 12% want managerial experience, 16% want interpersonal skills while 17% want leadership skills.

Retail: 13% rate security experience first, 16% rate interpersonal skills first, 15% rate leadership first while 14% rate innovators first.

Transportation: 15% rate security experience first, 15% rate management experience first, 16% rate interpersonal skills first, and 15% rate leadership first.

Another quantifiable question that was asked dealt with whether candidates should have a college education. Out of 105 respondents, 84 support a college education for management personnel; almost none support it for other security personnel. The question further suggested three possibilities in regards to what kind of college education—Masters degree in Security, Masters degree in Business, or Masters degree in Criminal Justice—but received very few responses to make any kind of judgement.

Dr. Richards answered another question that pertained to whom in the company the survey was sent. He responded that it went to high-level security managers such as the Director of Safety and Security. At this point, he opened the floor to more questions.

**Question/Comment:**

This individual remarked that it was interesting that over 1,200 people didn't feel this was important enough to respond.

**Question/Comment:**

Another person wondered if the answers might have differed had the survey been sent to human resources instead of security.

**Answer:** Dr. Richards recalled that in the past they had sent a survey to human resources and many security directors were offended that they hadn't received it.

**Question/Comment:**

As a respondent practitioner, this person suggests that many times it's a lack of time rather than a lack of interest that dictates which surveys are completed.

**Question/Comment:**

Someone else shared an experience they had with a survey. They put a research team on the road to interview 35% of the respondents to their survey. The results were very interesting: (1) there were problems with how respondents understood the instrument itself; (2) responses often varied with the background of the respondent; and (3) 30% of the answers were wrong, that is, when they tested the answers against the question, the answer didn't exist.

For this reason, they decided to use a focus group in their next effort to gather information.

# UPDATE: SECURITY EDUCATION & CAREER STUDY
# POWER POINT PRESENTATION

**Carl Richards, Ph.D.**
Vice Chairman, Academic/Practitioner Symposium
Moderator

**UPDATE**

**SECURITY EDUCATION & CAREER STUDY**

**PRESENTED BY**

**CARL T. RICHARDS, Ph.D.**

**University of Cincinnati** **May 30, 2002**

## BASIS FOR THE STUDY

- **ASIS ACADEMIC/PRACTITIONER SYMPOSIUM**
- **STANDING COUNCIL ON ACADEMIC PROGRAMS IN COLLEGES AND UNIVERSITIES**
- **BUILDING A MODEL OF THE "SECURITY PROFESSIONAL" WAS ONLY ONE STEP IN THE PROCESS**

## "INTENT"

**As the Chairman of the Council stated:**

**... If you (industry) seek graduates with a degree other than a security management degree, wéd like to find out why. Is it because you are not aware of the existence of security education programs or is it because those programs did not meet your requirements?**

## METHODOLOGY

- **QUESTIONS DEVELOPED.**
- **SENT TO FIFTEEN ASIS MEMBERS.**
- **CHANGES WERE MADE IN QUESTIONNAIRE AND RE-SENT TO CHAIRS OF ASIS COUNCILS THAT WERE TO BE SURVEYED.**
- **FINAL ADJUSTMENTS MADE.**

## METHODOLOGY(cont.)

- **200 CHOSEN RANDOMLY FROM EACH INDUSTRY SECTORS**
- **QUESTIONNAIRE EMAILED, FAXED, OR MAILED TO 1397 SMALL AND MEDIUM SIZE BUSINESSES AND OTHER ORGANIZATIONS**
- **QUSTIONNAIRES SENT TO FORTUNE 1000 AND DATA ARE READY FOR ANALYSIS BUT NOT INCLUED WITH THIS PRESENTATION**

## METHODOLOGY(CONT.)

**INDUSTRIES SECTORS SURVEYED**

1. EDUCATIONAL INSTITUTIONS
2. HEALTHCARE
3. HOSPITALITY
4. INFORMATION TECHNOLOGY
5. RETAIL
6. TELECOMMIUNICATIONS
7. TRANSPORTATION

## METHODOLOGY(CONT.)

- 105 of the 1397 recipients responded
- In survey research, a 7.51 % response represents a return of sufficient information that can support generalizations about the issue(s) under consideration.
- The analysis of the data follows.

## ANALYSIS

Three questions in the Survey, numbers four, five and six, were designed to gain information directly related to the objectives of the study and were structured so that responses could be quantified.

## SECURITY EDUCATION & EXPERIENCE

- Question Four:

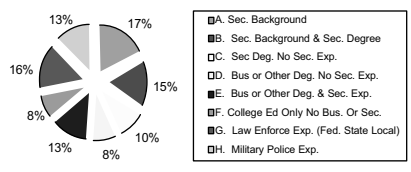
  Colleges and universities offer Associate, Bachelor, and Master degrees in security management, asset protection, and protection management. When filling any security positions, does your company consider candidates who have:

## SECURITY EDUCATION & EXPERIENCE(Cont.)

- A security background
- A security background & security degree
- A security degree but no security experience
- A business or other degree but no security experience
- A business or other degree & security experience
- A college education only in a subject other than business or security
- Law enforcement experience (federal, state & local)
- Military police experience

## SECURITY EDUCATION & EXPERIENCE (Cont.)

**Chart 4.1 Education/Experience All Industry Sectors**

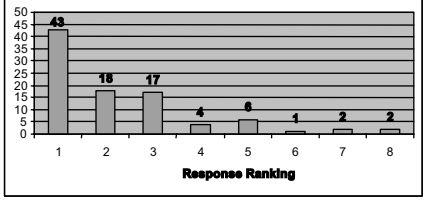



## SECURITY EDUCATION & EXPERIENCE (Cont.)

- Chart 4.1 provides a broad overview of what education and/or experience small and medium size employers suggest they are looking for when filling security positions.
- However, one may ask, how important is that particular education or experience to the respondents?

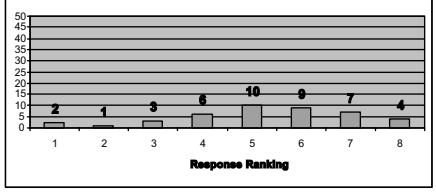
## SECURITY EDUCATION & EXPERIENCE (Cont.)

Chart 4. 2. 1 A. SECURITY BACKGROUND



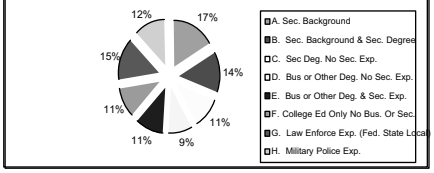

## SECURITY EDUCATION & EXPERIENCE (Cont.)

Chart 4. 2. 4 D. BUS. OR OTHER DEGREE BUT NO SEC. EXP.



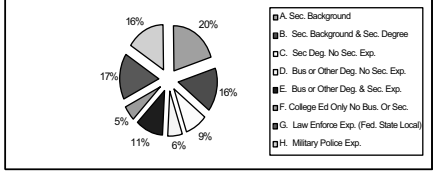

## SECURITY EDUCATION & EXPERIENCE BY INDUSTRY SECTOR (Cont.)

Chart 4. 2 Education/Experience- Educational Institutions



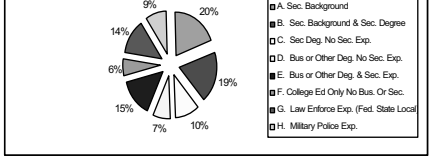

## SECURITY EDUCATION & EXPERIENCE BY INDUSTRY SECTOR (Cont.)

Chart 4. 3 Education/Experience - Health Care



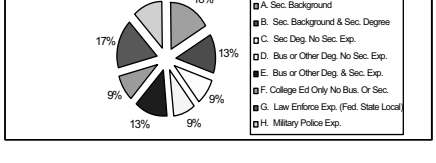

## SECURITY EDUCATION & EXPERIENCE BY INDUSTRY SECTOR (Cont.)

Chart 4. 7 Education/Experience - Retail




## SECURITY EDUCATION & EXPERIENCE BY INDUSTRY SECTOR (Cont.)

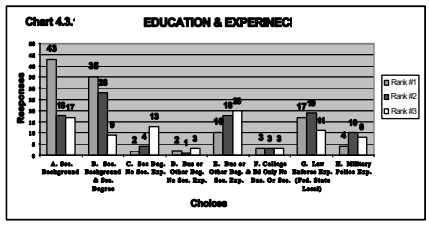
Chart 4. 9 Education/Experience - Transportation



## SECURITY EDUCATION & EXPERIENCE BY INDUSTRY SECTOR(Cont.)

- Data point to security experience as the key factor in small and medium size organizations' hiring practices
- However, security experience is not necessarily the only type of experience that counts with these employers.

## SECURITY EDUCATION & EXPERIENCE BY INDUSTRY SECTOR(CONT.)




## NON-MANAGEMENT SECURITY POSITIONS

Question Five was designed to provide some idea of what small and medium size organizations were looking for in their security personnel not in management positions

## NON-MANAGEMENT SECURITY POSITIONS (Cont.)

Question Five asked:

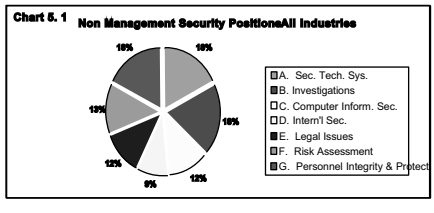
When recruiting for non-management security positions, what security competencies are you looking for from your candidates?

## NON-MANAGEMENT SECURITY POSITIONS (Cont.)

**Competencies:**

- Security Technology Systems
- Investigations
- Computer/Information Security
- International Security
- Legal Issues
- Risk Assessment
- Personnel Integrity& Protection
- Others

## NON-MANAGEMENT SECURITY POSITIONS (Cont.)



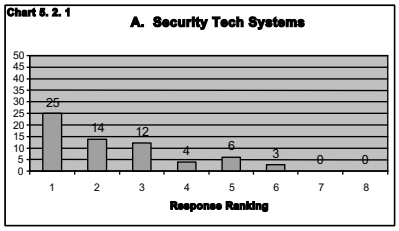
## NON-MANAGEMENT SECURITY POSITIONS
(Cont.)

Three attributes received 18 percent of the respondents' support

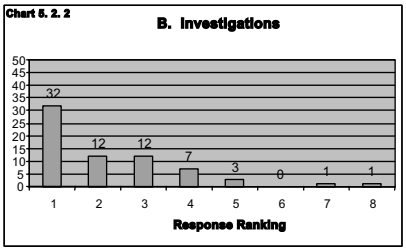
- Personnel Integrity & Protection
- Investigations
- Security Technical Systems

**Breakdown of responses follows:**

## NON-MANAGEMENT SECURITY POSITIONS
(Cont.)




## NON-MANAGEMENT SECURITY POSITIONS
(Cont.)




## NON-MANAGEMENT SECURITY POSITIONS
(Cont.)


## MANAGEMENT SECURITY POSITIONS

Question Six:

When recruiting management positions in security, what competencies are you looking for from your candidates?

