THE STATE OF SECURITY MANAGEMENT

A BASELINE PHENOMENOLOGICAL AND EMPIRICAL STUDY

By Kevin E. Peterson, CPP, CIPM II, Innovative Protection Solutions, LLC; and Joe Roberts, PhD, Business QnA

FULL REPORT 2022

The State of Security Management
A Baseline Phenomenological and Empirical Study
Full Report

Primary Authors:
Kevin E. Peterson, CPP, CIPM II
Joe Roberts, PhD

Preface

Built upon prior research and an in-depth study of the present state of security management, this project is meant as a snapshot in time of this specific field which is global in scope and affects peoples' lives, commerce and governance on a daily basis. Perhaps serendipitously, the originators of the idea for this effort chose 2020 as the target year for the study. As we have seen, the period from 2019 through 2021 has been "unique." With global upheaval on several fronts, from pandemic and civil unrest to natural disasters and supply chain disruptions, this period represents, or in some cases, has caused sea changes in the practice and perception of security, security management and risk management that will have lasting impact.

For the purposes of this study, "security management" is treated as both a field of study and a profession. It is distinct from what might be defined as a security discipline, such as physical security, information security, cybersecurity, or personnel security. This is an important point since our findings include a concern of the lack of a clear definition of the field and the need to improve its perception with chief executives as well as the public.

The findings and conclusions here will serve as a baseline for future studies and will support trend analysis to better define and influence the direction and evolution of security risk management and a number of related professions.

We truly appreciate the outstanding support from the ASIS Foundation, ASIS International, and the small, but talented research team we assembled. Of course, we would not have been able to accomplish this task without the many security professionals who participated in the survey, allowed us to interview them, brainstormed with us, and provided advice, ideas, information, and moral support. Finally, we thank by name, Beth Pierce, Peter Ohlhausen and Chris Vane for their patience, advice and assistance.

Table of Contents

EXECUTIVE SUMMARY

Study identifies themes and findings that set a baseline for the current state of the security profession and identifies how the security sector is evolving and changing.

Much has been written about the security industry, security risks and the how-to of security.

Despite the titles of many textbooks, college courses and training programs, there has been little in terms of a deep dive into the very distinctive realm of security management. This study is intended to provide a baseline for the state of security management as of the end of 2020. It views the topic through the lens of a senior security executive or chief security officer in a public or private sector organization of any size or type. The study assumes a global perspective and considers world events over the past two years as well as ways in which the security risk management field has evolved.

During the process of this study, our intent was to sideline discussion or inclusion of the COVID-19 pandemic as much as possible. Our team wanted to gather data based on as normal a condition as possible for the survey and interviews. We quickly learned that was impossible. Real-world events such as widespread civil unrest, economic calamities, natural disasters, and the pandemic were actually reshaping some aspects of security management perception and practice as we watched. This fact truly demonstrated in real time one of our key findings: Security executives and management professionals must embrace change (and do it quickly).

Overall, however, we found that the current state of security management is secure and positive. Despite this fact, as might be expected, there are some concerns and challenges within the profession that need to be addressed. This study seeks to highlight both the positives and negatives of the current situation, acting as a snapshot in time.

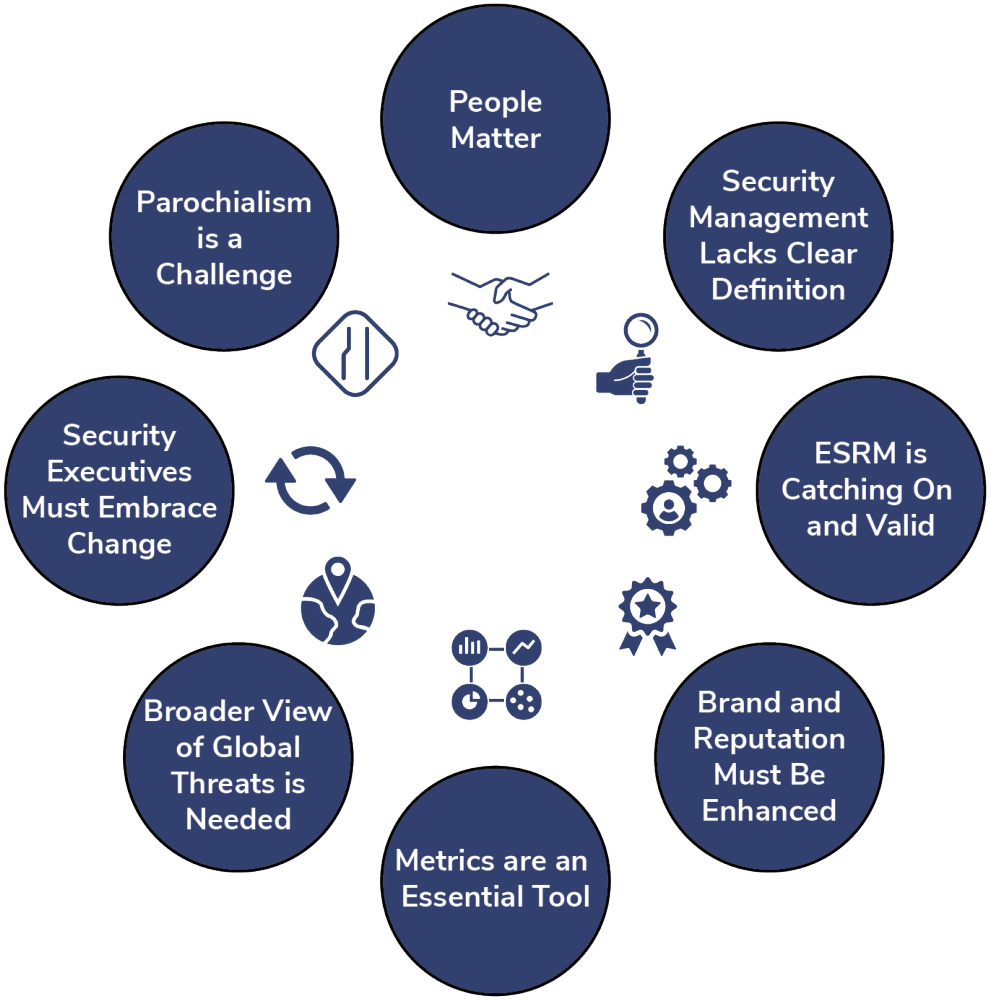
Based on the information gathered from these sources and our analysis, we developed eight key findings, as well as four noteworthy themes which are important, but don't rise to the level of a key finding.

Our Key Findings are:

- People matter (and by nature, security management is a people function as well as a business function)
- Security executives and management professionals must embrace change
- The security management field lacks a clear definition
- Parochialism in the security management field is a challenge
- Enterprise Security Risk Management (ESRM) is catching on and considered viable
- Security professionals need to broaden their perspectives global threats
- The security profession's brand and reputation must be enhanced
- Security management metrics are an increasingly essential tool

Through the noteworthy themes that emerged from the study, we take a brief look at a few issues related to the perception and practice of security management today. Among them are the gender gap within the profession, which is understandable in some ways, but not in others. Then there is the proverbial pink elephant in the room: the common practice of hiring former military or law enforcement members into senior corporate security positions, a practice which has pros and cons. We also note the trend toward security services providers diversifying their market as well as their service offerings to remain relevant and efficient in terms of their business models. Finally, we note that our survey results revealed, in some respects, a divergence between the views of English-speaking and Spanish-speaking participants. These four themes add to the deeper understanding of security management as a profession and some of the issues that influence both the perception and practices of the field. Each of the themes lends

Key Findings



Noteworthy Themes

- ✓ Gender Disparity is a Concern
- ✓ Sourcing of Security Professionals is a Concern
- ✓ Security Industry is Diversifying
- ✓ Views Differ by Language and Culture

itself to further study or research, and this report can serve as a launching point for such efforts.

The report concludes with 14 recommendations meant to be actionable steps which are addressed to a variety of audiences including security professionals themselves, employers, academics and researchers, C-Suite executives, and related and allied professional associations. The recommendations focus on areas such as education and certification, brand and reputation management for the profession, the need to expand the scope of risk assessments and other management thinking, increasing the use of data analytics and improved metrics for decision making, further integration of ESRM, and developing marketing strategies to bolster the security management profession.

The results of this baseline study will be useful as a standalone as well as in forming a substantial basis for periodic revisits. Such periodic revisits may update or expand on the issues key to the state of security management, and may also offer an opportunity to focus on specific subjects or challenges of particular interest over time.

Key Findings Infographic

The infographic above summarizes the results of the study. We identified eight key findings regarding the state of the security management field, and four noteworthy themes which also deserve special mention. A description of each key finding and noteworthy theme is provided in the body of this report. In summary security management is a collaborative effort. The individual is not meant to carry the burden on his or her shoulders, but rather serve as a trusted advisor and consultant to other executives and key decision makers throughout the organization.

Methodology

Our study team's methodology included an online survey, interviews of 10 energetic thought leaders in the profession, a literature search, and a special effort to seek definitions for the term "security management."

Coincident with the launch of our literature search, our team began developing a survey meant to be completed by mid-level to senior security executives and professionals (including chief security officers) in both public and private sector organizations. The survey audience specifically excluded security service or product providers, vendors, integrators, and others generally considered to be part of the security industry or services sector.

A pilot survey was distributed to 20 active ASIS International members who fit the profile of the intended audience. They were asked to complete the survey and offer feedback on its format and content. Thirteen security professionals responded to the survey and shared their perspectives. Based on their feedback, the survey questions and format were modified slightly, and a final survey tool consisting of 21 questions established. The survey included both demographic and substantive questions. Demographic questions allowed the team to analyze responses and seek correlation based on such distinctions as industry sector, reporting level, geographic region, ASIS member status, and gender. The substantive questions asked about the challenges faced by security executives, skills they seek, management tools they use, who they collaborate with, and their views on enterprise security risk management (ESRM). The survey was offered both in English and in Spanish in order to accommodate participants, but also to determine whether any significant differences might be found by comparing the results. A total of 545 security professionals completed the survey using a commercial online survey platform.

To complement the survey input, our team also conducted one-on-one (online) interviews with 10 selected thought leaders in the security management field. Interview questions were similar in nature to the survey questions, but offered the opportunity for open-ended answers and the sharing of more detailed thoughts. The thought leaders offered great insight and added context to the results obtained via the survey.

INTRODUCTION

Security management is constantly changing and evolving. Perhaps unlike many other professions, the security management community finds it difficult to achieve consensus on who we are and what we do.

A key characteristic of most professions is that the members and thought leaders tend to rally around a generally-accepted body of knowledge as a point of unity. For the security management community, that body of knowledge includes such sources as the multi-volume Protection of Assets set, the domain content from ASIS' four professional certifications, and ASIS standards and guidelines. There are also external references of value including certain international standards (e.g., the ISO 31000 [Risk Management], 27000 [information security], and 28000 [supply chain security management] series) and university curricula. Finally, there is educational content from other security-related professional associations such as the Security Institute, the International Association for Healthcare Security & Safety, the International Foundation for Cultural Property Protection, and the Loss Prevention Foundation.

A number of studies have been conducted in the past focusing on the security industry itself, or security functions and tasks, or particular security segments. One such landmark study called the Hallcrest Report, examined the private security industry and was published by Cunningham, Strauchs and Van Meter in 1990. This is still a go-to reference for baseline information on private security as an industry and on security-police relationships.

This study, however, is somewhat unique in that it focuses exclusively on the profession of security management in business and organizational settings. It does not address the security industry, per se, which is a separate and distinct entity. Nor does it focus on specific security disciplines, threats, or risks as other research efforts do. It attempts to view the world through the perspective of the chief security officer or senior security executive in a public or private sector organization – and represents a snapshot as of the end of the year 2020.

The study's tagline includes the terms "phenomenological" and "empirical" because there is a need to address both perception and practice to fully comprehend the state of security management.

The ultimate goal of this effort is to develop a baseline assessment of security management across global, discipline, and industry segments. The focus will be equally divided between perception and practice, as both can have dramatic effect on everything from the understanding of organizational threats and vulnerabilities to how and why safety and security programs are designed – and how they participate, interact with, and support the security and safety community, including senior security executives.

This study aims to help define the state of security management and set a benchmark against which to measure progress, areas of interest, and the evolution of the profession in coming years. Over time, these measures and their interpretation will serve to enhance organizational safety and security, inform new management techniques to enhance the value of security management executives in all types of organizations, identify common gaps in security practice or technology, aid in forming

relevant policies, and advance the development and application of enterprise security risk management (ESRM) as a foundational concept.

Need for the Research

The appellation "security management" means vastly different things to different people...and organizations. The differences can be based on such attributes as language, geographic location, industry sector, profession, specialty, or context. This disparity can lead to organizational conflicts that significantly degrade the security and safety posture, damage critical relationships, waste valuable resources, and hamper the ability to achieve strategic goals. Conflict can also negate potential synergies that could otherwise serve to more effectively and efficiently manage security-related risk or establish a more safe and secure posture.

The need for this research is aptly demonstrated by two occurrences. First, the 1999 ASIS Academic/Practitioner Symposium presented attendees with a task to define "security management" and relate it to a set of subspecialties. The results were unexpected and frustrating to the organizers. In the end, there was little consensus on what security management is. The question, it seemed, was far more complicated than the facilitators expected – and the objective of using the conclusions to help inform educational content and curriculum models was thwarted to some extent. The challenge was raised again at the 2000 symposium, and eventually a curriculum model for undergraduate and graduate studies was developed. The questions surrounding an accepted definition of security management, however, persisted.

Fast forward to February 2020. In an ASIS Connects Open Forum post, a corporate security manager was lamenting that a survey she conducted among company employees indicated that people in her company viewed corporate security as nothing more than security guards. This is a clear indicator that we need to do a better job at not just educating, but actually connecting perception to practice as a security risk management tool; and research like this project is needed in order to lay the groundwork for that to occur.

Confusion over everything from groundbreaking, but evolving paradigms like ESRM to fleeting concepts and ill-defined terms such as "convergence," compounded by an ever-changing relationship between cybersecurity and traditional (sometimes referred to as operational) security seem to cause havoc in our profession and among the organizations we serve. This makes it difficult to successfully carry out our job of enabling the achievement of an organization's strategic goals by managing security-related risk and providing for a safe and secure operating environment. Essentially, it makes a difficult responsibility even more difficult – perhaps unnecessarily so. And this is a global phenomenon.

In an era of constant and rapid change in all arenas, a clear understanding of security management – in terms of perception and practice – is critical. This study will help foster that understanding and carry it into the future. It can also serve as a tool to aid security professionals in communicating their profession's identity to executives and stakeholders of all sorts.

RESEARCH METHODOLOGY

Under the initial project plan, three primary instruments or research constructs were to be used to gather data and develop perspectives for the effort:

- Literature search
- Survey of senior and mid-level security executives
- Thought leader interviews

As the project planning progressed, the research team determined it would be helpful to make some further inquiry into the definition of security management. Therefore, a fourth instrument was developed in the form of a small, targeted literature search and a pretext inquiry sent to five professional associations that deal with security management. The limited literature search focused on university textbooks related to the field, professional publications, and an internet search. The pretext inquiry consisted of an e-mail sent to the organizations most likely to be able to provide a credible definition for the term or concept of security management. Although the subject of definition was addressed in both the survey of security professionals and the thought leader interviews, the team felt strongly that this additional step would provide valuable insight.

The research team developed and conducted a survey using an online tool to gather information and perspectives from current (or recently retired) senior and mid-level security executives. Survey questions were formulated to gather both demographic and substantive information, and designed to capture data on perceptions and practices of security management professionals around the world. In addition to typical answer choices, respondents were able to write narrative comments for most of the questions. This allowed the opportunity for participants to expand or elaborate on their answers, or explain certain aspects of their answer.

Researchers distributed an initial pilot survey to 20 known security executives, and 13 responses were returned. Based on the answers provided and additional feedback from the pilot audience, researchers made minor adjustments to the content and format of the questions. Due to the minimal nature of the changes, responses from the pilot audience were included in the overall dataset along with the subsequent primary survey responses.

ASIS International assisted with distribution of the online survey invitations directed toward active and recently retired senior and mid-level security managers, chief security officers, and senior security executives serving in both public and private sector organizations worldwide. The surveys were available in both English and Spanish language versions, with the Spanish version having been translated manually, tested, and adjusted to ensure equivalence with the English language version.

Overall, the survey responses were as follows:

- Pilot surveys returned (English language): 13
- English language surveys returned: 394
- Spanish language surveys returned: 138

Overall, the survey garnered 545 responses from individuals in 70 separate countries. Researchers analyzed the results across three main demographic categories: geographic region, industry sector, and primary security discipline of the respondent. Results were evaluated for validity and the answers analyzed and extrapolated to provide deeper understanding of how the three main discriminators as well as language used by the respondent affected survey data.

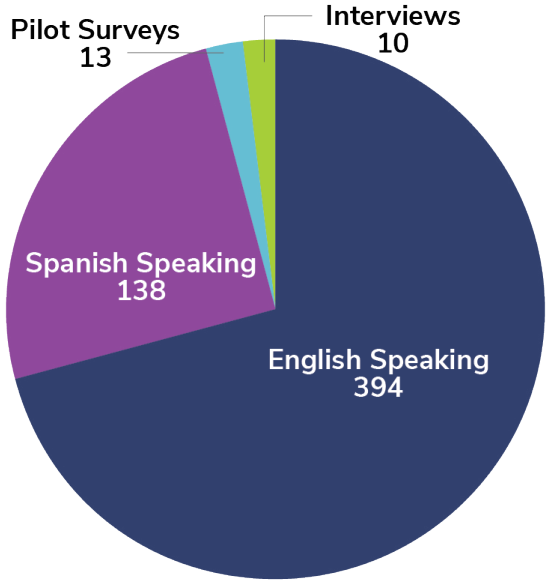
Researchers used SPSS IBM Statistical software and other tools to analyze the findings and gain an understanding of the data the survey gathered. Researchers also applied rigorous quality controls to ensure data gathering and analysis followed best practices. They checked and reviewed the questionnaire, conducted a pilot test with it, and used the feedback from the pilot test to adjust syntax and scaling to account for industry-specific nuances and jargon.

In addition the research team conducted one-on-one interviews, via an online meeting tool, of 10 selected thought leaders in the field of security management. These individuals were extremely well qualified, highly experienced, and heavily engaged in giving back to the profession (thought leaders and their qualifications are listed in Appendix D). Each has also published on the subject matter, taught classes or spoken at large-venue professional conferences.

Researchers asked the thought leaders a series of eight questions which were consistent with and similar to those asked in the online survey.

Information gleaned from the literature research, survey, thought leader interviews, and definition research was collated, interpreted and integrated to form the basis of this State of Security report.

Figure 2: Survey Participants by Category



DEFINING SECURITY MANAGEMENT

In order to test the theory that security management is not well defined, the research team took the following steps:

- A targeted literature search of textbooks and other references
- A pretext communication to security management associations requesting their definition of the term

The information gleaned from these instruments was integrated with other data points including results from the survey of security professionals, thought leader interviews, and primary literature searches. The assembled input from all of these instruments is reported in the Findings section of this report.