## MANAGEMENT SECURITY POSITIONS

**COMPETENCIES:**

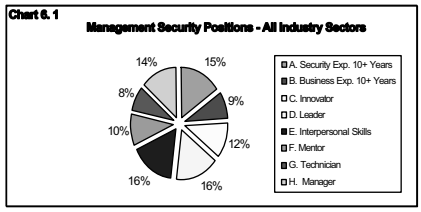
- Extensive security experience (10 + years)
- Extensive business experience (10+ years)
- Innovator
- Leader
- Interpersonal skills
- Mentor
- Technician
- Manager
- Other

## MANAGEMENT SECURITY POSITIONS

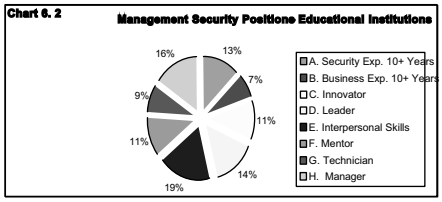
Age-old question is what makes a good manager? Text books usual suggest three competencies:

- Technical skills
- Interpersonal skills
- Conceptual skills

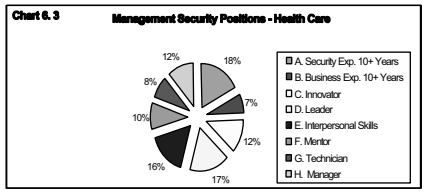
## MANAGEMENT SECURITY POSITIONS



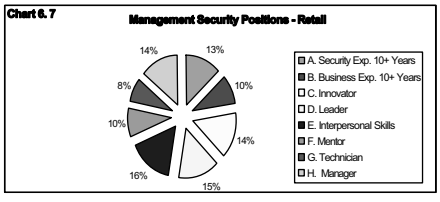

## MANAGEMENT SECURITY POSITIONS BY INDUSTRY



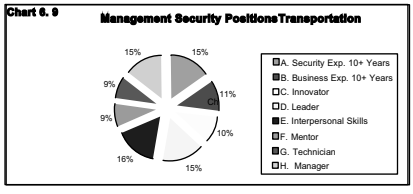

## MANAGEMENT SECURITY POSITIONS BY INDUSTRY(Cont.)




## MANAGEMENT SECURITY POSITIONS BY INDUSTRY(Cont.)



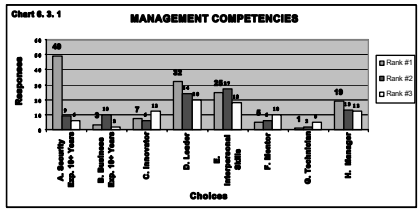

## MANAGEMENT SECURITY POSITIONS BY INDUSTRY(Cont.)



## MANAGEMENT SECURITY POSITIONS (cont.)

- Chart 6. 3. 1 provides a different way of analyzing respondents' information.
- What we will see is that 49 respondents out of 105 ranked Security Experience number one.
- An additional 15 respondents ranked it either second or third.

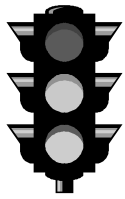
## MANAGEMENT SECURITY POSITIONS (cont.)




## COLLEGE-LEVEL SECURITY EDUCATION

- Question Seven asks if one believes that certain security professionals should have a college education.
- 84 of the 105 respondents supported college for management personnel.
- Three possibilities were suggested: security, business, or criminal justice.
- Not much guidance provide.

## SUMMARY AND QUESTIONS



## Plenary Session #3: Open Discussion and Q&A

**David H. Gilmore, CPP**
Chairman, Academic/Practitioner Symposium
Moderator

**Question/Comment:**

Dr. Eva Vincze expressed her frustration with the lack of internships available for students. Moreover, she worries that there will be an insufficient number of positions available for her students once they graduate. She feels that ASIS as a group should be educating the industry on the need for more internships and entry-level positions.

**Question/Comment:**

Someone else provided another side of the issue: he told the audience that last year, over 430 government internships went unfilled because there weren't enough qualified applicants, with the emphasis on qualified.

**Question/Comment:**

Another speaker brings up the reality that oftentimes, employers rely on the "good old boy system" when looking for employees.

**Question/Comment:**

Eva pointed out that because "we haven't put together a good program…we never produced a good practitioner…" which leads to the unfilled internships. And while she feels they are going in the right direction, the process has bogged down and there needs to be faster progress.

At this juncture, Gilmore updated the audience on Council activities.

The first project—the Academic Security Awareness Project (ASAP)—deals with a three-prong initiative to increase awareness.

1. Approach Peterson and Barrons – publishers of college directories. Right now, there are no programs in security listed in the directory. The goal is to have them list programs and educate them that security management exists as a field of study. Similarly, they planned to approach and raise awareness among high school counselors.

2. Approach the U.S. Dept. of Labor regarding the Occupational Outlook Handbook. In the section dealing with Protective Services, there is currently no entry for security management. The goal is to have security listed in the handbook.

3. Approach publishers of career guides. Ideally, "the optimum solution would be for somebody in this room to say I am going to write a book on security careers and get it published and just have one on the shelves. So if you go into Borders or Barnes & Noble you see a book that says 'Careers in Security.'"

The second project involved the reformatting of the ASIS website to make it more user-friendly and more accessible to a greater number of people.

The third activity focuses on developing and customizing more programs for student members. Gilmore asked everyone to encourage student members to attend the upcoming ASIS Annual Seminar & Exhibits in Philadelphia.

In the continuation of the question and answer session, the subject of student members was raised again. Kropp has a new recruitment effort underway, as ASIS has only 200 student members out of 32,000 members overall. This new effort involves several senior Regional Vice Presidents taking over various tasks; John Spain, CPP, has been named Senior Regional Vice President for Student Member Development.

**Question/Comment:**

Someone from the audience commented that he has seen less age bias in the overall business environment—perhaps this can be used as a type of model in the security industry.

**Question/Comment:**

Tippit shared what happened in the focus group they conducted with 35 executives. The results were "diametrically opposed to what we hear from security managers." Moreover, he believes an explanation lies in the possibility that "the security manager knows what he is talking about." Or more to the point, executives don't know enough about the function and are more apt to turn to someone else for this information. That is why they look for experience in a senior security manager—"enough to convince them that the person knew what they were doing."

He continued that managers didn't know "what a title suggested by way of a competency." Instead, they reasoned that if a person "was good enough for that agency, that entity for 20 years, his integrity must be unreproachable."

**Question/Comment:**

Ed Garcia was curious about the new Transportation Security Administration and whether ASIS had had any communication with the administration.

**Answer:** Kropp answered that at one point, the administration had enlisted their [ASIS's] help for recruiting purposes and to work on guidelines, but just as quickly withdrew the request. He went to say that ASIS now has a full-time lobbyist—actually more of a liaison—with the government.

Someone else from the audience did have some information on who was being hired for the Transportation Security Administration management jobs. According to him, the agency had identified three criteria for job candidates: certification such as the CPP; law degree; and graduation from an institution in criminal justice, be that a military, government, or private sector institution or police academy.

**Question/Comment:**

Several members of the audience expressed their frustration with trying to find qualified candidates for their internships. Some pointed to the fact that many internships are unpaid, and thus unattractive to students. Another possibility was that if a student didn't do well in the internship they could very well lose 6-9 credits. Someone else suggested that since many students aren't motivated to find these positions on their own, there needs to be a mechanism where they are required to do so before they can graduate with the security management major. Bob McCrie mentioned that this is the case at John Jay College.

**Question/Comment:**

Dan Kropp wanted to respond to something mentioned earlier, that is the issue of homeland security. It wasn't until ASIS, along with the IACP, went to Governor Ridge and "said collectively, we represent over 48,000 police and law enforcement, you should be listening to us…" that they finally got their attention.

**Question/Comment:**

One of the final comments came from Tippit who declared that the basic core competencies could be delivered from a four-year program. He and another speaker share the belief that the main problem is one of awareness: making employers aware of the benefits of a degree in security management; making students aware that this is a distinct and worthy field of study; and making universities aware that the need exists for this kind of program.

# Summaries of Breakout Group Sessions

# Summaries of Breakout Group Sessions

Participants were divided into four groups, with two concentrating on developing the core competencies, or outcomes, expected from students graduating from a bachelor's program, and the other two working on the same task, except for a master's program.

Once they determined the core competencies, they were asked to validate the core competencies against the curriculum model developed at a previous symposium in Norman, Oklahoma. In addition, they were to examine and validate the curriculum models in light of the events of September 11, 2001.

## Summary of Undergraduate Breakout Group # 1

**Michael S. Magill**
Facilitator

After introductions were made, the moderator noted that there was a good mix of practitioners and academicians in the group, which was important given the framework for their task.

Very early in the discussion, one of the members shared that he was currently in the process of pursuing his CHE (Certified Hospitality Educator). In one of his courses, they focused on "…how do you word a competency. How do you define an objective…" and most importantly, how do you measure or test for it?

He suggested that they first settle on a definition for competency. He wondered if it should be performance-based or an activity "that you can measure that has value to the company" or rather, a measure of a person's aptitude. If the measurement assesses simply what the student learned in school, it might have no value to the employer if the student can't translate the "textbook stuff" into real world skills.

A colleague responded that there is a "different approach and different philosophy" at work in the university setting that might require more application-based competencies.

Since the program is designed to take two years, someone asked at what point would the student be evaluated on these core competencies. In other words, how would one judge two years from now what a student learned in the first course he took?

One solution offered was that the student could create and maintain a portfolio, an assessment of which would be an "ongoing assessment process."

Another concern was expressed about where in the organization one would expect to place a graduate, given they're not even getting a full degree, but rather just a minor. If they can determine this level, then "we have to aim the competency" at that.

Although the group started to focus on determining the competencies, early on someone was concerned about the potential liability implications of establishing this curriculum. In other words, if a person receives what might be considered improper training, can the university be held liable for the consequences of his decisions or actions? And if this is the case, has the entire task of creating this curriculum become that much more difficult?

A lively discussion ensued and ultimately the case was made that these were only introductory courses, courses where principles were taught, as opposed to vocational types of courses.

The group then began to determine the core competencies in earnest. They began by developing a "generic skill set for those who work in a dynamic business environment…" and then proceeded to specialize those skills for security management.

Someone listed various skills that he believed any manager should have training in: personnel management; technical and physical systems; budget and resource; and supervisory skills and interpersonal skills.

Then they developed these topics more in-depth. For personnel management, they believed the security manager should be familiar with labor laws because a person could be held liable for various personnel decisions, such as hiring, negligent firing, unsafe workplace, etc.

For technical or physical systems, they envisioned everything from CCTV systems to parking lots to various pieces of equipment.

Analytical skills would require having a global view of their facility, including how to deal with data and what kinds of software to use. A member of the group asked if this also covered risk assessment with the answer being yes.

Another member brings up a concern about computer literacy—since the course is placed in a school of business, a case is made that students would acquire this competency outside of a security-specific class.

Eventually, the group refines the skill sets to human, technical, conceptual, and analytical skills. A question about ethics is posed, and the suggestion is made to add something called ethical concepts to the set.

The discussion returns once more to the types of positions that graduates would apply for (and get), during which the subject of research surfaces. The group agrees that graduates should know research methods, including "how to deal with information you already have and working through that."

Tied into this ability is the concern over critical thinking, which leads one of the academicians to ask a practitioner what they would expect from a recent graduate.

Interestingly, the first answer dealt with legal issues. "I expect them to come into the organization with a basic knowledge of the legal issues, first of all. What to avoid as well as the criminal issues. Some understanding of the basics…how that applies to that sector of business that they are going into, so they don't get into big trouble."

Another answer focuses on the ability to communicate in whatever environment the employee finds himself. Regarding this particular competency, someone describes a scenario where a younger employee reports to an older manager with 30 years' experience. What's expected in the way of communication? The reply was that in this case, he should understand the environment and probably "listen, listen, listen!"

This brings up a perceived need for either a mentoring relationship or internship where the student can acquire practical experience. Someone recommends that in addition to getting their degree, a graduate should have to also serve six months in some kind of evaluating process before seeking certification from ASIS.

Eventually, after several debates on the relative merits of being able to plan, avoid litigation, conduct research and/or needs assessment, and determine and implement the components of a critical incidence plan—among many others—the group developed ten competencies. In the process, they concurrently validated the competencies against the established curriculum model and found no gaps or discrepancies. As for the competencies, they purposely worded these as broadly as possible:

1. Demonstrate an understanding of the various bodies of law. This includes the statutes, limits and case law as they pertain to both business and security investigative functions.

2. Demonstrate an ability to manage physical security systems. This competency would encompass technical and physical resources.

3. Demonstrate an understanding of basic fiscal management. The group expects the graduate to be familiar—on a basic level—with fiscal items such as contracts, system budgeting, inventory, return on investment (ROI), etc.

4. Demonstrate an understanding of how to manage employees as well as contractors. Given the preponderance of outsourcing in today's business climate, several members believed this to be an important facet of personnel management.

5. Demonstrate an ability to gather, analyze, interpret, and act upon data and/or information. This could be risk information as well as operational information. One of the key elements is to know where to look for information.

6. Demonstrate an ability to understand critical incidence management plans. It took the group a long time to arrive at this competency since so many elements seemed to fall under the term "critical incidence." While no one expected the graduate to be able to deal, by himself, with a critical event, they did want him to understand the various components such as emergency planning and business continuity.

7. Demonstrate the ability to conduct and manage investigations. Again, this was left wide open to reflect the broad range of investigations that are conducted within the security framework.

8. Demonstrate an understanding of the principles regarding information protection. Information is not limited to computer data, but also includes proprietary information such as trade secrets.

9. Demonstrate an understanding of crime, crime prevention, and the criminal justice system. This competency would cover concepts such as crime prevention through environmental design (CPTED).

10. Communicate an understanding of ethical issues in the workplace.

Near the end of the session, they considered the issue of homeland security and whether it needs to be a separate competency. As one member put it, "…should a student understand the functions of security in the context of national security?" After a very considered debate, the group came to agree that ultimately, the elements attached with homeland security fall directly under critical incidence management and there's no need to build a separate course.

## Summary of Undergraduate Breakout Group # 2

**Jim McClanahan, Ed.D.**
Facilitator

This group followed a path similar to that taken by the other undergraduate group, though they elicited input from the practitioners right from the start. And just as early, the issue was raised of what kind of position will the student be qualified for when he graduates from the program.

The answers from the practitioners varied according to what industry or organization was involved. One person explained that in the contract security industry, the graduate could come in as a supervisor. Another felt that in the government arena, they would be considered physical security specialists. At the opposite end of the spectrum, someone used the example of Chris Richardson who went directly from graduation into a four-week management training program at Marriott, started as security manager for three small properties in Washington, D.C., and is now Director of Loss Prevention for the Baltimore Marriott Waterfront, a large property at Baltimore's Inner Harbor.

Just like their counterparts in the other group, they felt that the competencies should support the position that the student would most likely hold upon graduation. They eventually got beyond this sticking point by agreeing that while a graduate could use personal initiative to climb further up the ladder, the most realistic positions would be entry-level ones.

They began the process by brainstorming and listing various competencies or attributes. The suggestions focused on physical security, risk assessment, analytical ability, research ability, critical thinking and writing skills, and communication skills.

Before going very far, someone suggested that they consider defining what a competency is or the issue would continue to dog the group throughout the entire session. At one point, someone maintained that "it boils down to the role of education and the role of training" as to what outcome would be achieved. In order to keep the process on track, they worked with an open-ended definition of what a person could do, know, think, or evaluate.

In refining the preliminary list of skill sets into competencies, they also looked at the various course descriptions and validated the competencies against the curriculum at the same time. Unlike the other group, however, there was greater disagreement about where to place various "sub-competencies" as one person put it. Until the final presentation, some of these were fluid and could be temporarily found under several headings.

1. Communications skills, including the ability to speak in public or before groups; also, the ability to write effectively. This skill was considered by several—though not all—to be critical, mainly because of the training component often found in the security function.

2. Able to conduct risk assessments. This is a broad area where various group members included the identification and analysis of assets, threats, and vulnerability, and recommendation of appropriate counter-measures. Understand and use the tools for evaluating security systems and technology.

3. The ability to manage with a basic knowledge of items such as preparing a budget, performing an audit, and perhaps project management.

4. Business skills, which include the ability to perform various analyses such as cost-benefit, risk vs. non-risk, and return on investment.

5. Critical thinking or a decision making capability. The group would later add ethical thinking to this area. Subsumed under this category is the ability to apply a scientific method to approaching and solving problems. As such, research methods fall here as well.

6. Knowledge of legal issues. One person declared that "legal is the most significant issue in security." The expectation here is that the graduate would have an awareness of legal ramification and liabilities. In fact, someone tried to make the case that "legal liability fits under every" competency.

7. Basic investigation skills to include interviewing.

8. Ability to manage physical security systems, including a familiarity with both current and emerging technology.

9. Leadership skills, which translate into a knowledge of policies and procedures.

10. Risk management (which is different from risk assessment). This encompasses safety issues, crisis management, and disaster management as well information protection.

11. Theoretical aspects of crime prevention: CPTED and deterrence theory.

12. Domestic and international terrorism, cyber-terrorism, workplace violence. In the last minutes, the group added intelligence gathering to this category.

One particularly contentious topic throughout the sessions centered on the international arena and how much should be expected from the undergraduate level. One member believed very strongly that undergraduates should have a strong appreciation for the international implications inherent in security. Another believed equally strongly that this area was more suited to the masters level and that it was unrealistic to expect more from an undergraduate entering an entry-level position.

They reached a stronger consensus on the need for better cooperation between the government and the private sector regarding homeland security. So far as the curriculum goes, an additional

course might need to focus on terrorism. But on a more practical, timely level, they discussed how up to now, the government only notified law enforcement in the event of a credible threat. They felt the government was missing a huge opportunity to protect even greater numbers of people by not contacting security personnel in the private sector.

## Summary of Graduate Breakout Group #1

**Kevin Peterson, CPP**
Facilitator

The members of this group didn't immediately address the task at hand. Rather, they shared information about themselves, their current positions, and their experience in the security industry.

In time, Kevin Peterson suggested that they develop and organize competencies around three sub-areas: (1) performance skills, i.e., technically doing the work; (2) people skills, i.e., preparing students to deal in the corporate or government environment; and (3) business management skills, i.e., things such as marketing and budgeting. Just as the two undergraduate groups, they started the process by brainstorming possible core competencies.

While members of the group began jotting ideas, someone asked for a clarification of "performance." Peterson replied that was "looking at things like …risk management, risk assessments, physical securities, security systems, security contracting and that sort of thing as opposed to business management which would be more, put together a budget, how to hire people..."

Hard on the heels of this clarification, someone brought up the vast range of employers and the wide discrepancy between their respective needs. "I don't know how we can sort it (competencies) down to 12…The breadth of knowledge that is needed within the security field is overwhelming right now."

Peterson observed that this underscored a core-competency point of view—the analytical or research ability to "know where to look for information, to collect data."

A discussion of the difference between the undergraduate and graduate levels ensued, which in turn, led to someone expressing their reservations about taking the employer's perspective in this exercise. More time was spent on discussing the need to balance the desire of the student to find a job with the commitment to providing them with a sound and thorough education.

Using the original framework of the three sub-areas, they actually developed 13 core competencies:

<u>Business and organizational management skills</u>

1. Awareness of a systems approach to solving problems.

2. Ability to engage in strategic or creative problem solving. At the higher levels of management, graduates will face situations that require groundbreaking solutions.

3. Advanced communication skills, including written and oral communications as well as proficiency with common computer functions. Someone noted that "most people come to grief not because they lack technical expertise…but rather certain human skills (in communication)…"

4. Knowledge of how to financially justify your programs and needs within the context of the organization's budget.

5. Authority to manage large and small projects; function with equal ease within various organizational structures; learn to keep up-to-date with emerging technology.

Performance skills

6. Skilled with research methodologies and analysis at a high level. At this level, they should be expected to "identify the problem, solve the problem, and check to see if the solution is right regardless of the discipline."

7. Familiarity with legal matters and international business law.

8. Ability to perform risk management and assessment functions.

9. Ability to conduct or oversee investigations, to include audits and white collar crime.

10. Critical thinking skills.

People skills

11. Ethics as part of both the organization's dynamics and the individual's character. Oftentimes in today's organizations, the security director or chief is also the ethics officer. Moreover, he or she typically plays a role in establishing integrity programs, hotlines, etc.

12. Ability to influence people, especially those people not directly in their command, to achieve solutions.

13. Leadership ability in various situations. Although this often grows with experience, there are certain elements of leadership that can be taught within the academic setting.

**NOTE:** Although they did not want to elevate the following to competency level, the group felt that students should develop some kind of foreign language ability and a thorough understanding of the international business environment.

As they validated the core competencies against the curriculum, they perceived a need for some kind of capstone course, comprehensive exam, thesis and thesis defense, or a separate project management course.

Coming full circle, they returned to the idea of somehow adapting this program to accommodate and address the multiple end-users present in the security industry. One person proposed developing areas of concentration or specialization within the degree. The group ran out of time the first day, but took up the subject on the next morning. Someone indicated that a concentration in "security and protective technologies" would reflect real-world applications. Another person suggested "computer information security."

They also looked at the possibility of developing "analysts" so that one person could specialize in statistics; another could evaluate the effectiveness of various systems; indeed, "a number of areas…clearly lend themselves to an analyst topical area with specialties that happen at different phases of your systems engineering."