The objective of the targeted (limited scope) literature search was to identify a decisive and specific definition of security management (not "security" or the "security industry"). The team examined well-respected and recognized textbooks and other sources on the subject, including:

Textbooks

Effective Security Management, 6th and 7th editions, by Charles Sennewald (2016 and 2020); Elsevier Butterworth-Heinemann, Kidlington, Oxford UK

Handbook of Loss Prevention and Crime Prevention, 5th edition, by Lawrence J. Fennelly (ed) (2012); Elsevier Butterworth-Heinemann, Kidlington, Oxford UK

Introduction to Security, 10th edition, by Robert Fischer, Edward Halibozek and David Walters (2019); Elsevier Butterworth-Heinemann, Kidlington, Oxford UK

Introduction to Security: Operations and Management, 5th edition, by Brian Johnson and Patrick Ortmeier (2017); Pearson, London, UK

Professional Security Management: A Strategic Guide, by Charles Swanson (2021); Rutledge, London, UK

Security and Loss Prevention: An Introduction, 7th edition, by Philip Purpura (2018); Elsevier Butterworth-Heinemann, Kidlington, Oxford UK

Security Operations Management, 3rd edition, by Robert McCrie (2016); Elsevier Butterworth-Heinemann, Kidlington, Oxford UK

Security Supervision and Management: Theory and Practice of Asset Protection, 4th edition, by Sandi Davies, Brion Gilbride and Chris Hertig (eds.) (2015); Elsevier Butterworth-Heinemann, Kidlington, Oxford UK

Strategic Security Management: A Risk Assessment Guide for Decision Makers, by Karim Vellani (2006); Elsevier Butterworth-Heinemann, Kidlington, Oxford UK

Strategic Security Management: A Risk Assessment Guide for Decision Makers, 2nd edition, by Karim Vellani (2020); CRC Press, Boca Raton, FL

Other Reference Materials

Protection of Assets-Security Management Volume (2012 and 2021); ASIS International, Alexandria, VA USA

Chief Security Officer – an Organizational Model (ASIS Standard) (2013); ASIS International, Alexandria, VA USA

ASIS Security Glossary (April 2020); ASIS International, Alexandria, VA USA

Handbook of Security, Martin Gill, editor (2006); Palgrave MacMillan, New York, NY USA

In reviewing these references, the research team found that none of them offered a decisive and specific definition of security management. In *Professional Security Management,* Charles Swanson recognized the problem itself when he wrote: "Security management is a field of study and practical application that has developed particularly over the last three decades or so, and in my opinion is neither fully understood nor appreciated." He went on to speculate as follows regarding a definition: "I suspect if a cross section of security practitioners were asked to define security management, the answer would be something like, 'Security management is the practice of

ensuring the safety of the assets belonging to an organization.'" (Swanson, 2021)

The team's consensus was that Martin Gill, in the *Handbook of Security* came the closest to providing a viable definition: "Managers and executives directing ways to reduce losses in organizations and having the authority and resources to establish programs to meet those objectives." (Gill, 2006, p. 36) This definition is notable in that it recognizes that security management involves directing and operating a program to carry out the relevant functions.

It was surprising to the research team that a clear definition for security management was not included in the ASIS Glossary of Security Terms, or *Protection of Assets-Security Management Volume,* both published by ASIS International.

The website www.definitions.net did include a definition for 'security management,' however the team found it inadequate. This was primarily due to the fact that it described the "process" of security rather than the professional management function that 'security management' is.

Security Management Associations

In the second activity, a member of the research team sent emails to five professional associations that are related to security management. The associations selected were the most prominent ones in the field, and all have an international reach. The email asked each association to provide a definition for the term security management, whether it was a definition they crafted internally, one they borrowed from another cited source, or a generic definition that they use in general practice. The associations contacted were:

- ISMA (International Security Management Association)
  Liz Chamberlin, Executive Director, *Liz@isma.com*
  David McGowan, President, ISMA Board of Directors, *david.mcgowan@tiffany.com*
- ASIS International, *asis@asisonline.org*
- IFPO (International Foundation for Protection Officers), *adminifpo@ifpo.org*
- SIA (Security Industry Association), *info@securityindustry.org*
- Security Institute (United Kingdom), *info@security-institute.org*

The researcher posed as a university graduate student that needed a definition of the term security management for an assigned research project. If the association did not respond within a reasonable time frame, a second email was sent, and then a third if there was no response to the first two.

In the end, only two associations responded to our notional student. The International Foundation for Protection Officers (IFPO) advised that they could not provide a definition for the term. Their response stated: "Good luck with your research. We would love to help but we are really more entry-level security officers and really don't have much to do with the SECURITY MANAGEMENT side of things." In a way, this response makes sense, however at the same time, it is somewhat confusing since the organization oversees publication of a textbook entitled *Security Supervision and Management,* which is in its fourth edition.

The International Security Management Association (ISMA) provided a more substantive response. It read as follows:

> *Thanks very much for reaching out on this topic. ISMA does not adhere to one specific definition of "security management." Rather, we know that each business organization must adjust the definition to fit is individual needs, risks, and structure.*
>
> *That being said, in our opinion, any definition of "security management" will include a process through which the organization's assets are identified, and then systems are developed, documented, and implemented to protect those assets.*
>
> *I hope this is helpful – do not hesitate to reach out in future if we can provide any additional feedback or commentary.*
>
> *(Sent by: Liz Chamberlin, executive director)*

ISMA's executive director makes a good point about the need to tailor the definition in some respects. However, there is also great value in a baseline or standard definition.

Overall, the result of this exercise was disappointing and did not reflect favorably upon

some of the professional associations affiliated with security management.

SURVEY DATA INTERPRETATION

Following is a synopsis of the data gleaned from the responses to the survey of security professionals which was conducted during the final few months of 2020 and the first month of 2021. The surveys submitted were analyzed for accuracy and scale reliability, and found to be reliable. The analysis produced a Cronbach's alpha value of 0.78, indicating that there was internal consistency and that the scales used were reliable. Researchers performed crosstabulation and Pearson Chi-Square tests to determine the statistical significance level of relationships between certain variables in the study. These results are presented later in this section. The respondents agreed that the state of security management is thriving but faced several complex challenges.

Survey results are divided into demographic and substantive questions.

Figure 3: Survey Respondents by Geographic Region

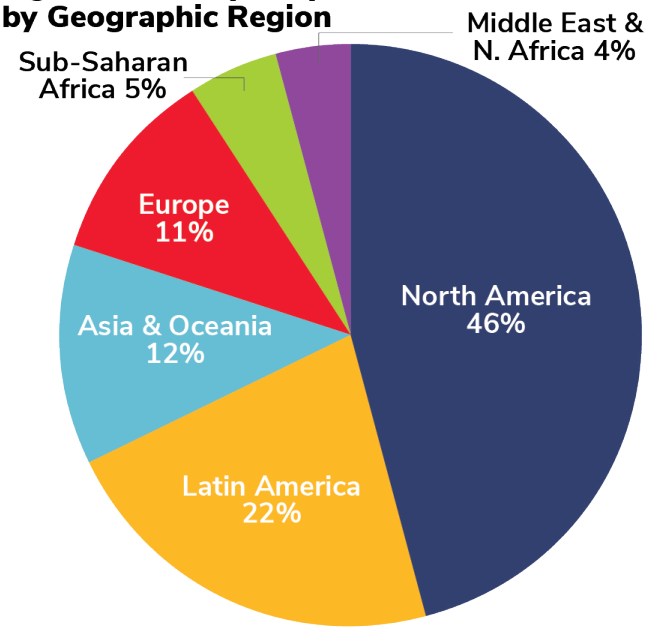
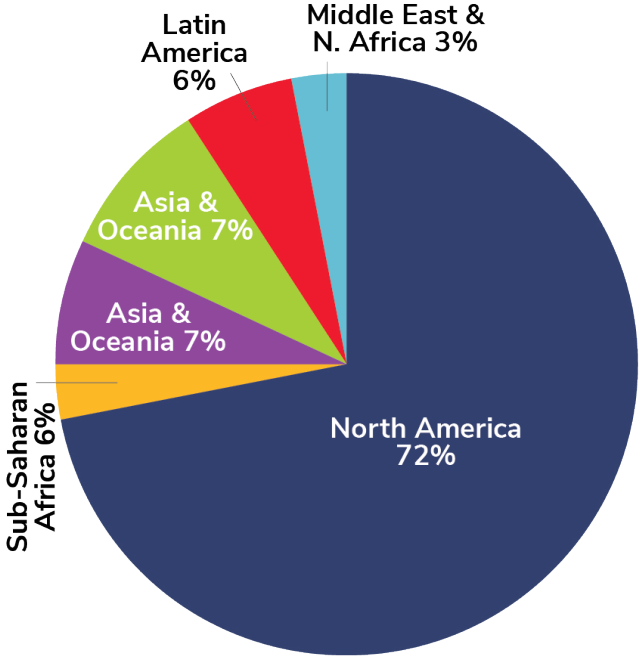


Figure 4: ASIS Members by Geographic Region-2020



Demographic Questions

Survey questions 1 through 8 provided demographic information on the survey respondents. The first demographic question asked about the respondents' location by geographic region. The results are shown in the chart below and compared to the adjoining chart which illustrates ASIS International membership by geographic region.

The industry sectors where the respondents work is seen as a key demographic to understand the landscape of the security management field. Of the 545 respondents, a majority of them worked with financial Institutions. The chart below shows additional industry sectors. Interestingly, the "other" category at 32 percent tells us that there are a wide variety of industries and settings in which security professionals operate around the globe. It should be noted that in the United States the sectors are defined by industry and government. In some other nations the government has direct control over the industry categories and how they are defined. Especially in some areas of Latin America, Asia, and Africa these categories are still emerging.

Overall, it appears that survey respondents represented security professionals across the spectrum of industries and both the public and private sector around the globe.

Another highly relevant demographic is the level within the organization at which the respondent works. The majority of our respondents are senior or C-suite level executives, or regional executives within their organization.

This was exactly the desired survey audience for this study.

Survey respondents belong to a wide variety of professional associations. There was significant representation from the following associations:

- ASIS International: 79.4 percent
- ACFE (Association of Certified Fraud Examiners): 4.2 percent
- ISMA (International Security Management Association): 3.3 percent
- $(ISC)^2$: 2.0 percent
- ISACA: 2.0 percent

Figure 5: Survey Respondents by Industry Sector Category

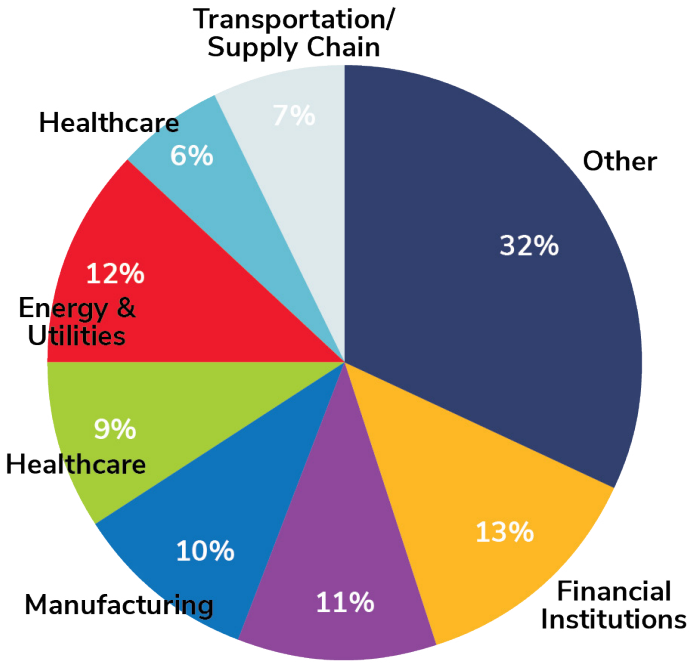
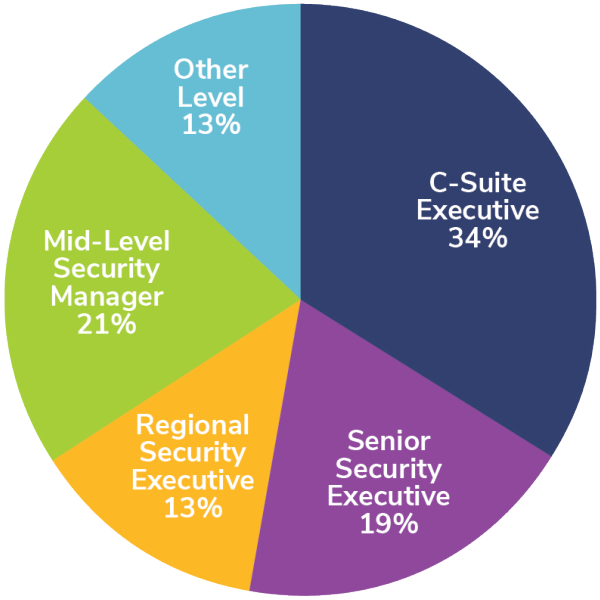


Figure 6: Survey Respondents by Organizational Management Level



Approximately 33 percent of the respondents also listed a number of other associations of which they were members. These included:

- IFPO .....International Foundation for Protection Officers
- IFCPP.....International Foundation for Cultural Property Protection
- IAHSS .....International Association for Healthcare Security and Safety
- IACLEA .....International Association of College Law Enforcement Administrators
- IAEM.....International Association of Emergency Managers
- IACP .....International Association of Chiefs of Police
- ATAP .....Association of Threat Assessment Professionals, The Security Institute
- NCMS.....National Classification Management Society
- BCI.....Business Continuity Institute
- DRI.....Disaster Recovery Institute, and
- TAPA .....Transported Asset Protection Association

This indicates active involvement on the part of mid-level and senior security professionals in professional associations including both those with a broad management interest and those that are specific to certain disciplines or specialties. Informal discussions reveal that there are multiple reasons for this involvement including networking, professional development, educational programs, and the desire to give back (to support others in the field or the profession in general). For many, the motivation to participate is a combination of these.

The survey asked participants to indicate their gender. The responses showed that 88.5 percent were male and 10.7 percent were female (0.8 percent declined to answer the question).

Substantive Questions

The remaining questions in the survey were designed to collect substantive information on challenges, skill sets, practices, and perspectives of security professionals.

Question 9: Which of the following comes closest to your personal definition of "security management?"

Based on the consolidated results for Question 9, two answer choices clearly emerged for the definition of security management. This is discussed further under "The Security Management Field Lacks a Clear Definition" in the findings section of this report.

The two definitions that represented the top choices were:

> A business function designed to protect an organization's assets and ability to perform its mission by identifying, assessing, and managing current and potential security-related risks.
> *and*
> A strategy to protect an organization against all possible threats it may face.

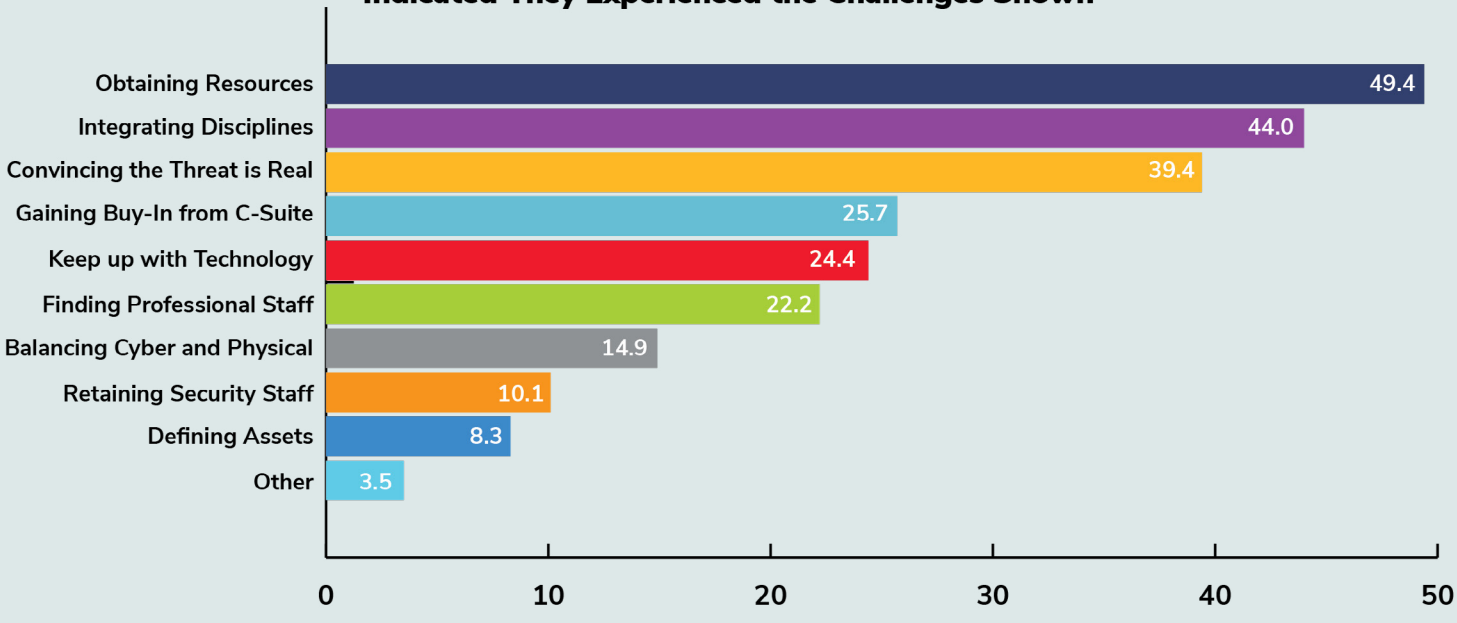
These were the two most comprehensive definitions among the answer choices offered in the survey, and it is not surprising that they stood out among the survey participants.

Question 10: What are your key challenges in performing your security management role and carrying out your responsibilities?

Security management professionals agree on the top challenges they face. Obtaining resources is one challenge that respondents strongly agree with. Other key challenges are integrating disciplines (i.e., avoiding silos) and convincing decision makers that the threat is real.

As shown below it is important to observe that the relationship with the various industry sectors and the key challenges point to some sectors being significantly related to only some of the key challenges. It is perhaps for a future study to answer the question why many of the industry sectors did not show a significant relationship. Perhaps there is a bias toward the challenges as the question was worded or understood. Perhaps the key challenges were shifting due to the COVID-19 pandemic. That so many sectors identified that these challenges do exist is in itself a key result. For this study it is important to mention that the key challenges as seen by the industry sectors need further examination and analysis. Recognizing that security management is borrowing from other fields in how it functions and evolves can also help with the understanding of this result and help with future studies and analysis. At the root of this question is the de-

Figure 7: Percentage of Survey Respondents Who Indicated They Experienced the Challenges Shown



sire to understand what challenges particular industries face so that security professionals can be better prepared to advise on them and address them effectively.

The chart shows where there is a statistically significant correlation between a specific industry sector and a particular challenge security professionals face.

For example, this analysis indicates that the leisure and sports sector finds it challenging to find security staff. This was one of the strongest correlations. A possible explanation is that this sector relies heavily on security officer and executive protection staff for high-profile events. The need for staff may ebb and flow, making it difficult to consistently plan for surges and reductions.

Statistical Significance Crosstabulation Results by Industry Sector on Key Challenges

Industry Sector	Obtaining Resources	Integrating Disciplines	Convince Threat is Real	Keep up with New Tech	Finding Staff	Balance Physical & Cyber	Gaining Buy-in from C-Suite
Federal Gov't							
Local Gov't							
Energy & Utilities							
Broadcast & Media							
Financial & Banking							
Transportation & Supply Chain							
Federal Gov't							
Automotive Sector							
Leisure & Sports Sector							
Education Sector							
High-Tech Sector							

No statistically significant correlation

Statistically significant correlation

Question 11: Please rank the importance of the functions that you believe comprise security management.