International issues took center stage again when a group member recommended a "certificate of international security."

They also addressed the validity of the curriculum in light of the events of September 11. The consensus was expressed by one person who felt that "the underlying security competencies really were there and are there" now. The problem was that officials did not appreciate the "validity of the threats."

Near the very end of the last session, someone wondered if a core competency shouldn't deal with helping the student "plot out a career development, career survival skills." While they acknowledged it was vital, most of the group believed that these skills could be acquired in a number of different ways. Someone did say, however, that the University of Cincinnati offers a "Professional Development" course to introduce students to the realities of a career in higher education. This course notwithstanding, the very nature of their education at the masters level should give them the tools they need to "learn how to think and to ask questions" outside of their discipline.

## Summary of Graduate Breakout #2

**Eva Vincze, Ph.D.**
Facilitator

With the best of intentions, the members of this group totally broke the rules of their assignment, or as they would rather put it, they "changed" the rules.

Which is not to say that they didn't try to achieve what was asked of them, that is, determine up to 12 core competencies for a graduate program.

Every time they attempted to come up with a competency, a nagging question just wouldn't go away: what exactly is the definition of security? And each time someone tried to get past this thorny issue, another would bring it to the forefront. Frustration alternated with excitement as they worked through the process.

Eventually, everyone was satisfied with the end result that took all three breakout sessions to achieve:

- Definition of Security: The protection of assets.

- Five elements subsumed under the definition:

1. Identify and describe threats to assets

2. Identify and describe vulnerabilities of assets

3. Design, select, and deploy countermeasures

4. Evaluate, understand and communicate consequences of losses

5. Understand the overall impact of security

- Core Competency: The knowledge and skills to efficiently and effectively manage and lead the security function.

While it appears to be a deceptively simple model, arriving at these conclusions entailed a great deal of dialogue. Nor did it follow a linear progression, but rather evolved over the course of the discussions.

In many ways and in many instances, the members of this group considered several of the same topics that were raised and developed by the other three groups:

- The value of research methodologies.

- What position will the graduate be qualified for.
- No such thing as a "single security person."
- Training for technical capabilities vs. an education in principles.
- The importance of critical and strategic thinking.
- What are the real expectations of the employer?
- Physical security vs. information security.
- The legal considerations of security functions.
- Ability to look at the "big picture" and make decisions accordingly.
- Define assets. Define threats. Define vulnerabilities. Define consequences of losing the assets.
- The integration and alignment of security with other functions in the organization.
- How to determine and communicate the value of security in an organization: revenue producer vs. cost center.
- In general, the current poor writing and presentation skills of students vs. the need for superior communication skills.
- Lack of a common glossary of terms.

A breakthrough of sorts occurred when the group agreed on the definition of security as the protection of assets. However, someone objected that it would appear illogical to jump from protection of assets to security management—why not call it "asset management?"

The response set the stage for the group to move forward:

"(It's not) asset management because … many times it excludes protection. The way we got to management was by defining the component disciplines of how do you do this. Where are the core competencies in executing that mission? Now, you can't effectively do this with just the (individual) component elements of any one of these, but rather you need to address multiple disciplines in the effective protection of assets and if you will, that formula is made up once you define what assets you are talking about, where they exist, how they are used, and all those types of things. ***So the management of security becomes the function of integrating these disciplines and the core competencies associated with them, managing that process to effectively do this."***

From this point, the group made steady progress in delineating the "five component disciplines" in the definition. For a few minutes, they struggled with the distinction between vulnerabilities and threats, especially when a member argued that one can neither manage threats nor can one eliminate vulnerabilities.

His reasoning was that to make something usable, functional, the minute it becomes available for use it becomes vulnerable. It's a necessary trade-off to allow functionality. As for threats, he contended that they are everywhere and that it's impossible to protect against threats. In his words, "You have to build systems with vulnerabilities in order to make them useful. So you have overlay protection over the top of those vulnerabilities to manage them and that residual that you have left over is the exposure and exposure is your problem, not vulnerability."

Regarding threats, the best that can be done is to keep a threat from succeeding.

Another contentious issue was raised when someone described the function of investigations as a reactive response to a failure in physical security efforts. In other words, it is a process separate and distinct from physical security. Going one step further, physical security is predicated on a reactive model that attempts to detect or contain a loss of assets.

As they neared the end of the second session, they embarked on a quest for another definition: what is a competency? Members offered terms such as knowledge, skills, and expertise but postponed the discussion to the next day.

During their final session together, they were more relaxed and joked about how "success was snatched out at the feet" at the last moment. However the task of developing core competencies remained. At first, someone suggested that the five components of the definition of security should be the competencies.

Before long, the group was once again debating, only this time the discussion revolved around which skills or abilities were expected at the undergraduate level as opposed to those expected at the graduate level. Someone suggested that "at the graduate level you would…have the ability to manage, develop programs, assess programs, all of those management skills…" Another person objected, however, with the observation that instead of "managing," a graduate-level person should be "leading." This led someone else to note that leadership "is one of the key fundamentals of management."

In the final analysis, a successful security practitioner would possess a combination of management skills as well as the skills needed to protect the assets.

Running out of time, they also agreed to an overarching description for the core competencies being "that knowledge and skill sets that would be required to accomplish the definition of security, that is, the protection of assets.

**Martin Gill, Ph.D.**
**Professor of Criminology, Leicester University**

Security Education: A British Perspective
Dinner Guest Speaker

After thanking the Society for the invitation to speak at this year's event, Professor Gill said he would like to talk about two things: (1) the difference in teaching between Britain and the United States and (2) the similarities in research between our two countries.

He first joked that in the past four or five years that he's attended the symposium, he's had to learn about "American English." For example, there is no "graduate" program in Britain. "You are either an undergraduate or a post-graduate."

More seriously, he wanted to talk about the differences between the two countries, "to attack as a friend" some of the realities about having to deal with a worldwide audience. He commends the Society for its efforts to "embrace the world" but it's inescapable that "the organization is American. It has grown up here and the culture is here."

One of the interesting things for Professor Gill is how "you deal with students and universities. For us it is a very interesting process to find out that you have the freedom to behave as you do." In Britain, universities are subjected to exhaustive and comprehensive reviews in several areas. He described the role of the "external examiner" who is independent of the university, but who provided oversight in the grading process. For example, a student writes a paper; the paper is graded [once by another student] and once by another member of the staff. Before the paper is returned to the student, it must go to the external examiner who "checks that the marks are correct, they are consistent, and that we have been completely fair." The same "onerous" regulation and oversight is applied to departments as well as to individual professors. In evaluating departments, they look at things such as:

- Department aims
- Lines of communication between staff
- Who chairs what committees and why they chair those committees
- Procedures we have for reviewing all courses
- Responses to any essays, any letters that have come in about any aspect of the work of the Scarman Centre [the academic unit Professor Gill heads within Leicester University]
- Feedback arrangements that we have for our students and they want examples

- Procedures we have for developing our staff
- How often we observe our staff
- Do we have peer observation of teaching?
- Recruitment strategies for students. How do we select them? How do we involve them in the work of the university? They want to see how we provide guidance to them afterwards.
- What sorts of facilities are available to them and how do we make sure they use the library, use the computer center?
- Staff research. What is the research strategy? How they manage research initiatives and how do we look after our Ph.D. students.

Therefore, he has been acutely aware "of the realities of trying to implement change in a very different environment where the circumstances are very, very different."

One area of similarity, however, is in the research taking place. ProfessorGill observed that "one of the sad reflections of the academic world in security is frankly the quite appalling state of much of the research that has been done in this area." For this reason, he was very happy to hear about the new research initiatives mentioned earlier in the day.

He continued to say, "much of the research that has been done in the whole world of security management is just not worth the paper it is written on. It is a lot of nonsense written by people who frankly should know better, who are turning out rubbish which is being swallowed up by other people."

As an example, he described a study he's currently involved in concerning closed circuit television (CCTV). On the one hand, research up to this point indicates that CCTV is a "wonderful success story" and now cameras have a ubiquitous presence all over Britain. In reality, Professor Gill believes that the evidence of its effectiveness is mixed and probably, on balance, "says it isn't effective at all."

He declared that very often, people attribute positive changes to one element without considering other possible, related factors. In the case of CCTV, it could very well be the extra street lighting that CCTV requires that acts as the true crime reducer, and not the camera itself.

He advised that one should also turn a skeptical eye on so-called "results" which oftentimes are proven to have begun before the measure was introduced.

Turning to a new subject, one of his recent projects involved money laundering, which has taken on greater significance in light of the events of September 11, 2001. Specifically, he was study-

ing financial institutions, "trying to find out how they were responding to the need to make sure that they don't and they basically said, 'This is absurd.'" The reason why they found this to be an absurd proposition was because of the enormity of what would be involved to detect a possible instance of laundering. Rather, they made a token effort by investing in technology because "whether you catch them or not, at least you can seem to be doing so."

The same problem of burdensome implementation occurs with a new license plate recognition system being used by British police. In this system, police have a camera that focuses on the numbers of the license plates. This data is entered into a national database that compares the numbers against other information; if the number on the plate has anything to do with a problem identified on the database, the unit alerts the police officer. At face value, it would appear to be an effective system; the reality is that on one day alone, the unit registered 426 alerts. Only three arrests were made and processed that day because the "backup system that it required generates too much information to be managed."

Early in his career, Professor Gill assumed that one of security's strategies was to understand the motivation of offenders and then respond with appropriate security measures. To his surprise, research on this subject was almost non-existent. Towards this end, he conducted his own research last year into the world of shoplifters. He announced that "I have been going shoplifting with shoplifters" with the very serious objective of getting answers to some key questions about robbers: How do they choose a target and decide whether it's easy or not? What things make it difficult for them?

His experience with the shoplifters led to some counter-intuitive results. For example, a store had placed a "very big guy" at the door for intimidation purposes. Far from intimidating the shoplifter, he was perceived as "too big and fat" to run after and catch the robber, and therefore, was not a deterrent at all.

He mentioned this "because I am trying to address this issue of what can we do as academics to make the world, evidence-based, to make security more effective."

For this reason, he interviewed robbers who had been convicted and sentenced to jail about their motivation, experience, modus operandi, etc., in the hopes of understanding how to better respond to these serious crimes.

According to Dr. Gill, planning is not a one-time exercise for a robber; rather, he is "always on the lookout for a robbery…always looking for an opportunity." Logistically, when it comes to bank robberies, single doors are better than double doors or revolving doors because they make for easier getaways. Likewise, there should be a short distance between the door and the bank counter. Ropes that keep customers in line are preferred over general crowding; however, when they get outside, busy streets are best. One-way streets or dead-end streets are not. Their one great priority, more than getting the money, is to not get caught.