Extremely Important (Score=67 to 100)
- Physical Security and Electronic Security Systems
- Employee/Team Awareness and Training
- Emergency/Crisis Management and Business Continuity
- Security Policies and Procedures

Significantly Important (Score=58 to 66)
- Personnel Screening and Background Investigations
- Cybersecurity
- Information/Intellectual Property Protection and Privacy

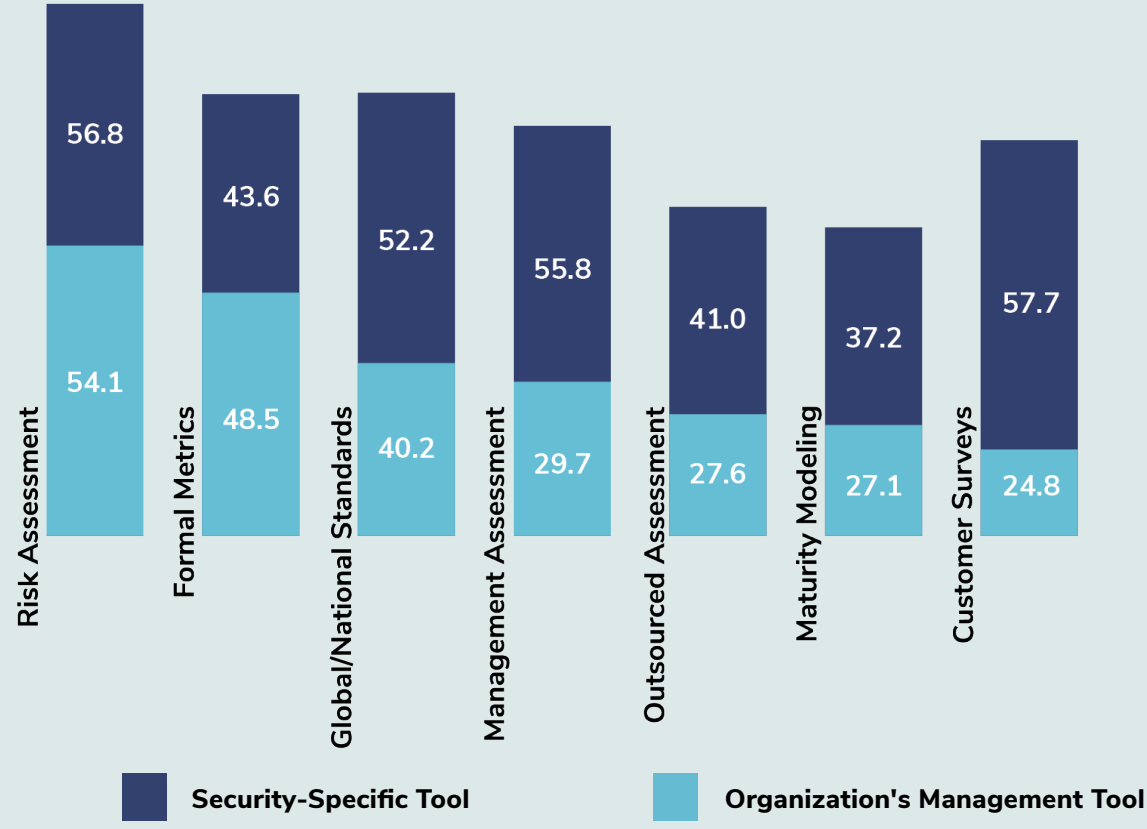
Somewhat Important (Score=30 to 57)
- Investigations
- Liability Management/Legal Protection/ Compliance
- Brand and Reputation Protection/Image Management
- Executive Protection
- Safety and Occupational Health

These answers indicate that, although all of the disciplines and specialties listed are important, some are particularly important to the typical senior security executive at this point in time. The authors believe that the answer choices may have been somewhat influenced by the events of 2019 and 2020 which caused security professionals to focus far more attention than what normally might be expected on crisis management and physical protection of property and people.

Question 12: What tools do you use to assist in performing your security management mission?

The intent of this question is identifying whether the tools needed by security management professionals are viewed as part of the organization's overall infrastructure or if it is viewed as specific to the security department/

Figure 8: Percentage of Survey Respondents Who Indicated They Use the Tools Shown to Assist With Security Management



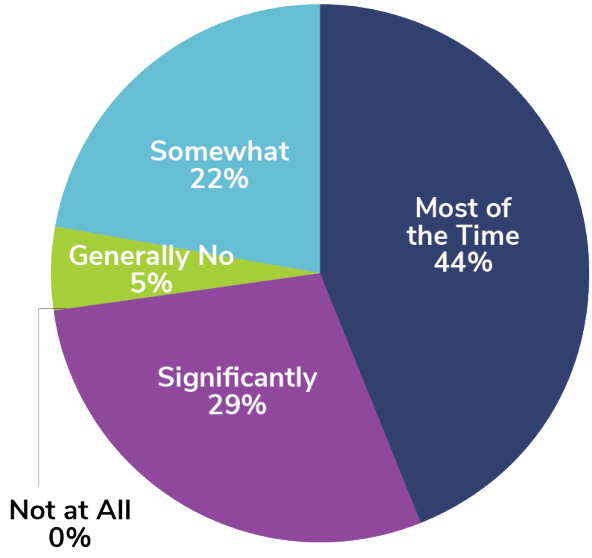
function. By far, the most utilized tool is that of risk assessment, which is not surprising considering the strong emphasis put on it throughout the profession.

Formal metrics programs and global/national standards are also commonly used tools, and generally seem to be more prominent as security-specific tools than do some others. This indicates that security professionals design risk assessments, metrics, and standards specifically as security management tools rather than adopting organization tools in these areas. That said, it does seem quite common for security executives to use general management tools as well.

Question 13: Please rate your ability as a security executive to influence decisions in your organization and among its executive management.
This is an important question as it relates to the ability of security executives to effectively fulfill their responsibilities. A majority of security management professionals stated that they do have some leverage to exert influence over most security management decisions. A small number of respondents stated that, generally speaking, they were not able to influence decisions or not at all able to do so. It is interesting that so many security management professionals agree that they can influence decisions made but yet the incidents and loss events do not seem to abate. This issue can be researched further in future studies.

Interestingly, several of the narrative comments provided by survey respondents indicated that their key to influencing decisions is to understand the business, support the strategic objectives of the organization, and be an active part of the team.

Figure 9: Percentage of Survey Respondents Who Indicated They Have the Ability to Influence Decisions in Their Organization



Question 14: To what degree do you feel the security management field is changing?
This question is discussed in detail in the Findings section, describing the researchers' conclusion that security executives must embrace change. Although this has been a topic of conversation for several years, the events of 2019 and 2020 have highlighted this as a clear and undeniable fact.

How is the Security Management Field Changing?		
Very Rapidly	Due to Ideas and Concepts	5.6%
	Due to Technology	3.2%
	Due to a Combination of these	21.2%
Rapidly	Due to Ideas and Concepts	4.2%
	Due to Technology	15.2%
	Due to a Combination of these	30.5%
Same as Society		13.3%
Slowly		6.1%
Not at All		0.2%

Most of the respondents stated that the security management field is changing either rapidly or very rapidly. The world has certainly gotten more and more interdependent and more challenging. Are the large organizations more susceptible to the global threats than medium and local businesses? Government agencies seem to be experiencing just as much in terms of threats as private sector organizations.

Question 15: To what degree do you use metrics and statistical analysis in performing your security management roles and responsibilities?
Most of the respondents stated that they do use metrics and statistical analysis in performing their tasks as security managers. A small number of respondents stated that they do not use metrics at all. This is worth taking note. If most of the individuals do use metrics and statistical analysis there is an expectation that the profession would be able to predict incidents that can occur and prepare for them more effectively. For example, we all seem to hear about ransomware every day. Organizations large and small and public and private are impacted by these. What we do not hear about are the physical threats and theft, as in the case of shoplifters and so on.

A Great Deal	10.7%
A Moderate Degree	21.0%
Somewhat	35.7%
Not at All	32.0%

Question 16: To what degree do you currently use advanced technologies such as artificial intelligence, machine learning or data analytics to aid in decision making or program management?
Although the survey responses indicated that these advanced tools are not currently in extensive use in the security management field, their adoption will likely occur in the fairly near future on a larger scale. It is interesting, however that six respondents indicated that their program management protocol relies almost entirely on advanced analytic tools such as these.

Question 17: What skills and qualifications do you feel are needed in the successful security professional today and in the future?
People skills were indicated as critical by survey respondents. This finding affirmed the earlier finding that security management as a profession, despite its association with physical barriers, firewalls, and electronic surveillance systems, is driven by the people in the profession. This survey question and the results are discussed in detail in the Findings section.

Several of the answer choices for this question received high scores as being either very important critical to the practice of security management. These included traits and qualifications such as:

- Interpersonal skills
- The ability to be flexible
- Strategic thinking abilities
- The ability to react quickly in a crisis
- Management skills
- The ability to adapt

The responses to this question were a strong indicator that, when it comes to the successful security professional, people skills clearly trump technical skills.

Question 18: What value do you place on each of the following components when seeking a candidate for a position on your professional security staff?
The responses to this question were mixed, indicating that all of the following components (candidate qualifications) are important.

- Education
- Professional Certifications

Figure 10: Percentage of Survey Respondents Who Indicated They Use Metrics as a Security Management Tool

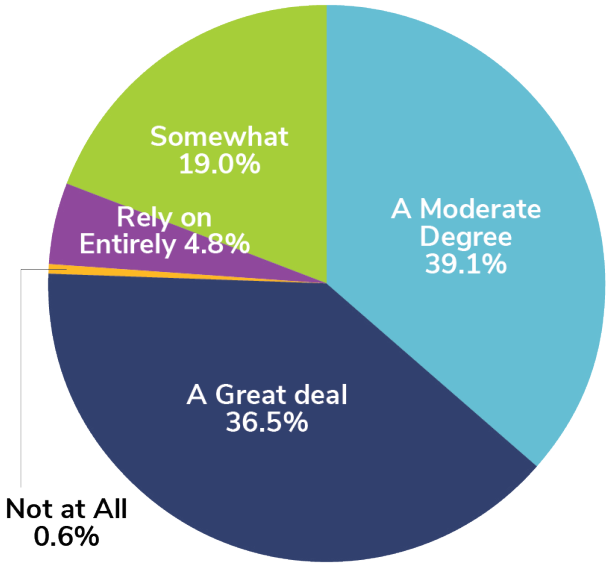
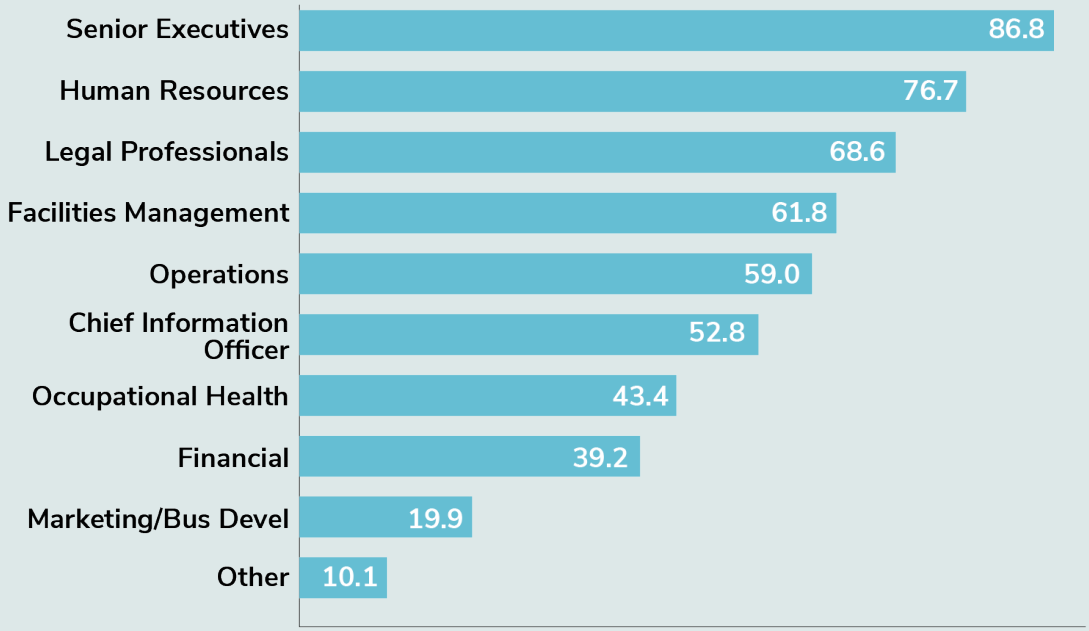


Figure 11: Percentage of Survey Respondents Who Indicated the Function Shown Was a Key Partner in the Success of the Security Management Program

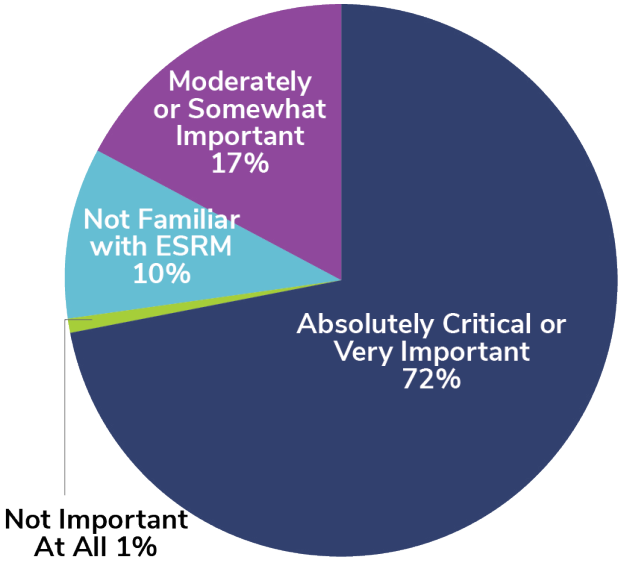


- Training in Security Skills
- Security Experience
- Specific Industry Sector Experience

Question 19: Which of the following do you consider to be key partners with you in the effort to manage security successfully? Senior executives and human resources are listed as the top two partners (corporate or organizational functions) in managing security successfully as shown in the chart below. Other highly rated partners included legal professionals (e.g., corporate counsel), facilities management, operations (e.g., manufacturing, production, or transportation), and the chief information officer (CIO). The authors expected that the CIO would be rated higher due to the importance of the IT infrastructure in almost any organization today. It is also likely that occupational health received as high a rating as it did because of their major role in the typical organization's pandemic response and recovery.

The 2005 *Scope and Emerging Trends* (ASIS Foundation, 2005) study asked a somewhat similar question. A significant percentage of survey respondents listed human resources as the compa-ny unit with which security staff most frequently interacted; the facilities unit was a close sec-ond. That survey also indicated that a relatively low number of interactions generally occurred with other units such as legal, risk management/auditing,

Figure 12: Number of Survey Respondents Who Placed the Indicated Level of Importance on ESRM



and financial. Our survey indicates that interaction with these functions is on the rise.

Question 20 – How important do you believe it is to apply the principles of ESRM in performing your duties and how do you implement them?

To this question, a significant majority of the respondents stated that ESRM is important and indicated that ESRM will be part of the landscape of security management in the future and beyond.

The responses to this question are monumental (see Findings section for more detail) and were consistent across English language, Spanish language, and the pilot surveys.

Question 21: Do you believe that ESRM is adequately defined as a concept and that enough useful reference material is available to successfully implement it?

Survey respondents indicated that ESRM is adequately defined (62%) and that adequate reference materials on the subject are available in order to successfully implement it (50%). This is welcome news for proponents, but also indicates that additional work should be done. The consensus is that ESRM as a concept is gaining momentum and becoming a popular philosophy.

SURVEY DATA: DEMOGRAPHIC DISTINCTIONS

This section highlights some connections and disconnects among various demographics such as industry sector, language, geographic region, and association membership.

English Speaking Respondents Compared to Spanish Speaking Respondents

There were a number of distinctions noted between security professionals who responded to the English language survey and the Spanish language survey, summarized below. The authors believe that these distinctions reflect actual differences in perspective rather than any effect of survey wording or format.

- In terms of "key partners in managing security successfully," English-speaking respondents identified legal professionals and facilities management professionals as other key partners while Spanish-speaking respondents identified operations and occupational health professionals, as well as CIOs, as key partners. This is in addition to human resources professionals that both groups identified.
  English-speaking respondents did mention CIOs, operations, and occupational health professionals as partners, but did not rank them as important as the Spanish-speaking group. These differences might be attributed to language, but more importantly, this is perhaps attributable to cultural differences and societal perceptions of safety and security for individuals and organizations.
- Regarding the definition of security management, participants indicated a clear divide. English-speaking respondents strongly supported the "business function" definition with "strategy" as a second choice. Spanish-speaking participants rendered the opposite result; they preferred the "strategy" definition with "business function" as a second choice. One possible explanation for this is that the strategy definition choice seems to focus on preparedness for any contingency rather than specific threats that are actually encountered. The idea may be that preparedness alone is not sufficient in many cases to either prevent or address a particular security-related risk.

	ESRM is Adequately Defined	Adequate Reference Materials For ESRM Are Available
Definitely	122	84
Yes, Somewhat	211	186
No	104	161
Not Sure	71	79
Not Familiar with ESRM	33	31

Another possible cause for the difference could be that the concept of strategy may resonate specifically with Latin American security professionals, whereas the term "business function" might be more meaningful to people in other parts of the world.

Discipline	ASIS	ACFE	(ISC)²	ISACA
Security Management (in general)	✓	✓	✓	✓
Physical Security	✓	✓	✓	✓
Cybersecurity	✓		✓	✓
Information/Intellectual Property Protection			✓	
Personnel Security/Insider Threat Mgt	✓		✓	
Investigations	✓			
Safety & Emergency Management	✓		✓	✓
Compliance	✓			
Risk Management	✓		✓	✓

- To the challenge of finding professionals, the Spanish-speaking group sees this as less of a challenge than their English-speaking counterparts. The same can be said about keeping up with new technology. This is more of a challenge with the Spanish-speaking group than the English-speaking respondents.
  It was enlightening to view the distinctions among participants completing the Spanish version of the survey and those taking it in English. Clearly security professionals living and working in Latin America have valuable perspectives and it is worth further study. Understanding the similarities and differences in how people view the core concepts of security management in various geographic regions, languages, and cultures is clearly a worthwhile endeavor. The events of 2019 and 2020 have probably given us an excellent opportunity to pursue this cause.
  See Appendix A for a more detailed comparison of English-speaking and Spanish-speaking survey responses.

Professional Association Membership

Several distinctions were revealed in the survey data among members of different professional associations. One of the more interesting connections is that survey participants who were members of ASIS International, ACFE, (ISC)2, or ISACA all agreed strongly that security management is defined as "a business function designed to protect an organization's assets and ability to perform its mission by identifying, assessing, and managing current and potential security-related risks." This was surprising to the authors since these associations represent communities that often have different perspectives from one another on terms and definitions relating to the field.

Another distinction was seen in the security discipline or specialty that individuals identify with compared to the professional association they belong to. The following chart presents a combination of survey question 5 (What is your personal specialty or discipline?) and question 7 (Which professional associations are you a member of?).

These results indicate that professionals with a specialty in security management and those in physical security affiliate with all of the professional associations listed in the chart. The same is true (except for AFCE) for people with specialties in safety and emergency management and risk management.

Industry Sector	Definition of Security Management	ESRM Adequately Defined?
Federal Government	Business Function	YES
Local Government	Business Function	NO
Energy & Utilities	Business Function	NO
Broadcast & Media	Business Function	NO
Financial Sector & Banking	Strategy	NO
Transportation & Supply chain	Strategy	NO
Manufacturing	Strategy	NO
Non-Profit	Strategy	NO
Automotive Sector	Business Function	NO
Leisure & Sports Sector	Managing Security Force	NO
Education	Strategy	YES
Healthcare Sector	Business Function	YES

The chart shows those instances where there was a statistically significant correlation between a respondent's personal specialty or discipline and their professional association affiliation(s).

This was somewhat surprising since many ASIS members work in the field of information and intellectual property protection, and many ACFE members are very involved in investigations and compliance. It should be noted, however, that the chart displays statistically significant correlations rather than all respondent answers from the survey.

Other distinctions of note related to professional association membership include:

- In general, ASIS, (ISC)2, and ISACA members indicated they find it difficult to convince their organization's management that the threat is real, while this was less of a concern among ACFE members
- ASIS, (ISC)2, and ISACA members indicated that the security management field is changing very rapidly; ACFE members believed it is changing, but less rapidly
- ACFE members indicated that it is a challenge to define and valuate assets that warrant protection, while members of other associations did not feel it was a problem in general

Industry Sector Distinctions

The only statistically significant distinctions based on respondents' industry sector were in the definition of security management and in whether or not the concept of ESRM is adequately defined. The following chart shows a crosstabulation of those results. Again, the chart entries represent statistically significant correlations rather that all answers from a particular industry sector.

Crosstabulation for Industry Sectors versus Definition of Security Management and Whether ESRM is Adequately Defined

It is interesting to note that the only industry sector that favored a security management definition other than business function definition or the strategy definition was the leisure and sports sector. As previously mentioned, this sector tends to rely more heavily than others on security officers and executive protection agents. This may color their view of what constitutes the field of security management and cause them to lean more toward the managing a security force definition. It is also noteworthy that, although survey respondents overall clearly indicated they thought ESRM was adequately defined, many of those from particular industry sectors disagreed.

Geographic Region Distinctions

It was interesting to note that the third most popular answer choice to the question "what are your key challenges in performing your security management role and carrying out your responsibilities?" was "convincing people that the threat is real." However, that answer choice was selected at a much lower rate among respondents in the Middle East & North Africa region and the Sub-Saharan Africa region. The authors believe that this may be an indication that people in those parts of the world take a much more serious view, or perhaps a broader view of threats than others do. For example, security professionals and the population in general, may see various social and geopolitical risks as security threats. This is addressed briefly in the Findings section and would also be a topic that warrants further research and inquiry.

A lesson learned from the data analysis that can serve as a reminder for security professionals is that we cannot, in all cases, simply take a security risk management paradigm, perspective, or model suitable for one environment and apply it in another setting, region, culture, or industry. For example, the CARVER risk assessment model was originally developed during the Vietnam War era as a tool to be used to prioritize targets and allocate resources appropriately in tactical military operations. Despite the numerous attempts over many years, it does not translate well to security risk assessment in the corporate security environment.

THOUGHT LEADER INTERVIEWS

Researchers gained valuable perspectives by interviewing 10 thought leaders in the security management profession. The following individuals participated (graph on next page):

Security Management Thought Leaders

Each of the thought leaders is a subject matter expert in one or more disciplines essential to security management. Seven of the 10 thought leaders are published authors on security management or related topics. All have presented at conferences, webinars, or taught classes on related subject matter—and all have demonstrated dedication and innovation in the organizations they've been a part of and in the field overall. See Appendix D for a brief biographic sketch for each of them.

The interview questions were similar to the substantive questions in the survey of security professionals, but were more suited to a narrative response. The interviews complemented the survey results nicely and provide further support to the study's findings.

Definition: What is your personal definition of "security management?"

The first question asked for the thought leaders' perspectives on their personal definition of 'security management.' The terms 'holistic,' 'risk management,' and 'strategic' were repeatedly used by the interviewees as part of their definition. Three of the thought leaders included unique and interesting concepts in their definition. Bonnie Michelman, CPP, CHPA, emphasized strongly the idea of "service," which is interesting since, in reality, most professions actually involve the provision of a service. The objective is to focus intensely on competence and quality in providing the service. Security management is no different. Another thought leader proposed that a key charge of security management professionals is to protect an organization's value, whereas we normally think of it as protecting assets. This was insightful as an organization's assets are actually tools to generate value in a typical organization. The concept of protecting assets as a means to an end-goal of protecting value warrants further discussion in the profession's various forums and reference materials. Finally, Axel Petri

	Primary Expertise or Specialty Area	Years of Experience	Location
**Howard Belfor, CPP	Security Management, Security Systems, Design, Systems Integration	42	Black Mountain, NC, USA
Earl Biggett, CPP	Security Management, Sports Venue Security, Investigations	29	Louisville, KY, USA
Inge Sebyan Black, CPP, CFE, CEM	Security Management, Investigations, Loss Prevention, Fraud Management, Cybersecurity	45	Saint Paul, MN, USA
Whit Chaiyabhat, MBCI, CBCP, CEM, CPP	Security Management, Cultural Properties, Sports Venue Security, Intelligence Analysis	21	East Greenwich, RI, USA
Kathy Macdonald, M.O.M, CPP	Security Management, Cybersecurity	33	Calgary, AB, Canada
*Bonnie Michelman, CPP, CHPA	Security Management, Healthcare Security, Workplace Violence	"Many"	Boston, MA, USA
Axel Petri	Security Management, Telecomm Security, Information Protection, Investigations	12	Bonn, Germany
*Dave Tyson, CPP, CISSP	Security Management, Cybersecurity, ESRM	35	Houston, TX, USA
Tim Wenzel, CPP	Security Management, ESRM, Research/ Development, Protective Operations	15	San Francisco Bay Area, CA, USA
Caroline Wong	Cybersecurity, Security Management, Security Metrics, Applications Security	15	Portland, OR, USA

*** Past President and Chairman of the Board, ASIS International**
**** Past Member, Board of Directors, ASIS International**

described security management as "connecting all the dots." This includes people, technical tools, and other management systems, such as business continuity, security risk management, and information security management. The concept of connecting the dots is a perfect segue to the philosophy of ESRM.

Challenges: What do you see as the key challenges to implementing effective security management today?

In terms of key challenges for senior security executives, the thought leaders had a lot to say. Their input on this question seemed to center on six general areas of concern:

- Finding and retaining the right people. This ranges from encouraging talented young people to enter the career field and advance through it, to ensuring mid-level to senior security executives continue to engage in professional development in order to remain relevant.
- Integration of traditional and cyber business risks, especially in terminology and language so that specialists (both internal to the security function and outside the security organization) can effectively communicate.
- Change, complexity of the global risk environment, and rapidity of changes. This includes, but is not limited to, unexpected events such as the COVID-19 pandemic.
- The need to align security risk management strategies to the business's strategic goals and organizational culture. One

thought leader, Dave Tyson, CPP, CISSP, advised that we must have a "ruthless focus on the business."

- Demonstrating value added for the security function, the struggle for resources, and ways to measure success (or notice if the direction is toward failure). According to Tim Wenzel, CPP, security professionals need to address "preconceived biases about what security is, what it should do and what it should cost." Another thought leader mentioned that the struggle for resources is something that "always has been and always will be."
- The need to educate organization executives on the importance of not only protecting tangible assets, but also intangible assets that are difficult to measure, but have far greater impact. These include reputation, intellectual property, resiliency, and similar assets.

One interviewee mentioned that a major challenge is dealing with, and educating others, on the fact that in today's world there are many inflection points where a single bad actor can cause harm with devastating and widespread impact. In other words, it no longer requires the scale of a nation-state or large malevolent organization to wreak significant havoc.

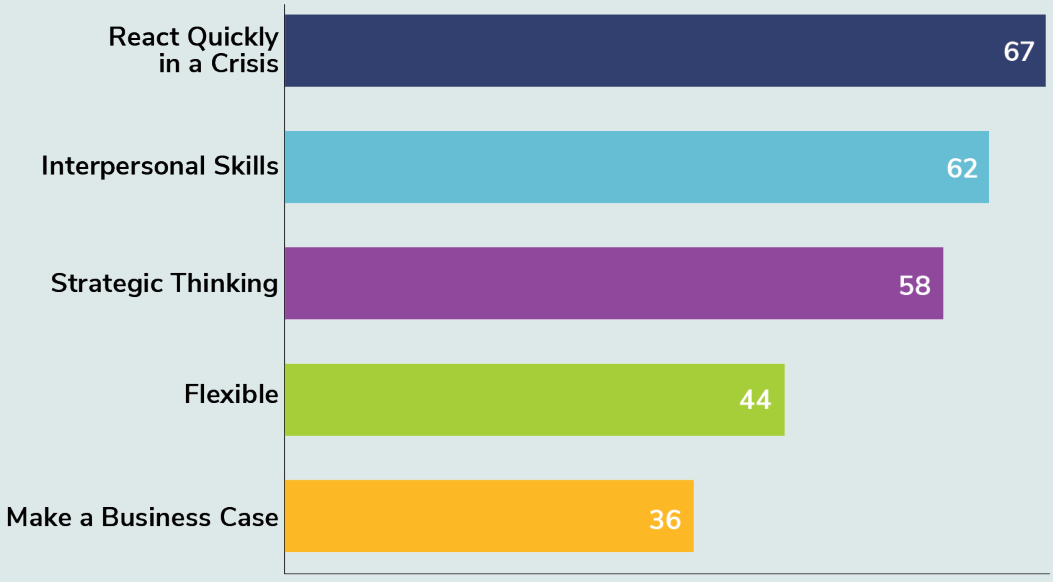
In addition, Howard Belfor, CPP, offered an interesting perspective on this question. He stated that one of the key challenges today is that we rely on technology to such a degree that no one knows what to do or how to react if the technology fails (e.g., the network goes down during a critical transaction or operation). This is a complacency that can have disastrous results.

Skills: What skill sets do security professionals need today in order to succeed?

The thought leaders discussed a wide variety of skills that not only lead to success, but are absolutely critical in the security management field. They include personal traits, professional skills, and an understanding of the connection between security management and the business or organization that is being supported. Here are some key skills that were mentioned by two or more of the thought leaders:

- Desire to learn and to work in a collaborative environment
- Willingness to embrace change
- Interpersonal skills; one of the thought leaders mentioned that there are a lot of touch points in a contemporary organization, and you have to be able to interact with all of them

Figure 13: Percentage of Survey Respondents Identifying These Skills as Absolutely Critical for Security Executives



- Ability to communicate in a way that a nonsecurity professional can understand and will support
- Business strategic planning skills and the ability to make a business case
- Desire to understand the culture, nature, and workings of the business or organization; and be able to speak the language of the organization
- Having a comfort with ambiguity and contrarians
- Being politically savvy
- Strong problem-solving abilities
- Critical thinking ability: the ability "to think inside the box, outside the box, and even around the box"
- Emotional intelligence and the ability to connect with people and build relationships

One thought leader pointed out that the skill sets needed depend on the size and nature of the organization. For smaller organizations, the security executive may need to do everything while in a larger business, more specialized skills may be necessary. Another noted that the sophistication of the position is expanding because everything that is simple has been outsourced, offshored or automated.

Caroline Wong made an excellent point about the importance of being an effective influencer. She said, "At the end of the day, security doesn't happen because of the security team. Security happens because of the effectiveness of the security team at influencing people and driving others toward more secure behavior."

C-Suite Perceptions: How do you believe business and organizational executives (C-suite) perceive security management today, and is that changing?

There was general agreement among the thought leaders that the perception of C-suite executives toward security management is changing. Most mentioned the COVID-19 pandemic and other challenging risks of 2019-2020 as catalyst for a shift in C-suite perceptions. In the past, many CEOs didn't want to know anything about security, and now they are far more interested and tend to view security executives as consultants or trusted advisors. A few of the thought leaders specifically mentioned the desire of C-suite executives to keep their name out of the news as a motivation to change their view of senior security staff. A number of interviewees also stated that security used to be seen as a necessary evil, but now is far more appreciated.

Earl Biggett, CPP, described the perception of security management as having come full circle. He said that after 9/11 everyone wanted to know about security – it was front and center. Over time that interest faded, but now – with the events of 2020, "it is back in the game." According to Axel Petri, ASIS introduced the idea of security management serving as a business enabler about 5 or 10 years ago. Today, he said security needs to be more than an enabler, it needs to actually be part of the business.

According to Whit Chaiyabhat, CPP, MBCI, CBCP, CEM, one way to expand the C-suite perception of security even further is for security executives to attend and speak at professional conferences for other fields such as chief financial officers, bar associations, human resources groups, and others. This is a form of outreach that can greatly benefit the profession.

However, some thought leaders indicated that many CEOs still see security executives as the people who deliver bad news. One individual mentioned that some executives are becoming more politician-like, and their main motivation is avoiding ending up on the front page of the news. This can affect their perception of security management and the role of security in general. The good news is that, on balance, the situation is changing. Caroline Wong mentioned that executive perception (and overall perception) of the cybersecurity field changed drastically when news media began actively publicizing security incidents, data breaches, and other loss events. The stature of cybersecurity professionals was significantly improved simply because of the publicity and public information.

Risk Tolerance/Appetite: Do you believe that the risk appetite or tolerance of business and organizational executives is changing?

The first noteworthy take away from this question is that a number of the thought leaders made a distinction between "risk

tolerance" and "risk appetite." Risk appetite is defined by the organization and usually more within the control of the executive suite. Risk tolerance is "what you accept because you have no other options." It is a reaction or threshold to things that are outside the organization's control. A couple of the thought leaders stated that risk appetite has generally not changed much, while risk tolerance has increased, primarily due to the expanding risk environment around us – especially in 2020. Most other thought leaders agreed that risk tolerance and appetite is increasing primarily due to a new appreciation of the threat environment and growing awareness. On the other hand, some executives are lowering their risk tolerance and appetite based on the regulatory and compliance environment as well as liability risk.

So there is no clear consensus on this. In fact, Whit Chaiyabhat, CPP, MBCI, CBCP, CEM, said there "will never be a steady state risk appetite." Once we recognize the ebb and flow, up and down of risk tolerance and appetite, "we can get better at using intelligence and forecasting to anticipate the next risk on the horizon."

Recent Impacts on the Field: What are two things that have impacted the practice of security management in the past few years?

COVID-19 and the other risk events of 2019-2020 were definitely included in many of the answers to this question. They had a major impact not only on security management practices, but also changed security management thinking in many ways. Other things mentioned as having a major impact on the field included the refinement of social engineering tactics, the explosion of ransomware attacks, digitization, the software supply chain (SaaS and cloud), security technology, and ESRM.

Future Impacts on the Field: What are two things that will impact the practice of security management in the next few years?

Many of the answers to this question were the same as the recent impacts listed above. Most prominently, our thought leaders believe that COVID-19 and the other events of 2020 will have a long-term, if not permanent effect on security management practice and thinking. Another set of issues that will impact the future will be privacy and identity. Privacy is going to be a major concern especially as it relates to medical and other data that can be collected, stored, and shared with growing ease. Similarly, identity credentials will increasingly be automated which opens them to fraud, manipulation, and misuse. Long-term work-from-home or remote work environments will also impact the risk posture of many companies and organizations, as will bring-your-own-device (BYOD) policies which will increasingly allow (or require) employees and others to use their own digital devices for work purposes. This will clearly affect the risk posture since corporate IT departments will have less direct control over network-attached devices and authorized systems and users.

Other answers included blockchain and social shifts. An interesting perspective was offered by Bonnie Michelman, CPP, CHPA. She indicated that a major impact on the future of security management will be how "elevated, visible, and reputed the field is, so we can recruit good people and diverse people who are smart and innovative."

Role and Relevance of ESRM: What is the role and relevance of ESRM in security management today?

As expected, there was strong consensus on the value of ESRM. Comments included:

- Very relevant
- Huge!
- Absolutely critical
- The foundation of security management
- Encourages people and departments to talk with each other, which always yields benefits to the organization
- Still a few years away from it being mainstream, but it's going in the right direction
- Helps engage with the business and ask the question why am I doing what I'm doing?
- Extraordinarily important and will continue to be
- It is "the tool to connect the dots"

This was welcome news, but it should be noted that some of our thought leaders are

also pioneers of the ESRM approach and contributed actively to its development. One thought leader also suggested that more education be made available on ESRM and that the concept should be repackaged to make its relevance more important to certain groups.

To summarize, the interviewer, Laneisha Hayes, CPP, provided her thoughts on some themes that emerged from the process. She concluded that the thought leaders agreed that the C-suite is beginning to view security management as something other than a necessary evil, but that resource and budget justification is still challenging. Communication and collaboration are key to future relevance in the field and ESRM is the wave of the future. Finally, it seems that all agreed with the strong need to align security management with the organization's culture and strategic goals. This is not a novel concept. It has been a focal point of those leading the profession for at least two decades. Now, slowly, it is becoming the accepted goal and will be even more so in the future. (Hayes, 2020)

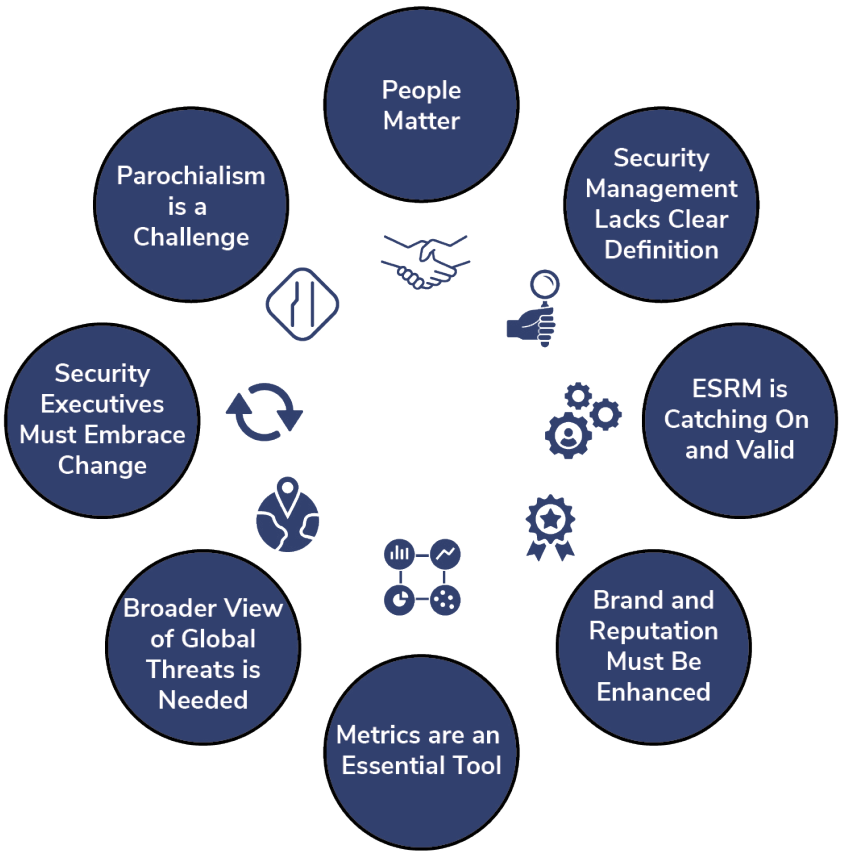
KEY FINDINGS

Based on the components of this study, the research team identified eight key findings relevant to the state of security management. As shown in the Executive Summary infoGraphic, the key findings include the following:

A description of each finding follows. These fundamental conclusions are substantiated, as described, by the study's survey of security professionals, thought leader interviews, literature search and other inputs.

Key Finding: People Matter

Despite extraordinary advances in technology and the rapidly increasing complexity of the global organizational environment, security management is still largely a people function. This conclusion was evident in both our survey and in our review of relevant writings; but it was particularly prominent in our thought leader interviews. Every individual we spoke to made it absolutely clear that security management revolves around people – and will contin-



ue to do so through the foreseeable future.

Of the eight key success factors of a successful senior security executive listed in ASIS's Chief Security Officer (CSO) Standard, six of them are people skills versus purely technical skills. Some of the specific terms mentioned in the list are innovation, integrity, ability to influence, ability to adapt, and relationship management. The standard describes a "core responsibility" of the CSO as "the management of positive working relationships among stakeholder and client groups." It goes on to define an effective model for a security executive as a hybrid that considers an individual's leadership talent and business acumen as well as subject matter expertise. (ANSI/ASIS, 2013) These points, along with the results of our research for this study, clearly demonstrate the human nature of senior security executive roles and responsibilities.

As Whit Chaiyabhat, CPP, MBCI, CBCP, CEM, put it during his thought leader interview, "At the end of the day, our profession is about people, and the way people, either individually or culturally, act. We're dealing with a human-based profession." He went on to say, "People, cultures and society are at the root of all of it. It's human behavior. Understanding that in a business sense and a cultural sense, as well as at the individual level [is essential]." (Chaiyabhat, 2020)

People skills were also clearly identified in responses to the survey question on which skills and qualifications are needed to be a successful security professional. (See Figure 2) The top skills listed as absolutely critical were:

- Ability to react quickly in a crisis
- Interpersonal skills and the ability to deal with people
- Ability to think strategically
- Ability to be flexible and adapt to changing situations
- Ability to make a business case, influence decisions, and advocate for a position

Another skill that received fairly high numbers as being absolutely critical was the ability to learn and adapt new skills. This is in contrast to much lower numbers for various technical skills.

Narrative comments from the survey respondents also confirmed that security management is about people. In the question asking "How do you influence decisions in your organization?" for example, the comments centered on human and interpersonal skills. A sampling of things mentioned include:

- Assertive communication
- Explaining and convincing by understanding the issue
- Demonstrating knowledge of the business and how the issue fits into the overall strategy
- Anticipating the needs of stakeholders
- Being included and recognized as a trusted advisor/partner/consultant
- Relationship building over time; garnering trust
- Exercising and demonstrating integrity
- Being viewed/recognized as credible

These terms were not merely mentioned by a few individuals. They were presented independently in a large number of the narrative comments provided by respondents regarding their ability to influence risk-related decisions within their organization. They align quite well with other sources including the thought leader interviews, documents we reviewed, security management textbooks, and ASIS International standards and guidelines.