It's the "easiness" of the crime that appealed to the robbers. One robber told Professor Gill how he was walking down the street with his wife and when he looked through the window of a

certain financial institution, he saw money—money that had just been delivered—being counted on the counter. He simply walked in and took it off the counter.

This kind of information carries clear implications for someone designing a security system or security architecture for a bank. In the same way, similar studies in other areas would be helpful in designing solutions for those problems.

**Question/Comment:**

Professor Gill was asked why he thinks western cultures invest so little "in the scientific evidence necessary to address the problem" of crime.

**Answer:** He agreed that it "is very difficult to justify why the situation has arisen." Unfortunately, the same mistakes not in research, but rather in evaluation, keep getting repeated.

**Question/Comment:**

Do Professor Gill and his colleagues find it difficult or feel pressured, "very circumspect," about the kinds of evaluations they make in light of new technologies?

**Answer:** He replied that they are always skeptical about the purported capabilities of a new product. And while he knows that a certain amount of cover-up occurs, he declared that this kind of thing is becoming less acceptable. As for ProfessorGill, "I am just going to say what it is and be damned."

**Question/Comment:**

Someone in the audience asks about the impact of Russian organized crime with the new Euro.

**Answer:** Professor Gill responded that they "are a bit closer" on some of the impacts of Russian crime. However, while money laundering has been a hot topic, the really big problem is in the illegal transportation of people from around Europe.

**Question/Comment:**

This person asked Professor Gill why he thinks we were not able to predict the events of 9-11. Specifically, why didn't we learn from the experiences of other people, for example the Irish? And has there been a feeling that the United States should "come down off your high horse?"

**Answer:** He replied that while Europeans and the British are more accustomed to the fear and worry of terrorism, they still experienced great outrage over the events of that day—and sympathy for the people who suffered on 9-11 as well as the ones who suffered in the Oklahoma City bombing.

A moment of silence was observed in memory of the people lost on September 11, 2001.

# Reports and Results

# Day 2
# Reports and Results

## Plenary Session #4: Breakout Group Reports on Task Assignments

**Carl Richards, Ph.D.**
Vice Chairman, Academic/Practitioner Symposium
Moderator

In an effort to accommodate those people who needed to leave earlier, they started immediately with the breakout group presentations.

### Breakout Group Presentations

**Michael S. Magill**
Facilitator
Undergraduate Group #1

Mike Magill explained that the following core competencies were purposely designed to be "about a general as you can get."

1. **Demonstrate understanding in the relative bodies of law.**

2. **Manage physical security systems.**

3. **Demonstrate an understanding of fiscal management** – "Covers the whole gamut, as far as we're concerned again. Our group felt very strongly to stay away from the specifics and stay with the general."

4. **Manage performance of employees and/or contractors**. "So many of us nowadays are going outside of our proprietary organizations to save money…"

5. **Demonstrate an ability to gather, analyze, interpret and act upon data and information.**

6. **Demonstrate the ability to implement critical incident management plans.** This includes everything from a dog wandering in a building to a terrorist showing up with his AK47.

7. **Demonstrate the ability to conduct and manage investigations.**

8. **Demonstrate an understanding of the principles regarding information protection.** Not necessarily just computer information, but sensitive information especially that related to the government.

9. **Communicate an understanding of ethical issues in the workplace.**

10. **Demonstrate an understanding of crime, crime prevention and the criminal justice system.** While all the other competencies would apply to both levels, this would be applicable to only undergraduates.

**Question/Comment:**

Where'd you put terrorism?

**Answer:** "We talked a lot about that dynamic. And, really, it does play within a lot of the categories. When you talk about crime prevention; terrorism is a crime. Certainly, asset protection, you know all the things that fall within that. So, the group felt very strongly that it all should be included.

"Regarding the 2000 Norman classes, we felt there was absolutely no changes needed in view of September 11th…that it incorporated everything that we thought should be there."

# Core Competencies Expected of Graduate with 18 Credit Hour Minor in Security Management: Power Point Presentation

**Michael S. Magill**
Moderator

## Undergraduate Group 1

**Core Competencies Expected of Graduate with 18 Credit Hour Minor in Security Management.**

## Undergraduate Group 1

- Eduardo Garcia
- Robert Granzow
- Christopher Richardson
- Michael Magill
- Michael Moberly
- D.A. Niichter
- Mark Raybould
- Stephen Sloan
- Robert Stokes
- John Sullivan

## Undergraduate Group 1

- **Demonstrate an Understanding of the Relative Bodies of Law**
- **Applies to Both Graduate and Undergraduate**

## Undergraduate Group 1

- **Manage Physical Security Systems**
- **Applies to both Graduate and Undergraduate**

## Undergraduate Group 1

- **Demonstrate an Understanding of Fiscal Management**
- **Applies to Both Graduate and Undergraduate**

## Undergraduate Group 1

- **Manage Performance of Employees and/or Contractors**
- **Applies to both Graduate and Undergraduate**

## Undergraduate Group 1

- **Demonstrate the Ability to Gather, Analyze, Interpret and Act Upon Data and Information**
- **Applies to Both Graduate and Undergraduate**

## Undergraduate Group 1

- **Demonstrate the Ability to Implement Critical Incident Management Plans**
- **Applies to Both Graduate and Undergraduate**

## Undergraduate Group 1

- **Demonstrate the Ability to Conduct and Manage Investigations**
- **Applies to Both Graduate and Undergraduate**

## Undergraduate Group 1

- **Demonstrate an Understanding of the Principles Regarding Information Protection**
- **Applies to Both Graduate and Undergraduate**

## Undergraduate Group 1

- **Communicate an Understanding of Ethical Issues in the Workplace.**
- **Applies to Both Graduate and Undergraduate**

## Undergraduate Group 1

- **Demonstrate an Understanding of Crime, Crime Prevention, and the Criminal Justice System**
- **Applies to Undergraduate**

**Jim McClanahan, Ed.D.**
Facilitator
Undergraduate Group #2

Dr. McClanahan prefaced his presentation by observing that "what we came up with … actually maps into, pretty well, what group one came up with."

1. **Communications skills**
    - Ability to speak in public or in groups
    - Ability to write effectively
2. **They should be able to do risk assessments.**
    - Ability to identify the assets, identify what the threat environment is, vulnerabilities
    - Know about information protection
    - Have vision and skills
3. **Ability to manage**
    - Know the basic things such as what is a budget, how to go about auditing, perhaps a little project management
4. **Being able to do cost-benefit, risk analysis, non-risk analysis, return on investment; to speak the language of business, basically, in dollars and cents.**
5. **Critical thinking, decision making**
    - Research methods
    - Ability to apply the scientific method to approach and solve problems
    - Make sound decisions based on empirical evidence
6. **Knowledge of legal issues**
7. **Investigation skills, physical security systems**
    - Knowing about available systems and how to manage them

**8. Leadership skills**

- Knowledge of and ability to write about policies and procedures

**9. Risk management**

- Safety and crisis management
- Disaster management
- Intelligence gathering

**10. Theoretical aspects**

- CPTED
- Deterrence

**11. Terrorism**

- Domestic
- International
- Cyber-terrorism
- Workplace violence

**Question/Comment:**

Under risk management, did you talk about (insurance) at all, as one of your subsets? Talk about liability?

**Answer:** While Dr. McClanahan didn't appear to have the opportunity to answer, someone described an emerging trend where corporations are looking beyond risk management as a negative process, but rather were starting to consider the opportunities that become available when risks are effectively managed.

**Mike:** Question about the Norman courses—What did your group come up with…?

**Dr. McClanahan:** "We talked about that and the one area that might need a little bit of tweaking concerns international terrorism. But that was still covered in those courses from Norman. It's interesting, even though the process might have been backwards, what resulted was pretty consistent. So, we felt that those courses did cover what we were looking at."

**Question/Comment:**

Under the core competencies for finance, auditing is listed as a core competency. And I'd have kind of a question about that, because auditing is a discipline in and of itself that people take masters degree. If it were an introduction to audit methodology or understanding of what auditors do, but I don't think auditing is a core competency for this kind of undergraduate degree.

**Dr. McClanahan:** "When we were looking at auditing, we're looking at it from perspective of conducting a site survey or inspection. So we look at auditing, even though, not necessarily in the financial sense.

"Also, one thing. We did stress this in our meetings: when we look at a core competency, we stressed to ourselves that we didn't expect the student to have expertise in this."

**David Gilmore:** One thing, I think it's safe to say that we're probably going to be coming back to group 2 and asking you perhaps, to do some reformatting. The reason I say that is because, when you look at group 1, group 1 indicated communicate X, or demonstrate Y, or do something and they put it into more of a measurable context. And I think we will be coming back and asking you to do the same thing. I think that's going to alleviate some of the questions here on business skills. For example, what is it you expect of a graduate? You want the graduate to demonstrate an awareness of budgeting?

The thing to keep in mind is that when you get into the validation part you can say, "Demonstrate an understanding of the principles of whatever by listing the following." Everything should be measurable. If you can't measure it, you have no way of knowing whether that has been accomplished. And that is one of the problems that everybody has with outcomes.

**Dr. McClanahan:** "I can't leave the room without saying something about 9-11. And, we did speak about the possible inclusion of homeland security. The word was not appropriate for the time, but we did speak about the possibilities of covering some of the gaps that the public sector needs as a result of redeployments. An example of that is the FBI's emphasis on counter-terrorism, who's going to watch banks, and other potential gaps. So, whether or not there's changes to the original curriculums and so forth, I think a healthy awareness of knowing the possibility of filling gaps."

# CORE COMPETENCIES: POWER POINT PRESENTATION

**Jim McClanahan, Ed.D.**
Facilator

Undergrad Group 2

## Core Competencies

- Communication Skills
  - Writing
  - Speaking
- Risk Assessment
  - Surveys
  - Identify Assets
  - Threats
  - Vulnerabilities
  - Information Protection

## Core Competencies

- Business Skills
  - Auditing
  - Budgeting
  - Proj Mgmt
  - ROI
  - Cost Benefit
  - Scheduling

## Core Competencies

- Critical Thinking
  - Decision Making
  - Research Methods
  - Ethics
- Knowledge of Legal Issues
  - Aspects
  - Authority

## Core Competencies

- Basic Investigation Skills
  - Interviewing
  - Background Investigations
- Physical Security Systems
- Leadership Skills
  - Supervision
- Policies & Procedures

## Core Competencies

- Risk Management
  - Safety
  - Fire Life Safety
  - Disaster Mgmt
  - Crisis Mgmt
  - Intelligence

## Core Competencies Cont.

- Theoretical Aspects
  - CPTED
  - Deterence Theory
- Terrorism
  - Domestic
  - International
  - Cyber Terrorism
  - Workplace Violence

## Summary of Graduate Breakout Group #1
## Breakout Group Presentations

**Kevin Peterson, CPP**
Facilitator
Graduate Group #1

Kevin Peterson explained how they categorized the core competencies into three areas, "that we called people skills, performance skills and business management skills. The people skills deal with the student's ability to interact with others at all levels. The performance skills get down to the core security functions, doing security. And then the business management skills are pretty much self-explanatory: how to operate in a business environment and incorporate security into business and business into security."

People skills

1. **Ability to effectively manage people in any type of organizational setting and deal with those human resources issues**
    - Definition requirements for personnel
    - Hiring
    - Evaluation
    - Motivation
2. **Ability or skill of being able to influence people, in various settings, both on a crisis situation and on a day-to-day basis.**
3. **Superior communication skills.**
    - Oral and written products
    - Ability to effectively leverage automation and be able to use those computer systems to gather information and communicate information in the business and organizational environment
    - Very heavy competency in liaison

4. **Ability to communicate at the executive level.**

Performance skills

5. **Ability to conduct research and analysis**

    - Gather and analyze information
    - Correlate data and using that to draw conclusions and applying that information.

6. **Critical thinking skills: the ability to quickly and accurately and creatively evaluate information from multiple sources.**

7. **Possess a thorough understanding of legal, regulatory and policy issues,** including ethical issues.

8. **Possess a thorough understanding and ability to deal with risk management and risk analysis. This covers the entire spectrum of risks.**

    - Terrorism
    - Internal threats
    - Financial threats
    - White-collar crimes
    - Business continuity issues
    - Crisis management, all those things

9. **Investigations, especially in the corporate environment.**

    - White collar crimes, ex., the Enron situation
    - Ethical issues
    - Strong auditing capabilities, not in the financial sense, but to have a good understanding of the auditing function
    - Understand the role of security and asset protection
    - As a conceptual issue
    - As it relates to the corporate or organizational environment:
    - Corporate politics, corporate mission and how the assets protection function fits into all that and vice versa.

Business and organization management skills

**10. Possess an understanding a systems approach**

- How many different aspects or functions work together
- Demonstrate creativity in addressing security-related issues

**11. Demonstrate the ability to manage very large and complex issues or projects.**

**12. Able to financially justify security programs and demonstrate value that is added to an organizational mission.**

**13. Understand the need and demonstrate the ability to operate across different types of organizational structures.**

This competency was developed to address the broad range of organizational structures in use today. The security professional needs to operate across the spectrum of those organizational structures.

In addition to the core competencies, they identified other skills that might prove helpful such as some foreign language ability and a thorough understanding of international business environments. They also agreed that any graduate program needs to include some mechanism to allow the student to demonstrate core competencies before they graduate. This could be a thesis defense or a comprehensive exam or some mechanism of demonstration prior to graduation.

Finally, Peterson reported that the group agreed that the core competencies could be achieved throughout the courses that were outlined under the graduate program at Norman. However, they also felt that some area of concentration or specialization might be recommended at the graduate level. Moreover, they also concurred that these core competencies and the courses that were outlined in Norman remain appropriate even in the post-9-11 environment.

**Question/Comment:**

Someone from the audience remarked on how the work between the undergraduate and graduate levels begins to overlap. At the undergraduate level, the effort seems to focus on "providing the basics, the understanding, the principles, just so that the person understands what's involved. At the graduate level, it's more application. In other words, taking that material and knowing what to do with it. Knowing the right questions, how to respond and providing solutions to problems."

# CORE COMPETENCIES FOR PROSPECTIVE EMPLOYERS
# POWERPOINT SLIDE PRESENTATION

**Kevin Peterson, CPP**
Facilitator

*2002 Academic/Practitioner Symposium*

Graduate Group 1

**Core Competencies for Prospective Employers**
**PEOPLE SKILLS**

Demonstrate the ability to effectively manage people in an organizational setting including the functions of requirements definition, hiring, evaluation, motivation, development, training and discipline.

Be able to diplomatically, but effectively influence people at all levels of an organization and in various organizational settings; and demonstrate the ability to direct, influence and control people to accomplish security and safety objectives in a crisis situation.

*2002 Academic/Practitioner Symposium*

Graduate Group 1

**Core Competencies for Prospective Employers**
**PEOPLE SKILLS** (continued)

Demonstrate effective communications skills including oral presentations, written products, the use of automated information systems resources, and and the application of both internal and external liaison; and demonstrate effective executive communications skills to deal with, convince and educate senior members of an organization's leadership and/or senior government officials.

*2002 Academic/Practitioner Symposium*

Graduate Group 1

**Core Competencies for Prospective Employers**
**PERFORMANCE SKILLS**

Apply sophisticated research and analysis methods to security and assets protection-related issues to gather data, analyze/evaluate data and draw plausible conclusions.

Demonstrate critical thinking skills in quickly and accurately evaluating information from multiple sources.

Understand the breadth of legal, regulatory, policy and ethical issues in a corporate, government or organizational setting, and its impact on security and assets protection.

*2002 Academic/Practitioner Symposium*

Graduate Group 1

**Core Competencies for Prospective Employers**
**PERFORMANCE SKILLS** (continued)

Demonstrate a thorough understanding of and ability to apply contemporary risk management approaches including risk assessment employing the most recent techniques and technologies.

Demonstrate effective investigative, auditing and white collar crime prevention and detection methodologies, particularly as they apply to the corporate environment.

Fully understand the role of security and assets protection from an organizational dynamics, ethics and corporate mission perspective.

*2002 Academic/Practitioner Symposium*

Graduate Group 1

**Core Competencies for Prospective Employers**
**BUSINESS & ORGANIZATIONAL MANAGEMENT SKILLS**

Fully understand the systems approach to problem solving and demonstrate creativity in addressing contemporary security-related issues.

Demonstrate the ability to manage large, complex projects.

Be able to financially justify security programs and strategies, and demonstrate value added to the organization's mission .

*2002 Academic/Practitioner Symposium*

Graduate Group 1

**Core Competencies for Prospective Employers**
**BUSINESS & ORGANIZATIONAL MANAGEMENT SKILLS** (continued)

Understand the need and demonsrate the ability to effectively operate in a variety of organizational structures including matrix organizations, vertical organizations, non-structured organizations, and be able to transition among them while accomplishing security objectives.

*2002 Academic/Practitioner Symposium*

Graduate Group 1

**Core Competencies for Prospective Employers**

OTHER ISSUES . . .

Desired/enhancing competencies

Foreign Language Ability

Thorough Understanding of International Business Environment

The Group agreed that a thesis/defense, comprehensive exam and/or some other means of demonstrating these competencies prior to graduation is important.

*2002 Academic/Practitioner Symposium*

Graduate Group 1

**Core Competencies for Prospective Employers**

OTHER ISSUES (continued) . . .

The Group agreed that the identified core competencies could be achieved through the courses outlined at the Norman, OK Symposium as long as additional courses in an "area of concentration" and electives also support the core competencies.

The Group agreed that the identified core competencies adequately address the post September 11 security and assets protection environment.

**Eva Vincze, Ph.D.**
Facilitator
Graduate Group #2

Dr. Vincze started by putting the audience on notice that "our rationale was a little bit different." Without a definition of what security management really was, they found it difficult to identify core competencies.

"So, we broke the rules, or we changed the rules, we didn't break the rules, and we decided to spend a large part of our time defining what security management was from step 1 and then doing core competencies from there."

- Definition of Security: The protection of assets.

- Five elements subsumed under the definition:

    1. Identify and describe threats to assets

    2. Identify and describe vulnerabilities of assets

    3. Design, select, and deploy countermeasures

    4. Evaluate, understand and communicate consequences of losses

    5. Understand the overall impact of security

After "developing this nice little elegant model… we had about, what, thirty minutes left, in order to go on to the next step." Therefore, without time to develop the core competencies, they developed a description of what a core competency should be.

- Definition of Core Competency: The knowledge and skills needed to efficiently and effectively manage and lead the security function.

They did agree that the various elements that were delineated in Norman linked directly to the core competencies as well.

**Question/Comment:**

Someone gave Eva a "heads up" that they would be asked to flesh out the competencies and reconcile their model with the other graduate group.

**Eva**: She responded that she felt that her group "did the first step, they (the other graduate group) did the second and then we've got the third step."

**David Gilmore**: Gilmore explained how their intention was to eventually reconcile the work produced by each group.

Gilmore continued by sharing a conversation he had had the previous day with Professor Martin Gill, who commented that the problem that many people have in defining security is agreeing on those underlying principles. Gilmore tends to refer to them as "defining characteristics."

In response to this problem, Gilmore suggested that they take the current 18-point model and "bump those elements against those principles, and see whether or not they fit. And if they fit one or more of those, they would stay as part of the model; if they did not fit one or more of those, they would drop out." This would also address a valid criticism that the 18-point model is not tied to anything.

Another benefit would be to help John Tippit in his efforts to define security from the standpoint of function, not from the standpoint of position. One of the troubles in creating the curriculum model, believes Gilmore, "was that people evaluated and determined those things that constitute the world of security, based on their own experience and their own situation. That's not really what we wanted them to do, but that's what they did." He continued, "The difficulty we had with the model was, we kept hanging things onto it, and we kept trying to make that umbrella bigger to put as many things under it as possible." The danger in making the umbrella bigger is that more things will need to be incorporated into a security education program—including core competencies—at which point how will students at either level acquire so many competencies?

**Question/Comment:**

Mike Magill makes the point that students should be exposed as much as possible to as many things as possible in school because they're sure to encounter it in the real world.

**Question/Comment:**

Dr. Calder reminded them that "universities are about teaching people to think, to read, to study, to evaluate, to analyze. They don't do well when they're into finite details such as parking lot striping…"

**Question/Comment:**

As a follow-up comment, someone draws attention to the fact that security positions and titles are dynamic and fluid, and often change as an organization's fortunes rise and fall. Therefore, they should avoid the danger of tying the core competencies to the "moving line, the ever-changing role of the security director…Because if we keep moving after that moving line, we'll never catch up to it."

**Question/Comment:** Dr. Vincze closed out this session with a comment on the difference between developing generalists and developing specialists. She believes that the group should be developing really strong generalists.

## SUMMAY OF GRADUATE BREAKOUT GROUP #2
## POWERPOINT SLIDE PRESENTATION

**Eva Vincze, Ph.D.**
Facilitator

### Graduate Group 2

Dr. Eva Vincze - Leader

### Assigned Task

Task 1 – Define those core competencies that students should have when they complete graduate security education Programs.

Task 2 – Validate the curriculum models that were developed in 2000 in light of 9/11.

### Security is the POA (anything of value)

- Identifying and describing threats to assets
- Identifying and describing vulnerabilities of assets
- Design, selection and deployment of countermeasures
- Evaluating, understanding and communicating consequenses of losses
- Understanding the overall impact of security

### Security Requires Competency in:

Knowledge and skills to effectively and efficiently manage and lead the security function

List of competencies should map directly to the individual components of POA

## Plenary Session #5: Open Discussion and Symposium Wrap-Up

**David H. Gilmore, CPP**
Chairman, Academic/Practitioner Symposium
Moderator

After taking care of a few administrative matters and before opening the floor to discussion, Gilmore indicated that Professor Gill had a few follow-up comments.