Elsa Lee, author of Homeland Security and Private Sector Businesses, summarized the issue nicely: "Today, relationship building is an important skill in the workplace. It is necessary to effectively interact, communicate, manage, and lead others. …When it comes to security, most organizations… overlook the human factor – people. All security measures begin and end with people." (Lee, 2015)

Why is this important?

Security executives must avoid the temptation to dismiss the critical and enduring role of human beings – both as a threat and as a resource – in performing their mission. Despite the undeniable and growing influence of technology in our everyday world, security management is still, and will continue to be largely a people function.

Key Finding: Security Executives and Management Professionals Must Embrace Change

The years 2019 and 2020 represented a sea change in security management and the changes are still developing.

For the past several years, change has been a popular theme at security professional development courses as well as in books, papers, and articles. In addition, the ASIS CSO standard listed "change agent" as a required skill for a senior security executive.

Although some in the security management profession may have scoffed at the idea of being a change agent in the past, the two to three years leading up to 2020 have clearly shown how truly relevant and meaningful that role is. In fact, in an interview for Security Management magazine, ASIS International President John Petruzzi, Jr., CPP, stated that "the rapidly evolving and overlapping crises of 2020 made that more apparent than ever." Using the example that 2020 represented one of the most active storm seasons in North America, with a series of hurricanes following one another in very short succession, Petruzzi said that there will always be security incidents, whether manmade or natural disasters, but "when they layer up it gets more complicated." (Meyer, 2021)

In an article for *Security*, the CEO of TAL Global, a California-based consulting firm described this piling on of layers of different types of risk events as "stacking" (Tal, 2020). This is an appropriate term – and actually, a useful way of thinking about the situation – since the tendency for diverse risks to stack up simultaneously appears to be a new and emerging phenomenon, at least in scale.

The 2020 Catastrophe Snapshot suggested the following as some of the noteworthy events:

- COVID-19 global pandemic
- Severe storms, flooding, and landslides
- Hyperactive hurricane season
- Widespread riots (U.S. and worldwide)
- Devastating wildfires in the United States and Australia
- Extremely large number of low severity events worldwide

(TigerRisk Partners, 2021)

Add to that the unprecedented number and scale of cyberattacks, particularly ransomware, in 2019 and 2020. The global risk environment is changing rapidly and unpredictably in general.

COVID-19

The COVID-19 pandemic, and its associated uncertainty, resulted in a variety of direct and indirect changes in the global risk environment.

As a result, according to a *Wall Street Journal* article, corporate security chiefs and cybersecurity leaders are "gaining prominence" in many corporate settings as they grapple with rising security threats during the coronavirus pandemic. Corporate executives and boards are bringing them into the fold a lot more often, and recognizing them as a "trusted advisor." (Stupp and Rundle, 2020)

Torsten Wolf, director of forensics at Control Risks-Germany, noted that the pandemic, "in combination with the pressure of an economic downturn, lasting uncertainty and, in many cases, a fight for daily survival, the current situation may prove to be a perfect storm" for fraud and other risks putting "corporations big and small to the test" (Wolf, 2020). He pointed to details in a recent report by the Association of Certified Fraud Examiners (ACFE), *Fraud in the Wake* of COVID-19:

- Businesses continue to grapple with the economic fluctuations, supply chain disruptions, remote operations, and the toll this year has taken on the health, safety, and well-being of the workforce.
- As of November 2020, 79 percent of respondents to the ACFE survey observed an increase in the overall level of fraud, with 38 percent indicated the increase was significant. Further, 90 percent of those completing the survey anticipated that trend will persist over the coming 12 months.
- Cyber-fraud (including hacking, ransomware and malware), payment fraud, identity theft, and unemployment fraud were listed as having the most significant effect on the organization.
- Most respondents indicated that preventing, detecting, and investigating fraud have become more difficult. Among the

reasons for this were travel restrictions (including reduction of travel budgets), the need to conduct interviews remotely, and lack of access to evidence.
- To help compensate for this, many businesses are investing in antifraud technology, making more use of consultants and external resources, and increasing budgets for antifraud training and professional development. ACFE (2020)

The report from ACFE also noted that the percentage of respondents observing increases in fraud grew consistently throughout 2020.

In addition, according to Paul Reece, the COVID pandemic eroded trust in companies and institutions, driving a wedge between these entities and people all over the world. (Reece, 2021) This will clearly have long-term implications related to security risks and both the perception and practice of security management.

Civil Unrest

Incidents, including a major one in May 2020 which was perceived by the public – fueled by news media – as racially motivated police brutality sparked an unprecedented rampage of vandalism, arson, looting, and in some cases, killing, in major cities across the United States. To some degree the consequent violence persists today. This criminal activity represents another impetus for sea change in the security management field. As reported in Security Infowatch, the violence "left a devastating trail of damage amongst businesses of all sizes in the communities where they occurred and have led many organizations to rethink risk mitigation strategies in confronting these types of events. Historically, incidents of civil unrest were isolated to individual cities and were infrequent occurrences, but the proliferation of social media and the speed with which information flows today has resulted in a paradigm shift in how these types of events unfold." (Griffin, 2021).

In fact, civil unrest has been expanding globally in recent years. For example, one source identified spinoff protests in the United Kingdom, France, New Zealand, and Columbia as well as the United States. A leading risk monitoring firm, Verisk Maplecroft, stated that "our quarterly Civil Unrest Index reveals that over the past year 47 jurisdictions have witnessed a significant uptick in protests, which intensified during the last quarter of 2019. … A quarter of all the world's countries saw significant increases in civil unrest during 2019." (Hribernik and Haynes, 2020)

More specifically from the Verisk Maplecroft Political Risk Outlook 2020:

> *The number of countries rated extreme risk in the Civil Unrest Index has also jumped by 66.7 percent, from 12 in 2019 to 20 in early 2020.*
>
> *An "extreme risk" rating in the index, which measures the risks to business, reflects the highest possible threat of transport disruption, damage to company assets, and physical risks to employees from violent unrest. Most sectors, ranging across mining, energy, tourism, retail, and financial services have felt the impacts over the past year.*
>
> *The resulting disruption to business, national economies, and investment worldwide has totaled in the billions of U.S. dollars. (Hribernik and Haynes, 2020)*

There are new political risks in the United States as well that will impact security management professionals and the organizations they serve. Thomas Navickas has served as a police officer, educator, corporate executive, trainer, consultant, and in nonprofit management. As a corporate executive in a large enterprise, he worked closely with senior security professionals on resource allocation strategies and policy formation for achieving security risk management objectives. According to Navickas, there are huge challenges today including social and political ones. For example, there are efforts to "reduce the authority and increase the liability for both security personnel and civilian policing." This, combined with the defund the police movement, may affect how security services providers and law enforcement agencies are structured and how they are able to perform their mission (in terms of strategies and tactics) in the future. Or it may result in a transition "from local control of police forces to central government control." In either case,

"customer requirements and the perceived value of both security and law enforcement agencies will be in flux." This, in turn, will impact corporate security professionals in terms of their overall risk management strategies as well as internal and external relationships.

Navickas also mentioned that any social or political shifts will likely affect the skills and competencies important for security officers as well as security management staff. "This will change the job profiles requiring not only expanded knowledge proficiency but also, to a greater extent, behavior and/or emotional intelligence attributes. … In some cases, we might also see a move toward outsourcing civilian policing to private security firms." In addition, he predicted that the demand for "physical security will increase, but cybersecurity intelligence will be the most sought after competency." (Navickas, 2021)

Cyber Risks

Monumental ransomware attacks on businesses, municipalities, law enforcement agencies, and notably, a critical energy infrastructure in the United States are impacting widespread geographic areas, industry sectors, and millions of people. The critical infrastructure incident occurred shortly after the 2020 cyberattack known as SolarWinds, named after the company that produced the software which was used as the platform over which the attack was conducted. SolarWinds stated that about 18,000 of its customers installed updates to a software product the company sells, and those updates contained malicious code planted surreptitiously by the perpetrator, believed to be a Russia-based hacker group. Among the customers known to have been victims were U.S. Government agencies including the Department of Homeland Security, Department of State, Department of Defense, and Department of Energy, as well as many major corporations (including large IT firms), universities, and hospitals. The cyberattack spread to the victims and went undetected for months. (Jibilian and Canales, 2021) Such incidents create widespread cyber-uncertainty among populations, businesses, organizations, and governments. They represent another aspect of the developing changes in security management priorities, thinking and practices.

Pace of Change

The relevance of change was also highlighted in our survey responses to a question which asked, "To what degree do you feel the security management field is changing?" In terms of how rapidly change is occurring, 50.1 percent of respondents answered rapidly and 29.4 percent answered very rapidly (for a combined total of 79.5%). In terms of the primary causal factor for the change, among those who answered very rapidly or rapidly:

- 9.5 percent attributed the change to evolving ideas and concepts in security management
- 26.1 percent attributed it to advancing technology
- 64.4 percent attributed it to a combination of the two factors

Narrative Definitions Provided by Survey Respondents

Among the more insightful definitions provided in the survey question comments were:

- The measures a business undertakes to prepare for, prevent, respond to, and recover from a range of threats and challenges to the ability of the business to achieve its objectives.
- A strategic and tactical coordination, implementation, and administration of required measures and approaches to sustain and secure any kind of operation from intrinsic and extrinsic detrimental influences. *(paraphrased)*
- A collection of practices designed to promote, enhance, and offer a safe and secure environment, protecting the company's staff, contractors, assets, guests, and brand.
- A discipline that enables an organization to accomplish its objectives more safely and effectively through the development and execution of security strategies.

In addition, the 10 thought leaders interviewed for the study agreed, almost unanimously, that change is accelerating both in terms of security challenges and C-suite risk appetite and risk tolerance. Axel Petri, senior vice president, Group Security Governance at Deutsche Telekom AG, put it this way: "The complexity of our surroundings and fast-changing environment is one of the most critical challenges we see" as senior security executives today. (Petri, 2020)

The convergence of a significant number of major risk manifestations over a relatively short period of two to three years, including global pandemic, natural disasters, accidental catastrophes, civil unrest, insider threats, economic downturns, supply chain disruptions, and cyberattacks has had a major impact on the security management field. Not only is this changing the way security executives think about the threats, vulnerabilities, and consequences their organizations face and how they plan and implement risk management strategies; but also how security professionals fit into the business decision-making process and organizational governance. It has been described by one source as a series of "tectonic shifts" in security management.

Whereas traditionally, for the most part, security executives have had to deal with one or two significant risk situations at a time, they are likely to face, on an increasing basis, multiple stacked risk events that strain resources, diffuse strategic focus, and confound traditional risk mitigation strategies. This has tremendous implications for the security management profession.

According to Michael Padilla-Pagan Payano, CEO and chairman at Al Thuraya Holdings in Nicosia, Cyprus, "...disruption is the rule, not the exception; ...the global landscape is rapidly changing [and] this demands business acuity, technical know-how, and a curious mindset" from senior security executives and risk analysts (Padilla -Pagan Payano, May 2021).

While change has always been a factor in business and organizational security management, the pace and nature of change will have significant influence on the profession and how we relate to the clients we serve, whether they be internal or external. As Michael Gips, JD, CPP, CSyP, CAE, puts it in a recent blog post, "Given today's environment, businesses are facing an existential threat, and security is top of mind. ... In this new environment, the CSO [more than ever before] can be a direct advisor to corporate executives or senior government officials." (Gips and Cook, 2020)

Why is this important?

Leaders must be prepared to deal with changes – sometimes radical, and always dynamic – in the risk environment which not only affects their organization, but the entire infrastructure that touches them. In addition, executives face changes in management principles, practices, and tools as well as social factors in organizational, national, and global governance.

Key Finding: The Security Management Field Lacks Clear Definition

There has been a longstanding controversy among academics and thinkers in the field over whether or not security management is actually a profession. Today, most leaders believe that it is. Purpura, for example, posits in his 2018 textbook, Security and Loss Prevention: An Introduction, that the security field "has reached the status of a profession, based on the fact that it has a history and body of knowledge recorded in books and periodicals; a theoretical foundation; academic programs; and associations that promote advancement of knowledge, training, certification, and a code of ethics." (Purpura, 2018) However, another critical characteristic of a profession is that it must be clearly defined.

Two studies, both conducted in 2010, one in Australia and the other in the United States, examined the security industry and addressed, in part, the issue of a meaningful definition for the security profession. Although these studies did not specifically pertain to security management, they did raise some relevant issues.

The Private Security Industry: A Review of the Definitions, Available Data Sources, and Paths Moving Forward was conducted for the U.S. Bureau of Justice Statistics (BJS). It examined the private security industry overall and reviewed several data sources including the Hallcrest Report, results of the ASIS Foundation-sponsored Academic/Practitioner Symposia (1997 to 2008), the ASIS glossary of security terms, and the ASIS-Foundation-sponsored *Scope and Emerging Trends*

study (2005). One interesting finding noted by the authors of the BJS study was that "relationships between public and private security agencies have improved in recent years, as both police departments and private security have paid greater attention to collaboration, information sharing, and partnership." (Strom, et. al., 2010)

This is important to this study because the relationship between public law enforcement and the security industry affects a variety of decisions senior security executives make, and the recommendations and perspectives they offer to the C-suite.

However, the BJS report also concluded that "it will be critical... to develop a concise definition of private security" in order to implement a national data collection effort on the industry. According to the findings, "there continues to be a significant need for more detailed information" on the roles, growth, and trends in private security. Future studies incorporating data such as this might be used to gain more precise insights into the economic impact; operational nature; employment needs; and roles, responsibilities and authorities of private security. Undoubtedly, these studies will also address the issue of private security functions performed by human beings compared to those that might be automated or carried out with robotic systems or assistance.

Also in 2010, a team at Edith Cowan University presented research at the Australian Security and Intelligence Conference. Their paper, "Defining the Security Professional: Definition Through a Body of Knowledge," echoed, coincidentally, the BJS report's conclusion that security "eludes a consensus definition." One way the Edith Cowan team stated the situation was that "...the relatively young profession of security appears to suffer from somewhat of an image problem." (Griffiths, et. al., 2010)

This study addressed the question of whether security is truly a profession as well as its definition. It described work by the Interim Security Professionals' Taskforce conducted in 2008 which surveyed literature in an attempt to define the term profession. Further, it referred to several key principles that embody the concept of profession among recognized professions such as medicine, law, education, and others. These principles are entirely consistent with the criteria presented in Purpura's 2018 textbook mentioned above, and include: "knowledge, competency, learning, ethics, and membership within an association of peers."

A key conclusion is that the field of security management meets all of those criteria, but still needs to go farther in terms of body of knowledge, academic programs, and theoretical foundation, due largely to the changing nature of the profession as well as the global organizational environment. More specifically, security professionals need a better definition of who they are. Professions rely on a common understanding of what the field entails – and that is what provides their identity.

In the introduction to the Handbook of Security, Martin Gill not only states the problem, but also that it has real-world implications. "There are still major definitional problems that have never been satisfactorily resolved... The problem of definition is not an abstract one deserving only the attention of academics, it has practical implications." (Gill, 2006)

In 2019, a retired professor from York College (Pennsylvania), Chris Hertig, CPP, established "The Security History Project" which seeks to more formally and thoroughly document the field of security, the security industry, and security management from an historical perspective. Under the current concept, information is gathered from credible sources around the world in a wiki-like format. It is meant to be shared openly and encourage connections and conversation among interested security professionals. In addition, a "This Day in History" column was added to Security Management magazine. The results of this work will add to the understanding and identity of the profession, and assist in defining the field by focusing conemporary light through an historical lens.

Defining Security Management: Survey and Thought Leaders

The definition of security management was also addressed in our survey and thought leader interviews under the current effort. In fact, the first question in our interviews asked our thought leaders for their personal definition of security management. Every one of them included some mention of "holistic security," "risk management," or both. Several of our thought

leaders also mentioned the terms "strategy" or "strategic" in their answer to this question.

The survey data produced less consensus, but also yielded interesting information. Five definition choices were offered and respondents were asked to select the one that comes closest to their definition of security management.

Although opinions varied considerably, according to the survey data the definition of choice seemed to converge on two of the response options:

- A business function designed to protect an organization's assets and ability to perform its mission by identifying, assessing, and managing current and potential security-related risks. (42% overall, 53% English-language respondents, 9% Spanish-language respondents)
- A strategy to protect an organization against all possible threats it may face. (23% overall, 16% English-language respondents, 42% Spanish-language respondents)

In total, these two choices accounted for 65 percent of the survey responses. It should be noted that approximately 5 percent of the respondents answered "other" to this question and provided their own definition.

The interesting disparity in definition choices between English-speaking respondents and Spanish-speaking respondents is discussed in the section on "Survey Data-Demographic Distinctions" and a side-by-side comparison is shown in Appendix A.

We believe the implications of the lack of a definition are significant – and may have even more impact in the future. If we, as a professional community, are not able to define ourselves, how can we articulate our identity to executives and decision makers, and advocate for optimal influence and resources, especially in tomorrow's dynamic and agile – and more ambiguous - global business environment?

Why is this important?

In order to thrive and advance as a profession, we must have a better understanding and vision of where we came from and who we are.

Key Finding: Parochialism in the Security Management Field is a Challenge

Most likely some degree of parochialism has always existed in the security field worldwide. Competition for resources, attention, or influence among various subspecialties or disciplines within the security field can easily lead to an environment where this attitude – and resultant behavior – thrives.

We have also seen this phenomena in the threats that take center stage within a particular time frame. Terrorism, economic crime, cybercrime, sexual abuse, violent crime, espionage and intellectual property theft, and natural disasters all vie for attention. As a result of the COVID-19 pandemic, we are certainly entering a phase where pandemic and health concerns will be front and center in the risk management priority schema globally. As we reflect on this time in history, threats from civil unrest and violent extremism may certainly be added to the mix as well.

Parochialism can also apply to other aspects of security practice. For example, approaching security risk management from a governance or compliance perspective versus having more of an assets protection focus. This is an important and real-world contemporary distinction because decision makers may need to choose between addressing the risk of noncompliance with a standard or regulation (fines, administrative penalties, legal actions) versus an actual loss event (crime, loss of life, injury, operational disruption, etc.). Still another way parochialism may manifest itself is the assumption that all organizations are like your organization. Security professionals and policy makers must understand that protective tools, techniques, and strategies that are entirely appropriate and effective in a large megacorporation may not work in small, medium-sized, and entrepreneurial businesses or small organizations; or what works in one part of the world may not work in other geographic areas.

Another factor is the traditional silo mentality between and among different security disciplines. Security professionals can begin to think and act in an insular fashion. Cyber, physical, personnel, homeland, and other security professionals, for example, may adopt the attitude that security risk management revolves around them with other disciplines as adjunct or subordinate functions.

Today, the most obvious and pervasive ten-

sion tends to exist between the cybersecurity and traditional security arenas. In fact, a new term has come into common use to describe those traditional arenas: "operational security." Unfortunately, operational security has other meanings in certain sectors such as law enforcement and the military. This is one of the difficulties brought about by repurposing terms in the absence of a thorough, collaborative thought process and research effort.

The situation is exemplified by the fact that during 2020, a number of seasoned security professionals expressed the position (usually verbally) that "today, everything is digital." This implies that all security disciplines other than cyber are irrelevant, and only digital or electronic assets are worthy of protection. In fact, one individual questioned whether there are still truly any organizational assets other than digital (i.e., no physical assets; no intangible assets, and no mixed assets). This idea is counter to foundational concepts such as ESRM, the all-hazards approach, and a sound assets protection philosophy. We might think of it as the "the cybersecurity dilemma," and it is a dangerous premise.

One respondent to our study survey mentioned the following in a narrative comment to the question "What changes do you see in the security management field?":

"Lack of clarity among many businesses about the difference between cyber and physical security. Many see them as part of the same discipline, but the skillsets are dramatically different. Sort of like saying police and fire are both first responders and either can handle any situation. Training, skills, and equipment are totally different."