**Martin Gill:** Professor Gill primarily wanted to speak to the group about *Security Journal* magazine and how this publication "is quite relevant to the audience here because the journal contains papers that are all independently refereed." Every discipline has a journal where quality, cutting-edge research is reported and for the security industry, that publication is *Security Journal.*. More importantly, he announced that all the abstracts from all the previous papers plus abstracts from papers in twelve other journals relating to security-related topics "have been put into the security-enriched database…" This gives anyone researching a security-related topic a powerful tool. He also encouraged anyone who is writing a paper or who knows of any one else conducting research, to contact Dr. Bonnie Fisher, the American editor.

In response to a question, Professor Gill noted that the turnaround time for response was less than six weeks. He also requested that if anyone is interested in reviewing a book or there's a book that they'd like to see reviewed, to please contact him.

**Dave Gilmore, CPP:** Gilmore reminded the group of the annual ASIS Student Writing Competition. Students at the undergraduate and the graduate level are invited to submit papers for consideration, with the goal of encouraging scholarly research and writing among college students.

An individual submitting a paper need not be majoring in security—they do need to write about a security-related topic. A panel of individuals—three academicians appointed by Gilmore and two practitioners appointed by the President of the ASIS Foundation Board—do a blind evaluation.

While it was too late as of the date of the symposium to submit entries for 2002, he encouraged academicians to have their students think about writing a paper and submitting it by the 15th of July 2003. The call for papers will appear on the Web site for next year.

With this, he opened the floor to Van Holladay who wished to make some remarks.

**Van Holladay, CPP**: Van Holladay suggested that it's time to "branch out a little bit and try to bring in another element to our conference so that we can advertise, sell, outreach, whatever you want to call it. Because I think we're preaching to the choir a little too much." He recommended bringing in college counselors, deans and others not in the security industry. Further, he supported the advertising effort because "we need to sell Congress, we need to sell the Fortune 500 security guys as well as their bosses."

**Dave Gilmore:** After thanking Van, Gilmore wanted to also congratulate him on the celebration of his upcoming retirement and recognize the many honors that he earned throughout his career, including being recognized as Professor of the Year at two different campuses of the Northern Virginia Community College system.

He went on to describe a conversation from the previous night where John Sullivan [faculty member at Penn State's Abington College] asked if it would be possible for ASIS to make available to the academic community, a list of those enterprises that would have internship opportunities. Gilmore's reply had been that he hoped whoever's enterprise was in a given geographic area, would also be represented in the local ASIS chapter, and that they would be prepared to support interns who had an interest in security.

Gilmore also checked with Dr. Richards and was reminded that in that second component of the security education career study going out to Fortune 500s, there is a question about intern programs. Once they receive and process the data from this questionnaire, they can see if there's a way to make that information available.

**Question/Comment:**

When Gilmore expressed his feelings that internships are often like "crap shoots," this audience member countered with his own experience placing students in various internships. According to this gentleman, "I select really good people that I know are going to be successful. Five years later those students are still bubbling and really great advertisement for security. So, I think we must select good people."

**Dave Gilmore:** Gilmore, putting his "crap shoot" comment in the proper context, asked John Sullivan to explain the possible responses from students in these internship positions.

**John Sullivan**: John Sullivan proceeded to explain that in general, the student comes back from an internship with one of three responses. (1) It was the absolute worst experience. As far as Sullivan is concerned, however, this is a successful internship because the student now knows that "he doesn't belong and he's willing to leave, fine, goodbye." (2) It was the absolute best experience. Once again, this is considered a successful internship. However, if (3) "a student comes back and says I still don't know what the hell I do," in that case, Sullivan considers that a failure because the student didn't learn anything, especially about their future career in the security industry.

It's a time-consuming, expensive process that could be made easier if ASIS provided a database of interested companies.

**Dr. Steve Sloan**: In his university's program, they're also very careful to make sure that the employer understands that they're not linking staff.

**Question/Comment:**

Dr. Eva Vincze shared how her university had been recognized as a "center of excellence on the information security side." The benefit of this designation is that the university, along with the National Security Agency (NSA), makes available one million dollars worth of scholarship money for students. Once a student is accepted into the program, the student performs a two-year internship and after graduate school, promises to work for two years somewhere in DoD. She wonders if the ASIS Foundation would consider making available scholarship money in conjunction with other companies or organizations in a similar approach.

**Question/Comment:**

Dr. Calder related how most universities look at internships as a vehicle for learning, and not career progression. He also noted that in universities that require internships, such as his own, there is often a full-time coordinator who can serve as a resource person. He also suggested contacting the local ASIS chapters as well criminal justice and business departments of those universities that do have internship programs.

**Dave Gilmore:** Before wrapping up the proceedings, Gilmore requested that Dr. Bob McCrie talk to the group about how the events of September 11 affected him and the John Jay College of Criminal Justice family. They lost some 70 people that day and Bob agreed to share with the group a little of how the college coped with that, what they went through in the aftermath of 9-11.

**Dr. Bob McCrie**: "This was a suggestion of Steve Sloan and I'm happy to respond to it. A word of orientation first. John Jay is part of the City University of New York, which describes us as the world's largest institution concerned with criminal justice and public service. It's natural, therefore, that among the 10,000–11,000 students we have right now, that many would have been involved in the problems that occurred on 9-11. I'd like to ask Jim Fowler to add on anything that he would care to add when I'm through.

Of the 2,823 victims, 70-some were from John Jay, and we knew before noon on September the 11th that we had some serious evaluations to do. School was suspended for two days and then for the next few days, students were welcome to come. We asked all our instructors to be sensitive to the situation to allow some students to respond in their own way and to talk about it in class in a personal way. Subsequently, we held two memorial services at which there was singing, and personal experiences shared among those who had losses and crying. Beyond that, programmatically, we made some changes. We, in my department, established a certificate in security management and anti-terrorism that will begin this fall. We've identified two new courses that we want to offer and those will not start until next spring. We turned to funding sources to help us start a terrorism center. And AOL-Time Warner, despite its problems, has indicated an interest in supporting this. Additionally, we have participated in numerous memorials for the fire department, the police department, for private businesses like Cantor Fitzgerald, where one of our students was working as a support person.

I'll just add some other comments about this. What we learned is that we're teaching the right thing. We have a course at the undergraduate and graduate level in this program on emergency planning. And, it was amazing to see how emergency plans were so successful. Not only was the immediate response effective, the coordination with the support facilities in the community, and contingency plans worked so well, organizations that were severely hurt, nonetheless could continue operations because they had hot sites and they had back-up facilities that went right into place.

Strangely enough, it was because of the concerns of Y2K that the reactions were as good as they could be. After Y2K, persons said that money was not so well spent. But, Y2K shows that for the New York area, it was well spent. We New Yorkers feel that we have been reattached to the nation after 9-11 by the heartfelt responses that have occurred from all over the country and all over the world. And, that's been pretty important to us. What we think about 9-11 as it affects our thinking…

First, that it was the largest, grossly largest, terrorist event ever to have occurred. Second, it was the largest single loss of American lives in one day ever to have occurred, even in wartime. And third, there's never been a circumstance where four airplanes have been skyjacked simultaneously. What we also observed in this event is that it represents a kind of terrorism never seen before. We know about Baader-Meinhof, the M-19, the Irish Republican Army. All of these have had their agents commit harm … they knew their lives were at risk when they acted. But, their intention was not to give up their own lives. With now the success of 9-11 in the eyes of terrorists, there is bound to be further attempts in the future. It seems logical to us. Though, because of the control measures that we're putting into place, they are far better than they were on 9-10 and will be far better one year from now. The likelihood of a terrorist event being successful is likely to be pushed off by quite a period of time. And that's germane to the teaching of our discipline.

Today's a special day for me personally; it's graduation at John Jay. And we have a record number of students graduating from our masters in the Protection Management Program. But, I figured this is more important, for me to be here, to learn how we can make our programs better. And I don't regret that decision. Jim?

**Jim Fowler, CPP**: Well, let me say that I concur with everything Bob has suggested. I would call your attention to an airplane crash in early-December. This was an American Airlines plane that took off, was on its way to Santa Domingo, took off from John F. Kennedy. And when that plane crashed, we thought, my God, the whole thing has started over again. You will remember that they decidedly announced about two hours later, no, though we lost some, 160 or more people in that crash, that it was an accident, it was not terrorism. Last week I was at the Brookings Institution, for a day long evaluation of this, the same issue that Bob is treating. I think his turn of phrase that New York rejoined the rest of the country is very true. We've had fire fighters and police officers and Port Authority officers traveling to various parts of our country. A town in Tennessee bought us a fire truck and presented a fire truck to the City of New York. That makes you feel kind of special and it's a stand up thing. From a personal standpoint, Unilever's position, we were at midtown. We might as well have been in Pittsburgh be-

cause you could see some smoke coming up and later on, you were to become aware of people who lost family in the World Trade Center. This brokerage firm that was mentioned lost approximately 600 people. Towns…suburban Connecticut towns…New Jersey towns…there were a lot of cars remaining at the stations because the owners didn't come back. I think the perspective that Bob is giving you is excellent and I certainly appreciate his decision to be here rather than someplace else today, and to join in this communion of ideas. I don't think that many of us or any of us really predicted what was going to happen irrespective of the clues that are now coming to mind. But, I'd like to ask a question. Please signify by raising your hand, if you think there's going to be another attack. Well, I've asked that question a couple times lately and get the same answers, so you're challenged to think, to be as imaginative as you can be.

**Dave Gilmore:** Gilmore thanked Bob and Jim, and related his personal experiences of that day. He operates out of Arlington, Virginia, and on that day was supposed to have lunch with the top security official in the Department of Defense. Later, he was able to get an Assistant Chief of the Arlington County Fire Department to speak at one of his classes. The chief had been the Incident Commander at the Pentagon because the Arlington County Fire Department held incident command for the first ten days of the incident at which point they officially handed it over to the FBI. He came in and not only did a PowerPoint presentation, but he also stayed for an hour-and-a-half answering questions. During that time, he keyed in on command control communications and some of the issues that they dealt with in handling that incident.

The chief pointed out that there had been a convergence of three major incidents together at the Pentagon: a major structure fire; an airplane crash; and a building collapse. And they were dealing with all three of them, simultaneously. He talked to the group about the lessons learned: a lot of the liaison, a lot of the coordination that had been established beforehand, paid off as a result of that.

In closing this 6th Annual Symposium, Gilmore thanked everyone for doing a great job, especially the breakout group leaders. He expressed his appreciation for the time that the entire group had carved from their schedules to assist ASIS in its mission.