A few examples serve to demonstrate the overemphasis on cybersecurity:

- CSO Magazine focuses almost exclusively on cyber topics whereas it exists to present informative discussion on all topics of concern to chief security officers and security executives.
- A number of books have been published in the past five years on risk management, but actually cover only cyber risk management.
- The term "information security" is often used synonymously with cybersecurity or information technology security whereas its true definition is far more broad and includes a variety of traditional security strategies to protection information in any form, along with cybersecurity; in essence, the term has been hijacked by the cyber community, which causes confusion and consternation.

According to Robert McCrie, a well-respected subject matter expert and educator, "cybersecurity has risen to the top overall management concern. But conventional issues – business continuity planning, workplace violence, employee selection, privacy concerns, and many others – continue to challenge the high-performing security operations manager." (McCrie, 2016) As stated in Aon's *Global Risk Management Survey* report, "Our research has emphasized that risk management needs to continue to evolve...as an enterprise-wide, rather than siloed, approach and function. In parallel, risk managers of tomorrow should continue to...ensure risk is identified, assessed, and managed in an integrated way across the organization." (Aon, 2019)

In our study, over 44 percent of survey respondents identified "integrating security disciplines" as one of their key challenges as a security executive.

As expected, when asked to identify their

personal specialty or discipline, most survey participants chose "security management." It is telling, however, that in addition to the eight other answer choices, many respondents chose "other" and listed 16 additional specialty fields in their narrative comments, for a total of 24 specialties or disciplines. This mimics the results the 1999 and 2000 ASIS Academic/ Practitioner Symposia where security practitioners and security educators where brought together to discuss the components of security and how that foundation can be used to develop relevant curriculum models for university programs in security management. During the 1999 Symposium, attendees developed a set of nine "common elements in the security model" (i.e., components or subspecialties which comprised security). At the outset of the 2000 Symposium, nine additional common elements were added to the model for a total of 18 constituent functions. (ASIS, 2000) Attendees concluded that security was more complicated and difficult to concisely define than previously thought.

One strategy is to focus on the end state – management of an organization's security-related risks – rather than individual disciplines that contribute toward that objective. This assists in viewing the contemporary battle between cybersecurity and other security through a different lens. Security, and hence, security management, is not a simple or straightforward endeavor. It is a multidimensional and increasingly complex profession wherein professionals hone and leverage a variety of diverse and interdependent tools for managing security-related risk, and ultimately allowing an organization to accomplish its strategic objectives in the most safe and secure manner possible.

Hopefully, as it continues to take hold, the ESRM philosophy will represent a significant step toward helping resolve this dilemma in security management today.

Why is this important?

Security executives must recognize and manage potential parochialism both within themselves and their organizations. The effects of this challenge can include discord among security professionals, partners, and vendors – and may also reduce the ability to proactively and effectively manage relevant risks.

Adopting an ESRM mindset will help diminish the adverse impact of parochialism.

Key Finding: ESRM is Catching On (and Considered Viable)

This study serves to provide definitive confirmation that ESRM is alive and well. Like any professional field, buzzwords seem to be introduced on occasion and tend to consume time and attention with little legitimate value in the end. Despite the early perception by some that ESRM was one such buzzword, its development, application, and advancement since its inception have proven the value of the philosophy.

ESRM began to enter the lexicon, generally as an amalgam of the concepts of security risk management and enterprise risk management (ERM) almost two decades ago. Since then candid discussion, critical thinking, pilot application, and strong advocacy have led to a fairly widely accepted, practical, and maturing approach. Many individuals and groups participated in initiatives to define and develop ESRM. Publication of the ASIS Risk Assessment Standard, a collaborative effort in 2014-2015 between ASIS International and the Risk and Insurance Management Society (RIMS) served to advance the thinking in this area as well.

A bibliometric study published in Security Journal in 2021 analyzed 463 articles and concluded that "Security risk management is a subject area on its own and is closely linked to ERM" It went on to partially define and discuss the progression of ESRM:

> ASIS International has played an important role in the past few decades in improving a new security paradigm in the context of risk management… The first major initiative was the joint creation by ASIS-ISACA in 2005 of the Alliance for Enterprise Security Risk Management (AESRM), which proposed that ESRM requires multifunctional collaboration in the ERM context across various management areas, including but not limited to physical and logical security, occupational risk prevention, legal, risk management, … crisis management, and business continuity planning. (Marquez-Tejon, et. al., 2021)

Additionally, a paper produced by the ASIS International CSO Roundtable in 2015 emphasized the holistic nature of the ESRM approach. Later work (in 2016) by Petruzzi and Loyear discussed the life cycle of ESRM and "highlighted that this philosophy encourages all company sectors to proactively recognize and deal with risk from a security perspective… ."

Earlier this year, Michael Gips, JD, CPP, CSP, discussed the status of ESRM in an *International Security Journal* article. In discussing its early years, he stated "The Enterprise Security Risk Management philosophy had been lurking on the periphery of mainstream security practice since the early 2000s, when ASIS International, ISACA, and ISSA created the *Alliance for Enterprise Risk Management.* That group generated a few reports then fizzled out." (Gips, 2021)

There appeared to be a lack of clarity for several years. One challenge: "even experienced professionals still conflate[d] ESRM with related concepts such as convergence, resilience, and enterprise risk management." One individual responding to a survey, according to Gips, stated that "ESRM is unclear and obscure for many security professionals."

That situation appears to have changed. It has become a valid and fitting approach which can be effectively leveraged especially considering the growing complexities and interdependencies of security management evident from survey findings, interviews, literature search, and observation.

Very Important or Critical	71.7%
Moderately Important	14.6%
Somewhat Important	2.6%
Not Very Important	<1%
Not Familiar with ESRM	10.2%

Even the authors of this study were surprised by the survey results with respect to ESRM. Overall, almost 72 percent of the respondents indicated that applying the principles of ESRM is either very important or absolutely critical in performing their duties.

When asked about the role and relevance of ESRM in his thought leader interview, Whit Chaiyabhat, CPP, MBCI, CBCP, CEM, immediately answered "absolutely critical." He went on to say that "What we need to continue to do as an industry is partner with other functions and other professions that own other aspects of operational risks in the business." (Chaiyabhat, 2020)

In her thought leader interview, Bonnie Michelman, CPP, CHPA, was asked for her personal definition of security management, and concluded with "It is Enterprise Security Risk Management." (Michelman, 2020)

The survey results also indicated that, for the most part, information is available to assist security management professionals in implementing ESRM practices.

- 60.9 percent of the respondents stated that ESRM is adequately defined
- 49.4 percent of the respondents stated that adequate information and educational materials about ESRM are available

Several white papers, studies, and a book have been published on the subject. Also, in 2019, ASIS International published the ESRM Guideline, which memorialized the concept and provided a unifying baseline. According to the guideline, ESRM "is a strategic approach to security management that aligns an organization's security practices to its overall strategy using globally established and accepted risk management principles." Further, it states that security executives must understand the context of the organization in terms of its "mission and vision, core values, operating environment, and stakeholders. … It addresses all domains of security risk in a holistic manner and without silos." (ASIS International, 2019)

Why is this important?

ESRM is the wave of the future for many, if not most security management executives. The study confirmed that the philosophy is indeed becoming accepted globally and that good progress has been made in defining the principles, making security professionals aware of the concept and developing educational and informative materials on its practice.

Key Finding: Security Professionals Need to Broaden Their Perspectives on Global Threats

The concept of the global business environment has been a topic of conversation for a long time, but increasingly, that conversation must inform security risk management thinking and approach. In some respects, global issues affect every business and organization today – there is no avoiding it; and it will only expand in the future. As such security executives need to broaden their perspectives on the meaning of common vernacular such as threats, vulnerabilities, and risk mitigation. Even the concept of assets may have to be adjusted in some cases.

One example that most executives rarely consider is that risk management strategies may need to be tailored based on considerations such as the ability or willingness of government security forces or law enforcement to respond to incidents or provide protective support. From another perspective, private or contract security forces under the auspices of a business or organization may overreact in a civil unrest situation and become part of the problem rather than the solution. To some security executives, these are simply part of the everyday thought process, but for more and more, a broader, bigger-picture perspective is necessary. This is especially true as the global supply chain continues to expand and become more complex.

During a discussion within the ASIS International Human Threat Management Community, the question of just what constitutes a human threat was raised. One of the steering committee members opined that it is much more than we commonly think of when we talk about the insider threat to organizations. He stated that in MENA countries, for example, human threats may include disputes over access to natural resources, land, and water. In other words, threats to human needs. (Padilla -Pagan Payano, April 2021) This can affect not only social climate, but also factors such as the crime and threat environment, workforce availability, incidents that may occur on an organization's property, utilities access, personal safety, transportation, and the supply chain. Social and geopolitical risks must factor into risk analysis and security executives' mindset and protection strategies. In addition, the impact of social media as a

tool to disseminate real or perceived grievances globally must be considered.

Writing in *Security Management* magazine, Riskpro Senior Vice President Mangesh Sawant noted that "The 20th Century CSO was primarily concerned about protecting the physical assets of an organization from threats like theft, pilferage, and robbery. But as issues like emerging risks, regional instability, and local conflicts affect companies, the contemporary CSO must understand the geopolitical dynamics of the 21st Century. … Geopolitical risk is at a post-Cold War high and everything is moving faster than before." As such, says Sawant, the chief security officer must become the chief security strategist." (Sawant, 2021)

During their interviews, a number of the thought leaders also mentioned the growing relevance of geopolitical risks, civil unrest, social strife, and political violence. As Whit Chaiyabhat, CPP, MBCI, CBCP, CEM put it, "We need to look at [human behavior] as a complicated dynamic because the world is complicated. (Chaiyabhat, 2020) In addition, the Political Risk Outlook-2020 from Verisk Maplecroft states: "The pent-up rage that has boiled over into street protests over the past year has caught most governments by sur-

prise. Policymakers across the globe have... reacted..., but without addressing the underlying causes. ...even if tackled immediately, most of the grievances are deeply entrenched and would take years to address." (Hribernik and Haynes, 2020) Therefore, these aspects of the worldwide risk environment will be with us into the foreseeable future even if no further turmoil develops.

McCrie, from the John Jay College of Criminal Justice, relates these real-world issues to the recruitment and advancement of security professionals. He put it: "Increasingly, the need for security services is managed on a global basis. This calls for people who can absorb, respect, and work with those of different cultures." (McCrie, 2016)

Why is this important?

To more effectively operate under an ESRM paradigm and address the evolving and dynamic threat environment of today and tomorrow, security executives must expand their perspectives and widen the lens through which they view the world. In addition, educational materials, curriculum, training programs, and professional development forums would be well served to incorporate more in terms of global and regional perspectives, as well as geopolitical and social threat considerations.

Key Finding: The Security Profession's Brand and Reputation Must be Enhanced

Perceptions of the security profession as a whole, the supporting industry, and the people who comprise it are critical. They have a direct impact on the effectiveness of protection strategies and the resources required to carry them out. Security executives must be mindful of how their mission is perceived by the public, by the customers they support (whether internal or external), and by the decision makers they aim to influence.

To help manage how these audiences perceive the security profession, both brand and reputation must be developed and maintained. Brand is generally viewed as how an individual or organization presents itself to the outside. The image that is intentionally projected to others. How the person or group would like to be perceived.

Reputation, on the other hand, is how others actually perceive you – from the outside looking in. It is generally beyond the organization's direct, short-term control, and may be influenced by incidents, news reports, social media, the nature of interactions, and how satisfied the customer base is. Both play a key role in perception.

Perception, brand, and reputation can affect many aspects of the mission. They can serve to detract or support the security risk management objectives. For example, ESRM is inextricably related to the practice of ERM, which enjoys high regard and importance in many commercial organizations. Therefore, employing an ESRM approach and educating senior management about the philosophy can naturally improve the security executive's credibility, and perhaps level of influence in the C-suite. It may also improve the ability to garner necessary resources and encourage closer working relationships with other organizational elements, even external partners.

Perception can be adversely influenced at all levels of security operations. The reputation of the security services industry is harmed, for example when incidents occur that generate a headline like "15-Year-Old Girl Beaten While Three Security Guards Watch ." Regardless of the facts of the case, the headline is what remains in the public's memory. In terms of perception, this negates the good that tens of thousands of security officers do every day around the world. Similarly, at the management level perception is affected when a security executive fails to accurately assess, or effectively communicate, the security risk implications of a strategic inflection point or critical business transaction.

A poor public image of security has many downsides including entry-level recruitment. When the field suffers from a poor reputation, people fail to see security as a desirable career choice at the entry level. Their perception may be limited to security officer positions with no potential for advancement or financial reward. Prospective members of the workforce often fail to recognize career potential for security officer services – or the existence of other career entry points such as security systems (installers, developers, manufacturers, R&D), security sales, corporate security administration, trainers, investigative assistants, intelligence analysts, etc. This hurts the

industry overall. Organizations such as ASIS International and the International Foundation for Protection Officers (IFPO) do highlight the positive aspects of the career field, and even sponsor award and recognition programs, but more can be done.

One excellent initiative was recently launched in the United Kingdom. As reported, "The British Security Industry Association (BSIA), has joined forces with the Security Institute and the Security Commonwealth to run an awareness campaign designed to reset public perception of the security professional and the essential role that they play in public life. The campaign will showcase security professionals as a respected, valued, professional service provider contributing to and creating a safe and secure environment..." (OBeirne, 2020) This type of collaboration among allied security organizations also contributes the effort to improve the brand and reputation of the security industry and the people who comprise it. More initiatives like this would be a welcome development.

Another positive step would be an effort to address the enormous legal liability faced by the security services industry and security management profession. In the Seattle, Washington incident, for example, the security officers on duty – and their employer – would probably have been sued if they stepped in to take action, even though they would have been protecting life and limb. Legal liability is an issue that inhibits security services, systems, and equipment providers globally. In today's environment, the legal liability issue is also beginning to impact public police forces and law enforcement agencies in some areas. It will be increasingly important to seek a reasonable balance between use-of-force policy and the ability to perform the security or law enforcement mission.

Brand and reputation can affect the C-suite as well. Their perception – or the lens through which they see senior security executives – "influences the security professional's ability to influence."

"Security is always seen as too much until the day it is not enough." This is a popular quote that has been attributed to William H. Webster speaking at a 2002 debate at the University of California, Santa Barbara. Webster had previously served as Federal Bureau of Investigation (FBI) Director in the United States and then as Director of the Central Intelligence Agency. Eighteen years later, his words still resonate with at least some senior security professionals. A recent LinkedIn post by Mary Hough, CPP, vice president security management at Corporate Security Overwatch, stated "This is so true. I don't understand why the people at the top won't listen to the subject matter experts they hire. Proactive is so much easier than reactive and potentially saves more lives." (Hough, 2021) As indicated in our survey, the thought leader interviews, and throughout the literature, a prime solution is the ability to build relationships with C-suite officials and other influencers in an organization.

Further emphasizing continuing or advanced education within the profession will also serve to enhance the credibility and perception of security management. One of the study survey questions asked participants what value they placed on various qualifications when considering a candidate for a professional staff position. Although experience was the most preferred qualification, 55 percent of the respondents stated that they place significant value or the highest value on education.

For one chapter in the book *Security in 2025,* editor Lawrence Fennelly asked a small group of security professionals to answer a series of questions and share their perspectives on how they see the profession evolving by the year 2025. He called it "A Brief Survey of Our Peers" and the first question was "What are four problems in the security industry?" Almost every one of the security professionals mentioned some aspect of education. Some of the comments were:

- Security education, graduate development programs in security
- Gaps between higher education and industry
- Educating the next generation of security practitioners is primarily restricted to the United States and is not an international strategy
- Lack of academic training in technical areas of security
- Lack of industry knowledge/education amongst clients and many operations personnel charged with building and maintaining security programs

In addition, one of the peers mentioned "Increased academic involvement in evaluating various aspects of security" as an emerging trend that will help form security in 2025. (Fennelly, et. al., 2017)

Education and certification programs must better integrate business, strategic thinking, and executive communications skills with security skills to truly enhance the ability to implement security management and further professionalize the field.

ASIS International Past President Shirley A. Pierini, CPP, PCI shares how she persevered and advanced in the security management profession:

"...in the 1980s, corporate security was beginning to emerge as a viable profession...[but] was primarily a male-dominated industry..." "I again fought back with formal education...and began seeking certifications through...ASIS Inter-national." "...to be a woman in a male-dominated industry takes a vision to achieve, tenacity, and, most importantly, the willingness to educate and gain the certifications necessary to stand out." *(Pierini, 2017)*

Brand and reputation can have an enormous impact on the ability – of both individuals and organizations – to influence risk-related decisions. As one survey respondent noted in narrative comments, the ability of a security executive to influence decisions "boils down to two things: 1. people skills, and 2. metrics, threat analysis, and risk assessment." Any efforts to enhance the reputation, perception, and public image of the profession would enhance the effectiveness and influence of security management.

Why is this important?

The greater the brand and reputation of the security profession, the more effectively members can carry out their duties in providing a safe and secure environment for businesses, organizations, communities, and people. Improved perception of the field in general also increases the amount and nature of influence security executives can leverage in the risk management decision-making process.

Key Finding: Security Management Metrics Are An Increasingly Essential Tool

Three quotes eloquently summarize the role of metrics and decision-making tools in security management today:

> "Security operations managers who demonstrate the ongoing worth of their programs, through efficient operations, measurable benefits, and reliable services, will thrive." (McCrie, 2016),
>
> "Introducing risk management into the field of security and assets protection also presents an opportunity to apply metrics." (Mahoney and Peterson, 2016), and
>
> "To manage today's risks and anticipate tomorrow's challenges, organizations need to harness the power of data and analytics." This provides the ability to efficiently and accurately "create meaningful and actionable insights" to address enterprise-wide risks. (Aon, 2019)

The idea of metrics being an essential tool for influencing executive or organizational decisions was prominently featured in the narrative comments from our survey. Some of the comments on the question asking "What changes do you see in the Security Management field?" were:

- Changes toward AI and ML [artificial intelligence and machine learning]
- Growing interest in intelligence-led security programs
- Starting to see intelligence collection and analysis for security professionals
- Intelligence and technology now drive security delivery and innovation
- Technology advancement in terms of AI
- We are seeing more focus on intelligence models and tools for more proactive response to security threats

The survey also explored the current use of metrics, data collection ,and technology tools such as AI in the security management function. The overall results are presented in the

"Survey Data Interpretation" section of this report. However, some particularly relevant points are:

- In terms of general tools to assist in the security management function, almost 50 percent of the respondents indicated they use security-specific, formal metrics and analysis tools. A slightly lower percentage (43.6%) use more generic organization-wide metrics.
- It was interesting to note in the same question that 54.1 percent of the respondents said they use risk assessment as a security-specific tool in performing their security management mission. Based on all the research done for this report, we believe that organizations may use risk assessment in support of security operations, but less so as a management tool at the security executive level.
- Also, slightly over 40 percent of the respondents use security-specific international or national standards as a measurement tool; whereas 52 percent indicated they use more general standards such as the ISO 9000 series.
- When asked to what degree respondents use metrics or statistical analysis, 72 percent stated they use these tools to a moderate degree or a great deal. Additionally, 3.4 percent of the respondents mentioned they base their security management program entirely on metrics and statistical analysis.
- The final question in this series asked about the use of advanced technologies such as AI, ML, or data analytics to aid executive decision making or program management. Almost 11 percent of the respondents use these tools a great deal, 21 percent to a moderate degree, and 36 percent at least somewhat. On the extremes, 32 percent stated they do not use these advanced tools at all, and 0.5 percent base their entire program on output from this type of tool set.

In the future, advanced tools such as AI, ML, and data analytics will be used extensively in executive program management and strategic decision making. However, they will also assist from a tactical or operations perspective to cut through the fog of high-stress or crisis situations. An important operational function such tools may perform more commonly is the sorting, prioritizing, evaluating, and consolidating of emergency calls and calls for service. One past example where this would have been extremely helpful was the active shooter incident in October 2017 targeting the Route 91 Harvest Music Festival from the MGM Mandalay Bay Resort & Casino in Las Vegas, Nevada. First responders were frustrated by information overload which delayed them in reacting effectively and efficiently to the real threat. News media and personal reporting of the events at the scene touched off a rash of 911 calls reporting active shooters and explosive devices being found all over the Las Vegas strip area. Calls were being made by panicked individuals who provided inaccurate, misinterpreted, or inadvertently false information. This caused significant confusion and diverted first responder resources from the actual scene and the location of the active shooter on the 32nd floor of the Mandalay Bay.

Encouraging Metrics and AI as Security Management Tools

In 2014 the ASIS Foundation sponsored a research project to study security metrics. The introduction states "Security metrics are vital, but in the field and in the literature one

A POINT OF REFERENCE: SIZE OF THE WORLDWIDE SECURITY SERVICES MARKET

As a point of reference, the size of the worldwide security services market in 2020 was estimated at approximately $132 billion. A study published by Statista also indicated that in 2020, "Asia overtook Europe and North America to become the largest market for security services worldwide, valued at $37 billion. ...Europe was the second largest security services market, valued at $36 billion." (Statista, 2021)

Both BizVibe and Grand View Research projected a 10.3 percent growth rate (CAGR) in the market through 2025. (BizVibe, 2021 and Grand View Research, 2021)

finds few tested metrics and little guidance on using metrics effectively." (Ohlhausen, et. al., 2014) The project resulted in the development of a Security Metrics Evaluation Tool, a library of metric descriptions, and guidance on putting metrics into practice. It also established a recommended protocol consisting of technical, operational, and strategic criteria for security metrics.

Further advice was provided in 2016 to assist in developing a security metrics program geared toward larger enterprises. In an article entitled "Some Unconventional Security Metrics," Roger Johnston, PhD, CPP, articulated some important attributes of "any good security metric." The important things should get measured, not just the things that are easy to measure. Quality must be emphasized over quantity. Recognize that compliance and security are not the same thing. He reminded readers of the ultimate goal, especially in large or complex organizations: "Risk needs to be minimized while considering hundreds of different security parameters (variables) involving security personnel, technologies, spatial and temporal deployment of resources, possible security strategies, assets to be protected, threats, vulnerabilities, training, etc." (Johnston, 2016) This is where a sophisticated security metrics program demonstrates its value.

Process improvement is another valuable benefit of a metrics program according to security professional Rod Taylor. "Measuring the value of programs which are designed to prevent events form occurring has been a difficult challenge for security professionals. A well-defined security metrics program allows security professionals to examine specific processes and components of their program and identify weaknesses, performance trends, and [potential] process improvements." (Taylor, 2013)

Regardless of the size or type of organization involved, it is clear that security metrics are becoming more and more of a necessity, and that advanced technology to support security risk management and security program decision making will become increasingly the norm. One forward-thinking graduate student put it this way: "Chief security officers must embrace artificial intelligence now and begin integrating it into the profession or face losing their relevance and [perhaps being] replaced by AI. ...Bringing AI into the team,

training themselves to focus on doing what only humans can do, training AI properly, and letting it loose to help secure people [and organizational assets] is imperative to the business." (Crysler, 2020)

Why is this important?
Metrics and advanced decision-making tools have many benefits in the practice of security management and add value; however, they must be properly planned, designed, and employed. Security executives who understand and make the best use of these tools will be the most successful trusted advisors within their organization.

OTHER THEMES OF NOTE

Although not considered key findings, the following themes came to light during this study and warrant mention. The first two relate to people issues in terms of past, current, and future security management professionals. The third theme deals with a trend in the security industry itself.

Gender Disparity Among Security Professionals

One of the demographic questions in the study survey asked for the respondent's

gender. Approximately 88.5 percent of the survey participants were male and 10.7 percent female. Although the number of female respondents was surprisingly low, as shown in Figure 14, these numbers very closely reflected the percentage of male versus female ASIS members.

Interestingly, 4 out of the 10 thought leaders we interviewed (or 40 percent) are women. That was not by design, but simply resulted from our team choosing people it felt were truly leading thinkers and longstanding trendsetters in the profession. One of our female thought leaders is a past president of ASIS International, and all four of them are extremely well-respected in the field having published, taught, and presented on security management-related topics extensively.

From the authors' perspective, there seems to be a dichotomy since the overall number of female security executives and senior managers seems to be low (based on ASIS membership, our survey, and the literature), yet women appear to be prominent at the highest levels in professional security associations and thought leaders in the fields of security management and cybersecurity management.

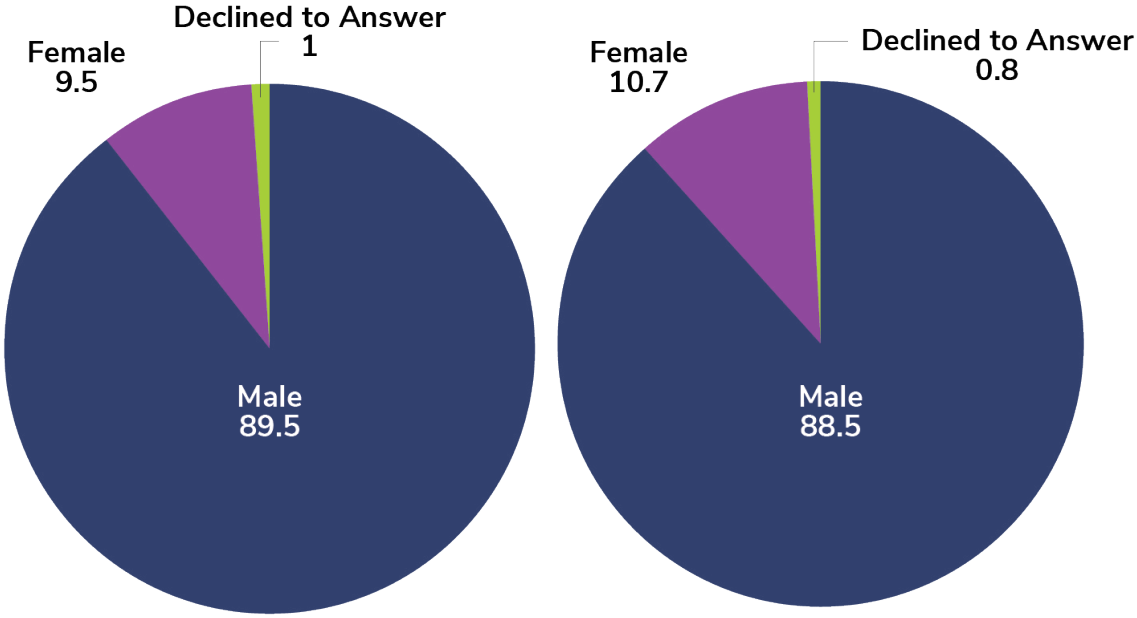
Since its inception, ASIS International (originally the American Society for Industrial Security) has elected six female presidents, the first in 1985.

In addition, the following numbers representing females who were named as IFSEC Global Influencers (for the category indicated) in 2019 demonstrate the respect earned by women in the profession:

- *Security Management:* 3 women out of 5 total awards
- *Security Thought Leadership:* 5 women out of 20 total awards
- *Security 'Ones to Watch':* 4 women out of 5 total awards
- *Cybersecurity:* 9 women out of 20 total awards

As Andrew Woods, CTP writes as a contributing author in the book Women in *The Security Profession*, "...in uniform, in the boardroom, and in the computer lab, women offer unique skills that can increase productivity and reduce risk...for companies... Recognizing these opportunities and learning how to leverage them will be one of the industry's key challenges moving into the future." He prefaced these remarks with "An industry that is increasingly focused on interpersonal and computer skills does not benefit from a per-

Figure 14: ASIS Membership by Gender: 2020 (left) and Survey Respondents by Gender (right)



sistent image of padlocks and brusque men." (Woods, 2017)

Again, the perception and image of the profession by prospective security executives (and others) can have a tremendous influence on people who may be considering entering the field or remaining in the profession and reaching for advancement once onboard. The need to provide better mentoring and encouragement for women will indeed be an ongoing challenge as Woods states.

Security professional Liz Martinez summarizes the situation nicely and also echoes Shirley Pierini's advice (see sidebar) on how to overcome existing obstacles. "Women have found acceptance in many security jobs and organizations, but their presence as middle- and upper-level security managers still lags behind men." However, "Women are also attaining higher education and are rising through the ranks in security organizations... [and] these changes have led to an increase in women in higher levels of security organizations, and the trend seems likely to continue." (Martinez, 2017)

Former Law Enforcement and Military Members Entering Security Management Careers—or Sourcing of Senior Security Executives

Although it wasn't planned to be addressed in this study, the subject of former military and law enforcement members entering the security management profession appeared fairly prominently in the literature reviewed. More importantly, it was broached in the narrative comments of survey respondents and also in the thought leader interviews. This is an issue which has been a topic of discussion for at least the past three decades.

The concern arises in the situation, which has been common, where hiring managers choose a former military member or law enforcement official to fill a corporate security director (or CSO) role rather than selecting someone who has advanced through a security management career within the business arena. The practice has been widespread and engenders strong opinions among the security community in many cases.

Overall, our research found that comments on this issue were fairly evenly divided among those who presented a negative perspective, those who took a positive approach, and those who commented on both the pros and cons of law enforcement or military experience.

Security professional and researcher Santanya Mahoney framed the situation nicely in a 2016 piece on the history of the security risk management concept. She writes that when former police officers and military members enter the security field for the first time "a shift in mindset is necessary – a transition from solving problems that had already occurred to [addressing] risk-related loss events before they happen. These security professionals have to consider the enterprise and how security can help with abating business risk. In other words, a more proactive approach is warranted and this leads to a natural progression toward applying risk management principles to security functions." (Mahoney, et. al., 2016)

In his book, *Security Operations Management,* Robert McCrie expresses concern over this tendency. "The military or police command and control method does not work well, or for an extended time, in nonmilitary or policing organizations, even those concerned with security services. The workforce in the 21st Century is highly mobile. Contemporary leaders endeavor to provide [others more] authority when delegating tasks. ...in effect, the leader gains by the efficiencies from decentralization and...empowerment." (McCrie, 2016) In short, some individuals with a military or law enforcement background have difficulty transitioning to a corporate or business mindset. However, this is not always the case. Their success often depends on the individuals themselves and the preparation or mentoring they receive as they enter new environments.

In some cases, having security professionals with military or law enforcement perspectives on the team can add value. Business professor and consultant Michael Roberto emphasizes that in many businesses and organizations, a combination of intuition and the use of a formal decision-making model is best in terms of decision outcomes. He states "Leaders should find ways to combine intuitive judgement with formal analysis." (Roberto, 2009) In other words, a blend of strategic thinking and tactical thinking is highly effective in most decision-making situations. This

is particularly true in the security management field.

Based on their training and experience, many individuals with a military or law enforcement background possess excellent intuition or gut instinct that can be a benefit in tactical decision making (recall that senior security executives employ a mix of strategic and tactical decision making approaches). Note that in Figure 2 (under the "People Matter" finding), survey respondents indicated that one of the absolutely critical skills needed for a successful security professional is the ability to react quickly in a crisis. This is primarily a tactical thinking skill, but also has a strategic component. Again, a good fit for some former military or law enforcement members.

Martinez also points out that the low number of women in the senior security ranks may be, in part, due to the tendency to hire former military or law enforcement professionals. She stated, "it is difficult for some male managers to accept [women] as qualified professionals. This attitude was more common in previous decades, when the male hiring managers were frequently retired military or law enforcement who would have had few women working for or with them in their previous careers." However, she adds that "The number of women in military and police service increases each year, and now…" many of those former military or law enforcement members entering the security field are, indeed, women. (Martinez, 2017)

Describing security as "an industry stereotyped by former law enforcement professionals" Bonnie Michelman, CPP, CHPA continued that "This was a positive as these people were structured, disciplined, and well trained. …Later that stereotype was changed to former federal agents, police leaders, and other high-ranking public safety/law enforcement professionals who were trusted and able to handle a protective strategy job with a good network." Again, a mainly positive perspective, however, she also wrote that "This transpired as the sophistication level and complexity of security programs in corporations increased along with regulatory pressures, business collapses due to breaches, and changing risks." (Michelman, 2017) Therefore, business acumen, collaborative thinking, strategic agility, and alignment with the organization's strategic goals are increasingly critical to the senior security executive in today's global business environment.

Individuals with military or law enforcement backgrounds can bring special skills and value to a private sector security management function. However, they must also be people who can adapt to the environment and adopt a mindset that suits the organization, which is likely quite different from their previous experience, especially in terms of objectives, process, and decision making. Completing educational programs in security management and attaining appropriate professional certifications will aid greatly in this endeavor. In addition, associations such as ASIS International have launched mentoring programs to help prepare individuals with diverse backgrounds for this new environment. In many organizations, the best situation may well be a hybrid of senior security staff with a military or law enforcement background integrated with those who have advanced through the private sector security arena.

Security Services Industry Diversification

Also noted in the research was the fact that in response to potential future shrinkage of the traditional security officer market, providers

are branching out into risk assessment, cyber security, travel security, intelligence analysis, and other services. This is especially true among the larger security services firms like G4S, Allied Universal, and Securitas. However, smaller firms are also following suit.

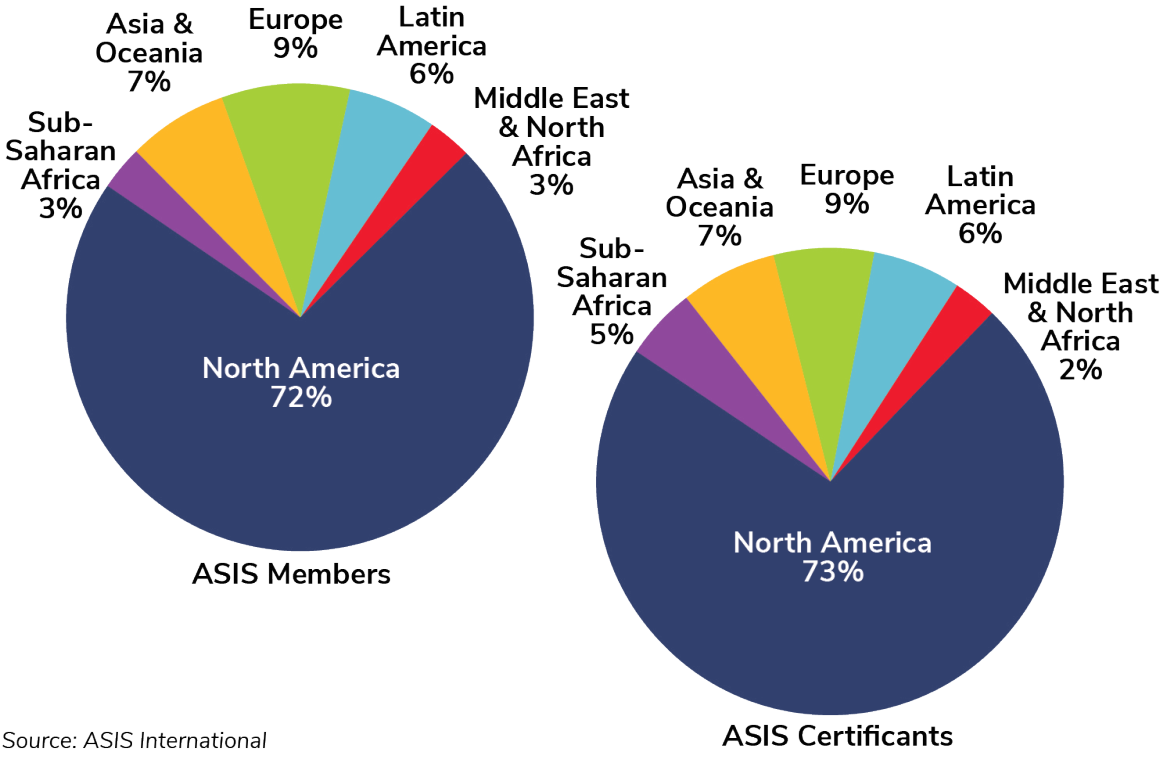
As described in the book Security in 2025, "One trend that has recently and slowly emerged is that of security firms diversifying their business portfolio. In some cases, this diversification occurs within the general security arena. For example, a security officer provider may offer to conduct physical security assessments, or a lock and key company might expand into electronic security systems. In other cases, the diversification is somewhat broader. Some security firms are moving into commercial property maintenance, transportation services, cleaning services, or renovation and remodeling." (Fennelly, 2017)

In fact, this has been happening in years leading up to 2020. "One large security officer services firm has expanded into electronic systems integrator services as well. More such firms are providing assessments, prisoner transport, language translation, security training, and other related services."

As an example, Allied Universal , the third largest security company (BizVibe, 2021), is now structured into three subsectors: Security Services, Technology Services, and Professional Services. Their vision statement is telling: "Be the most trusted corporate service partner in a world of evolving risk." This not only communicates their goal, but also their recognition that their focus must be on addressing risk which is constantly evolving. Among their Professional Services subsector are Risk Advisory and Consulting Services, Executive Protection, Intelligence Services, Event Services, Janitorial and Landscaping Services, and a staffing service. (Allied Universal, 2021)

Layered on top of this trend in diversification of services is the trend over the past several years of mergers and acquisitions within the industry. Although these conditions are not directly related to the security management profession as addressed in this study, it is incumbent upon contemporary senior security executives to remain vigilant and up-to-date on industry trends. They have

Figure 15: ASIS Membership vs. ASIS Certificants by Governance Region: 2020



Source: ASIS International

a strong impact on both contracting strategies and the overall protection approach an organization may implement locally, regionally, and globally – now and in the future.

For reference purposes, a current snapshot of the global security service market is provided in the sidebar. It should be noted that it is difficult to accurately measure the size of the market due to variations in what various research organizations consider to constitute the industry. As stated by the research firm Statista, "The security services market can be broadly divided into three main segments: security systems, private security guards, and security consulting services. There is much cross over between these segments, for example, with security guards being part of an overall security system, which in turn was created through security consulting services. IT security is also sometimes included as part of the security services industry but not always. Taken alone, IT security has a similar total market value to the entire traditional security services industry." (Statista, 2021)

In a September 2020 interview with Security InfoWatch, Allied Universal CEO, Steve Jones commented on the events of 2020 and how they "created unique and staggering challenges for security solution providers and clients alike." This resulted in a paradigm shift, in many ways like the one caused by the 9/11 terrorist attacks, according to Jones. Speaking about Allied Universal's experience, he said "we were able to leverage our size and scale our resources – technology or manned guarding options – which [put us in a unique position]. What's changing is the industry is getting demands that companies be able to have the resources and capabilities in many different areas." He continued, "The events of 2020 have only amplified all of these issues. Clients, more than ever, now really want the ability to…scale up in almost any situation…" (Lasky, 2020)

In short, the security services industry will need to be even more flexible, multidimensional, and scalable in their service offerings in the future as they support clients and security executives increasingly dealing with stacked and ambiguous risks. They will also continue to integrate technology, in various forms, into their service offerings regardless of their core business model.

Views Differ by Language and Culture

Throughout this study the distinctions in perspective based on language and culture are prominent. These are two of the most significant factors in how people think, perceive, compare, and strategize – including their approach to security management. Although this is an important theme of note for this study, it is addressed here very briefly because the issue is articulated well in the "Demographic Distinctions" section and other parts of the report. The Spanish-speaking respondents see the industry as changing rapidly, but the change drivers they identify are different than those identified by the English-speaking respondents. The "one size fits all" approach clearly does not work in today's dynamic global environment. From different ideas about the definition of security management to different perceptions of threat, and the inclusion of social a geopolitical risks – which mean different things to different people – this is a critical theme to consider. As mentioned, it should be an important part of future education, publication, and discussion as it relates to the security profession.

CONCLUSIONS AND IMPLICATIONS OF THIS RESEARCH

This project is meant to have tangible and directly applicable benefits to a wide cross section of readers. Among the projected uses of the study results are:

- Developing position descriptions for security professionals and practitioners.
- Developing and updating educational programs or curricula related to security management and functions.
- Defining skill sets and training necessary to implement security programs.
- Defining inter-relationships among organizational functions or departments.
- Identifying distinctions in security practice between the public and private sector, and among various industry sectors in order to benefit professionals transitioning from one sector to the other, and improve relationships among sectors with respect to security management.
- Future planning for security program

development and strategy relative to strategic plans of the organization.
- Trend analysis and metric development (and refinement) for security management.
- Facilitating conversation among security professionals operating in different industry sectors, disciplines, and global settings.