Even if there hadn't been any breakout group reports, he believed the symposium would be a great success because it set the stage and provided the opportunity for "academicians talking to practitioners and…academicians talking to other academicians. You've got them talking about what works, what doesn't work, and what are the possibilities. That's exactly what we're about.

# APPENDIX

# Letter of Invitation

February 28, 2002

Dear Colleague:

On behalf of ASIS, I would like to invite you to attend the Sixth Annual ASIS Academic/Practitioner Symposium, which will be held May 29-31, 2002, at the University of Cincinnati, Cincinnati, Ohio. The Symposium will begin with a welcoming dinner on Wednesday, May 29 and will conclude with lunch on Friday, May 31.

Administrative and scheduling information concerning this year's event is shown at Enclosure 1. **Please complete and return the reply form (Enclosure 2) in the enclosed envelope not later than April 5, 2002.**

Questions concerning the administrative and logistical arrangements should be directed to Sally Krahn, at (703) 518-1441; fax (703) 518-1506; e-mail: skrahn@asisonline.org.

Questions concerning the content of the Symposium should be directed to the undersigned at (703) 685-0826; fax (703) 685-3854; e-mail dgi.csfg@starpower.net or to the Symposium Vice Chairman, Dr. Carl Richards at (202) 561-4382; fax (202) 561-7263; e-mail richarct@webster.edu.

Last year, at the University of Maryland University College, we developed proposed criteria to be used by ASIS in the future accreditation of security education programs. A lot has happened since that Symposium. The attacks of September 11 and the anthrax incidents have put security into the spotlight and have increased the public's awareness of security. I think they have also increased the public's expectations of security. The public expects law enforcement and public and private security to protect them from a widening range of threats. Homeland security, aviation security, and protection against weapons of mass destruction (WMD) have taken on a priority and an urgency that we haven't seen before. Those of us involved with security education need to ensure that we are developing courses and curricula that respond to the needs, requirements and expectations that derive from this new environment in which we find ourselves. This year's Symposium will provide an opportunity for us to determine if we are doing that.

In Cincinnati, as with previous Symposiums, we'll be dividing the attendees into undergraduate and graduate breakout groups. This year, we want to build on the 2001 Symposium by defining those core competencies that we expect individuals to have when they successfully complete undergraduate and graduate security education programs. The identification of core competencies is a necessary part of the accreditation process. At the same time, the development of core competencies will enable us to validate the curriculum models that were developed in Norman,

Oklahoma at the 2000 Symposium. We actually want to validate those models from two perspectives:

- Do the courses that were identified in 2000 correlate with the core competencies that we will develop in 2002?

- Do the courses that were identified in 2000 respond to the challenges resulting from the events of September 11, 2001 and the subsequent anthrax incidents?

The development of core competencies and the validation of the curriculum models will be the primary tasks for this year's Symposium. In addition, Dr. Carl Richards will present a summary of the preliminary findings of the Security and Education Career Study, for which he is the project leader. As you will recall, the Study was a spin-off from a past Symposium.

As you can see we've established two significant tasks for this year's Symposium, as part of our on-going dialog between security academicians and security practitioners. Communication and interaction between these two groups is what the Symposium is all about. I hope you will be able to join us in Cincinnati to help bring these tasks to fruition.

Sincerely,

David H. Gilmore, CPP
Chairman, 2002 Academic/Practitioner Symposium
Chairman, ASIS Council on Academic Programs in Colleges & Universities

## AGENDA

*American Society for Industrial Security*
Sixth Annual Academic/Practitioner Symposium
May 29–31, 2002
University of Cincinnati
Cincinnati, Ohio

**Wednesday, May 29, 2002**

2:00 pm - 6:00 pm **Registration and Refreshments**

6:00 pm - 8:30 pm **Welcome Reception and Dinner**

**Thursday, May 30, 2002**

7:00 am - 8:00 am **Continental Breakfast and Registration**

8:00 am - 10:00 am **Plenary Session #1** - *Welcoming Remarks and Symposium Overview*

**David H. Gilmore, CPP**
Chairman, Academic/Practitioner Symposium
Moderator

**Daniel H. Kropp, CPP**
President- Elect, American Society for Industrial Security
Welcoming Remarks

**Lawrence J. Johnson, Ph.D.**
Dean, College of Education, University of Cincinnati
Welcoming Remarks

**David H. Gilmore, CPP**
Symposium Overview

**John D. Tippit, CPP**
"Research to Support the Education and Training of the Professional Security Practitioner"

10:00 am - 10:15 am **Break**

10:15 am - 11:00 am **Plenary Session #2** - *Update on Symposium Projects and New Initiatives*

**Carl Richards, Ph.D.**
Vice Chairman, Academic/Practitioner Symposium – Moderator

| | |
|---|---|
| 11:00 am - 11:45 am | **Plenary Session #3** - *Open Discussion and Q & A*<br>**David H. Gilmore, CPP –** Moderator |
| Noon - 1:15 pm | **Networking Lunch** |
| 1:30 pm - 3:30 pm | **Breakout Session #1 -** *Organize and begin work on task assignment* |
| 3:30 pm - 3:45 pm | **Break** |
| 3:45 pm - 5:30 pm | **Breakout Session #2 -** *Continue work on task assignment* |
| 5:30 pm - 6:00 pm | **Open Time** |
| 6:00 pm - 8:30 pm | **Reception and Dinner**<br>**Speaker -Professor Martin Gill, Ph.D**<br>University of Leicester, "Security Education: A British Perspective |

**Friday, May 31, 2002**

| | |
|---|---|
| 7:00 am - 8:00 am | **Continental Breakfast** |
| 8:00 am - 9:30 am | **Breakout Session** |
| 9:30 am - 9:45 am | **Break #3** - *Complete work on task assignment* |
| 9:45 am - 10:45 am | **Plenary Session #4 -** *Breakout Group Reports on Task Assignment*<br><br>**Carl Richards, Ph.D.**<br>Moderator |
| 10:45 am - 11:45 am | **Plenary Session #5 -** *Open Discussion and Symposium Wrap-up*<br><br>**David H. Gilmore, CPP –** Moderator |
| Noon - 1:30 pm | **Networking Lunch** |

# Attendees at the 2002 Academic/Practitioner Symposium

Patrick W. Albright
SBC Communications
St. Louis, MO

Randolph D. Brock, III
Fidelity Investments
Boston, MA

James D. Calder, Ph.D., CPP
University of Texas at San Antonio
San Antonio, TX

Leslie N. Cole, Sr., CPP
Leslie Cole Associates, Inc.
Union, NJ

Bonnie S. Fisher, Ph.D.
University of Cincinnati
Cincinnati, OH

James L. Fowler, CPP
Unilever US, Inc.
New York, NY

Eduardo U. Garcia, CFE
MTSSI-Management & Technical Support Services
El Paso, TX

Mary Lynn Garcia, CPP
Sandia National Laboratories
Albuquerque, NM

Dennis M. Giever, Ph.D.
Indiana University of Pennsylvania
Indiana, PA

Martin L. Gill, Ph.D.
Leicester University
Leicester, United Kingdom

David H. Gilmore, CPP
Colonial Safeguards Inc.
Arlington, VA

Michael E. Goodboe, Ed.D., CPP
The Wackenhut Corporation
Palm Beach Gardens, FL

Robert F. Granzow III
Central Pennsylvania College
Summerdale, PA

Van Dale Holladay, CPP
Northern Virginia Community College
Manassas, VA

Dean Hunter
Federal Protective Service
Washington, DC

Thomas R. Jacobus
Genuity Inc
Phoenix, AZ

Daniel H. Kropp, CPP
CAP Index Inc.
Exton, PA

Michael S. Magill
Magill & Associates
Colorado Springs, CO

James R. McClanahan, Ed.D.
Eastern Kentucky University
Richmond, KY

Robert D. McCrie, Ph.D., CPP
John Jay College of Criminal Justice
New York, NY

Michael D. Moberly
Southern Illinois University
Carbondale, IL

D.A. Nichter, CPP
The Institute
Las Vegas, NV

Stanley Onye, Ph.D.
University of Maryland University College
College Park, MD

Walter E. Palmer, CPP
Contact Inc.
Lexngton, KY

Dale Palmgren, PhD
Arizona State University East
Mesa, AZ

Kevin E. Peterson, CPP
Innovative Protection Solutions
Herndon, VA

Philip P. Purpura, CPP
Florence-Darlington Technical College
Florence SC

Mark E. Raybould, CPP
Siemans Building Technologies
Buffalo Grove, IL

Carl T. Richards, Ph.D.
Webster University
Washington, DC

Christopher D. Richardson
Baltimore Marriott Waterfront
Baltimore, MD

Bradley B. Rogers, Ph.D.
Arizona State University-East
Mesa, AZ

Stephen Sloan, Ph.D.
University of Oklahoma
Norman, OK

John D. Spain, Ph.D., CPP
Information Risk Group
Atlanta, GA

Richard St. Clair, Ph.D.
Webster University
Kansas City, MO

Robert Stokes, Ph.D.
University of South Carolina
Columbia, SC 29208

John F. Sullivan
Penn State Abington
Abington, PA

Darryl R. Thibault, J.D., CPP
Pexis Corporation
San Diego, CA

John D. Tippit, CPP
The Tippit Group
Foster City, CA

Eva Vincze, Ph.D.
George Washington University
Lake Ridge, VA

Michael J. Witkowski, Ph.D., CPP
University of Detroit/Mercy
Detroit, MI

# Undergraduate and Graduate Breakout Groups

## May 2002

### Undergraduate Group 1

Eduardo U. Garcia, CFE
Robert F. Granzow III
Michael S. Magill
Michael D. Moberly
D. A. Nichter, CPP
Mark E. Raybould, CPP
Stephen Sloan, Ph.D.
Robert Stokes,Ph.D
John F. Sullivan

### Undergraduate Group 2

Dennis M. Giever, Ph.D.
Michael E. Goodboe, Ed.D., CPP
Dean Hunter
Van Dale Holladay, CPP
Thomas R. Jacobus
Daniel H. Kropp, CPP
James R. McClanahan, Ed.D.
Stanley Onye, Ph.D.

### Graduate Group 1

Randy D. Brock, III
James D. Calder, Ph.D., CPP
Bonnie S. Fishe, Ph.D.
James L. Fowler, CPP
Mary Lynn Garcia, CPP
Robert D. McCrie, Ph.D., CPP
Kevin E. Peterson, CPP
Dale Palmgren, Ph.D.
Richard St. Clair, Ph.D.
Michael J. Witkowski, Ph.D., CPP

### Graduate Group 2

Patrick W. Albright
Leslie N. Cole, Sr., CPP
Martin L. Gill, Ph.D.
Walter Palmer, CPP
Philip P. Purpura, CPP
Carl T. Richards, Ph.D.
Bradley B. Rogers, Ph.D.
John D. Spain, Ph.D., CPP
Darryl R. Thibault, J.D., CPP
John D. Tippit, CPP
Eva Vincze, Ph.D.