Following are some ways to translate the study findings into actionable steps and, ultimately, tangible benefit to enhance organizational safety and security.

Definition

One of the key findings of this study focused on the lack of a decisive and specific definition for security management. This harms the profession in a number of ways and has adverse effects both in terms of perception and practice. Following is a proposed definition based on a combination of the two most widely accepted answer choices in the survey of security professionals, and the definition offered by Gill in the Handbook of Security.

Security Management – a business function designed to protect an organization's assets and ability to perform its mission by identifying, assessing, and managing current and potential security-related risks through a strategic program management framework that actively engages executives, managers, asset owners, and other relevant stakeholders.

Recommendation: This proposal can serve as a starting point for discussion over an appropriate and meaningful definition for the term security management. We recommend that the final consensus definition be added to the ASIS Glossary of Security Terms, and that it be incorporated into ASIS International educational and marketing materials as well as publications and communications. In this way it will seamlessly become a part of the security body of knowledge.

Lexicon

The definition of security management is not the only obstacle across the profession related to terminology – there are many others. Perhaps one of the more salient examples, since it causes considerable confusion, is the term 'information security,' however this is but one instance. An excellent opportunity to promote a useful definition was missed when the term information security was omitted from the Terms and Definitions section of the recently published Information Assets Protection Guideline. This is another term that should be clearly defined and included in the ASIS Glossary and other materials.

Clearly, one detriment to the advancement of security management is the lack of consensus on definitions of key terms. One step toward a solution would be to establish a series of candid roundtable discussions among professional associations in allied fields on a common lexicon.

Recommendation: We suggest that ASIS International initiate such an effort. Among the associations that should participate are:

- ISACA (information technology audit, assurance, governance, risk, and security)
- $(ISC)^2$ (cybersecurity)
- International Security Management Association (ISMA)
- International Association of Privacy Professionals (IAPP)
- Society of Human Resource Professionals (SHRM)
- Association of Certified Fraud Examiners (ACFE)
- International Association of Emergency Managers (IAEM)

The effort might also include representatives from academic institutions offering graduate programs in security management and closely related fields. The discussions will likely yield benefits far beyond lexicon, perhaps extending to many other potential concerns and conflicts, while also advancing interdisciplinary collaboration.

Education and Certification

Obvious objectives that have emerged from this study include the need to improve the perception or image of the profession, increase credibility of security professionals, and enhance their ability to influence decision makers. Each of these objectives can be met, in large part, through education and certification programs, as long as they are meaningful. Many security professionals currently partici-

pate in such programs, however there is room for expansion and improvement in the programs, and most importantly, the emphasis placed on them by employers.

Writing in Security in 2025, Mark Beaudry, CPP, a respected security management practitioner and researcher stated that "The private sector's need to protect its people, property, and information will continue to grow in response to crime and terrorism and a decline in assistance from law enforcement. The demand for security education will grow as the field itself clamors for greater professionalism and outside groups call for security regulation, standards, and certification." He also predicts that, eventually, there will be a demand for terminal degrees in security management as the need for academic programs expands. (Beaudry, 2017)

Advanced education and certification can be beneficial for all security management professionals whether they have transitioned from the military or law enforcement careers, have come up through a corporate security pathway, or have entered from other career fields. Following are some suggestions for advancing toward these ultimate goals.

As mentioned in the Findings section of this report, advanced education programs must better integrate business, management, strategic thinking, critical thinking, interpersonal, and executive communications skills with security skills to truly enhance individual value and further professionalize the field.

> **Recommendation:** Institutions offering graduate degree programs, graduate certificates, and professional development programs in security management should reassess curriculum and delivery models to better balance outcomes related to security skills with those related to business, management, strategic and critical thinking, interpersonal, and executive communications skills. Additional emphasis should be placed on graduate and professional certificates that do not require the time and financial commitment of an academic degree.

This recommendation is supported by this study as well as previous studies such as the Security Industry Survey of Risks and Professional Competencies, a 2014 research study sponsored by the ASIS Foundation in cooperation with the University of Phoenix. It concluded that "Along with its exponential growth, the security industry is also rapidly changing, relying more than ever on workforce innovation, professional development, and relevant education to maintain success." Regarding curriculum revamps, the study also noted that "Decision making, oral communication, critical thinking, maximizing others' performance, and persuasive influencing were the highest-ranked competencies for tomorrow's security professionals." (University of Phoenix, 2014)

> **Recommendation:** Further efforts should be made to encourage institutions to integrate curriculum or employ interdisciplinary study models to improve crossflow among security management, homeland security, cybersecurity, emergency management, intelligence, and business courses. Approaching the issue from an ESRM perspective will provide a launching point to help facilitate mutual respect and understanding among these various academic communities and others.

In addition, the profession could benefit from more tailored course materials and textbooks. As mentioned by contributing author Joshua Bamfield in the Handbook of Security Management, "Whilst there can be no doubt that 'security management' is a branch of management, security itself has been the subject of very little research or comment by management specialists. Many management texts on 'security' tend to be technical guides rather than discussions of different management approaches…" (Bamfield, 2006)

The Wharton School at the University of Pennsylvania has collaborated with ASIS International since 2004 on the Program for Security Executives. The program format was updated in 2014 to make it more convenient and less expensive. This five-day, intensive course is offered once or twice per year and caters to senior security executives and CSOs seeking greater exposure to business and management perspectives.

> **Recommendation:** Although the Wharton program has filled an important gap for a

number of years, new programs should be developed with similar objectives. Programs offered by other institutions can challenge the Wharton School, but more importantly, make this opportunity more widely available globally and tailored to specific needs on a regional, industry, or situational basis. Ideally, a number of such programs, each with a slightly different emphasis, would be available for current or prospective security executives on a convenient and cost-efficient basis around the world.

Professional certification is another avenue to success and advancement in the security management field, and complements education, training, and experience as individual credentials. ASIS launched the Certified Protection Professional (CPP) certification in the 1980s as a professional security management designation. In subsequent years, ASIS established three additional certifications tailored to the specialties of physical security and investigations, as well as an associate designation meant as a predecessor to the CPP . The CPP, however, remains the pre-eminent security management certification worldwide.

In terms of numbers, 25.4 percent of ASIS members hold the CPP designation, and 35.5 percent of ASIS members hold one or more of the certifications offered by the association (current as of August 2020).

The percentage of ASIS members holding an ASIS certification in each geographic region of the world is fairly consistent with the percentage of ASIS members located in each region. For example, 7 percent of ASIS members reside in the Asia & Oceania Governance Region, and 7 percent of ASIS certificants reside in that region. North America residents represent 72 percent of the ASIS membership and 74 percent of ASIS certificants (see figures below for comparison).

Professional certifications are also available through a number of other associations including:

- Certifications that are specific to certain disciplines or specialty areas such as cybersecurity, fraud examinations, crime prevention, forensic interviewing, privacy, emergency management, business continuity, and security systems project management
- Certifications that are specific to certain industry sectors such as healthcare security, retail loss prevention, industrial security (defense contractors), and cultural property protection

Unlike some other professions, certification is not required (in a regulatory sense) in order to be hired to a position in security management. To get to that point would require an extremely resource- and time-intensive effort which is, at this point unlikely to be pursued. Nonetheless, it is highly beneficial for individuals to attain one or more certifications in order to enhance their skills, bolster their credibility, and stand out among their peers in the field.

Another opportunity for education and learning has presented itself in the past few years: online and informal learning platforms. Currently popular examples include LinkedIn Learning, Udemy, and Coursera. A wide variety of subjects and courses are available around the globe and many have options for participation in a number of different languages. Among other content, Udemy and Coursera offer full university courses which can be taken on a credit or noncredit basis under different pricing models.

Recommendation: Security professionals should explore and take advantage of new venues for learning such as LinkedIn Learning, Udemy, or Coursera. For example, one of the study's thought leaders, Caroline Wong, recently developed and posted a course on the LinkedIn Learning site entitled "Learning Security Metrics." Her course centers around cybersecurity metrics, but a similar course for security management in general would be extremely valuable. In addition, tools like LinkedIn Learning and Coursera provide a convenient and user-friendly platform for sharing information and educational content globally with minimal cost or complexity. Security management professionals and educators should look into these platforms and consider developing far more educational content that can be shared in this manner.

Brand and Reputation

Individuals, organizations, and entire professions carry with them a brand (something they portray or attempt to portray to others) and a reputation (the way others view them based on information or experience). Wayne Hendricks, managing director and head of global security at the Macquarie Group in Australia, summed this concept up nicely in a short video produced by ISMA: "We are more than just security professionals, we are risk leaders. We are change leaders. We are brand ambassadors. We are culture carriers. The values that we push out directly correlates to your brand and to your reputation." (Hendricks, 2020)

If everyone viewed the profession in this way, the practice of security risk management would be much more straightforward. That is not always the case, however. Michael Fagel, CEM, said the situation is varied, "we are viewed as a necessary evil by some, and as a critical [asset] by others. …staffing and funding is still an issue in many organizations, especially post-COIVID." As a result, "We must continually educate our principals on the ever-emerging threat patterns," appropriate business cases and security management value propositions. (Fagel, 2021)

Communicating with and educating organizational leadership will also assist with encouraging employers and C-suite decision makers to emphasize education and certification among their senior security executives as well as security staff at all levels. As mentioned, this enhances the brand and the perception of security executives and benefits all.

Recommendation: Study ways to encourage employers to focus on education and certification when recruiting, hiring, and advancing security professionals, and to actively support ongoing professional development.

Recommendation: ASIS International work with other related associations to encourage the establishment of commercial career academies for entry and mid-level security professionals. Such academies could include specialties such as security officer programs; security technology programs (electronic security systems, robotics, mobile and aerial surveillance systems, etc.); and security systems installation, design, and development programs. Successful graduates from these programs would serve to raise the professionalism of the career field and, at the same time, improve the perception and brand of the security field. Although this is not directly applicable to security management, it will impact the practice and perception of security management in organizations of all types.

Whit Chaiyabhat, CPP, MBCI, CBCP, CEM, expressed concern during his thought leader interview that one issue hampering the profession's image is the lack of a unified risk assessment approach in most organizations. With regard to risk assessment, he stated "each community has its own schema. …How can the C-suite get a straight answer as to what risks bubble up to the top when cyber, operations, security, facilities, and others all use unique methods and present their assessment results in different ways?" He suggests that security professionals "be the catalyst for change." According to Chaiyabhat, "We need a holistic common methodology for assessing risk using a common platform for depicting risks across domains and functions. Security professionals can be viewed as a trusted risk advisor by coordinating with other disciplines to develop a shared risk picture in a manner and design preferred by executive stakeholders." (Chaiyabhat, 2020)

Recommendation: Security executives should work with professionals from other staff functions to develop well-orchestrated and consistent risk assessment and display protocols so that senior decision makers are presented with a holistic view of the risks they face. This is in sharp contrast to a siloed approach that is in common use today and has been for many decades.

Recommendation: Incorporate social, cultural, and geopolitical factors into risk assessment protocols as appropriate for the organization and situation. These factors are often ignored, but can rapidly become the primary influencing factor in a drastically changing risk posture.

Recommendation: Encourage appropriate use of data analytics and decision-making technologies as tools in strategic planning. In addition foster a spirit of continual improvement in developing and applying metrics for security management application.

The following additional recommendations are meant to enhance the brand and reputation of the profession as well as facilitate recruiting and onboarding of mid-level and senior security executives and staff.

Recommendation: Job descriptions for security positions should be factual and accurately describe the roles and responsibilities envisioned by the senior executives. For example, does the position involve strategy development, strategy implementation, or strategy monitoring (or some combination of those)? These are very distinct functions and the candidate and hiring organization should be aligned in their understanding of the role. Also, be clear about whether or not the position involves cybersecurity responsibility and if so, the nature and extent of those responsibilities. Misunderstandings over issues such as these have led to situations where there is a very poor fit between the individual security professional and the position they were selected to fill. This degrades the quality of the security management for that organization and can also cause significant harm to the reputation and image of security and the individual involved.

According to Miranda Coppoolse, CFIP, founder and CEO of MC Global, "We cannot so much affect a technical failure, a natural disaster, or the motivation of a person with a bad intent, but we can control the opportunity with better risk planning. We have the responsibility for ensuring we have the greatest understanding of the risks facing us and we cannot do that if we continue working in silos. Only together we are stronger and smarter. Only united we can make this world a safer place!" (Coppoolse, 2021) The tagline for MC Global is "where security, risk and human behavior intersect." This is an excellent word picture for an effort to enhance the brand and reputation of the profession. Through collaboration and excellent marketing that unifies disparate communities within the profession, security management can become a far more respected, and hence more effective partner and advisor – and greatly enhance both perception and practice.

Recommendation: Orchestrate and launch a deliberate and aggressive marketing and branding strategy for the overall security management profession. This must involve marketing experts as well as security professionals around the globe. Campaigns must be tailored to the culture, language, and region of a particular area. Although professional associations have long worked in this direction, their efforts have been focused, to some degree, on marketing the organization rather than the profession as a whole.

Recommendation: ASIS International in cooperation with other associations should facilitate collaboration whereby the profession moves toward a more holistic and multifaceted model. Educational programs, materials, publications, and communications distributed by the associations should deliberately identify and avoid terminology conflicts and occurrences of the profession continuing to operate in silos. We must move toward ESRM and collaborative model. By presenting a united and responsible story to the C-suite, stakeholders, and the general public globally, the profession can improve its image and reduce negative perceptions of the field and what it entails.

STATE OF SECURITY MANAGEMENT: FOLLOW-ON

This study is meant to serve as a baseline of the security management profession, both in terms of perception and practice, at a point in time. It should be used for future benchmarking and trend analysis. Among the key topics that the authors feel should be tracked over time are:

- The key challenges faced by senior security executives and their teams.
- How the skills and individual attributes needed for success in the profession are evolving.

- What tools senior security executives use (or have at their disposal) to support their ability to influence business decisions and garner resources.
- How people interact with technology, especially in terms of decision making, data analysis, and management of the security function, and relationships with internal and external stakeholders.
- How core philosophies such as ESRM develop and are applied over time (including changes in how they are interpreted and applied).

Because many changes in the field are occurring rapidly, the recommended interval to revisit the findings in this report is two to four years. This interval allows an appropriate amount of time for both business and risk environments to evolve, technology advances to develop and be implemented, and conceptual thinking to progress within the profession.

AREAS THAT WARRANT FURTHER RESEARCH

Based on the findings and conclusions of this report, the following efforts are recommended in terms of future research related to the security management profession.

- An evidence-based study of root causes for the lack of women in senior security executive positions or positions leading up to that of a senior security executive. The study might suggest strategies for appropriately expanding the number of women in the field such that benefit accrues to the profession, the people who comprise it, and the organizations they serve.
- A proposed strategy for incorporating geopolitical and social risk into the field of security management (including defining, measuring, and communicating such risks).
- A detailed study of how advanced educational programs can best serve the security management profession and organizations that engage security executives.
- A proposed strategy for assessing and bolstering external perceptions of the security profession and security risk management practices and precepts.
- An examination of how technology tools such as AI and data analytics can most effectively be incorporated into the decision making regimes that support senior security executives in carrying out their responsibilities.
- A study of employer perceptions of the security management field and to develop strategies for recruiting, hiring, developing, and advancing mid-level executives to senior-level security executives. Further, it would be of value to conduct such a study using a variable of geographic regions and cultures.

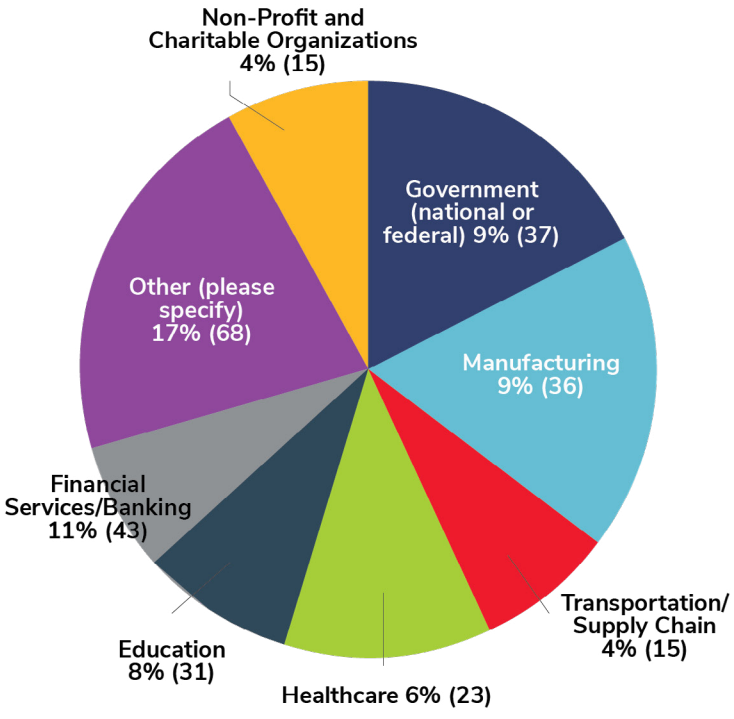
Note that these recommendations do not include important "operational" topics such as potential new uses for drones in support of security operations, and the effective use of robots and robotics in the field. The list is limited to security management subject matter that clearly warrants further investigation. Ideally, research on these and similar topics will complement this study.

Appendix A

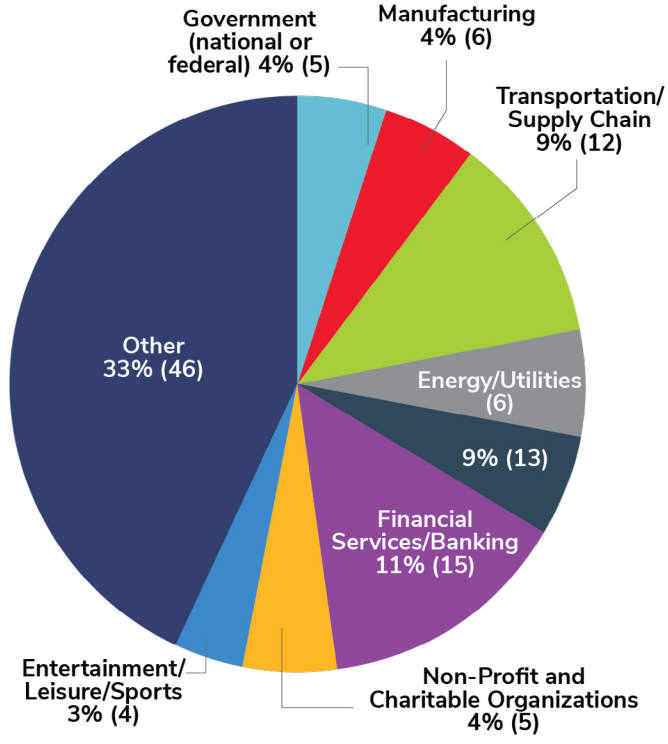
SURVEY COMPARISON BETWEEN ENGLISH-SPEAKING AND SPANISH-SPEAKING RESPONDENTS

One of the clear results of this study is that English-speaking and Spanish-speaking respondents viewed many things differently, while also seeing some things the same. This appendix provides a side-by-side comparison of the survey question results for both respondents to the English and Spanish version. Where appropriate, there is also narrative comment on the results and added perspective. The information is provided for the benefit of readers who wish to explore this issue further.

The following represents the primary industry sectors respondents work within. To the question, "What is the primary industry sector in which your organization operates?". The English-speaking respondents stated that besides Government, Transportation/Supply Chain, Manufacturing sectors, the other categories identified are Hospitality, Security Consultants, Oil & Gas and Real Estate. The differences between the English- and Spanish-speaking respondents are displayed below. 11% of the English-speaking respondents work for Financial Services and the Banking industries. Interestingly, the same percentage, 11% of Spanish-speaking respondents also work for Financial and Banking industries. Following this group of English-speaking respondents, the other industries with which they work are Government, Manufacturing, Education, Healthcare, and 'other'. The other category consists of 18% of the respondents. The Spanish speaking respondents work with Transportation/Supply Chain, Energy/Utilities. 33% of the Spanish speaking respondents selected the 'other' category.

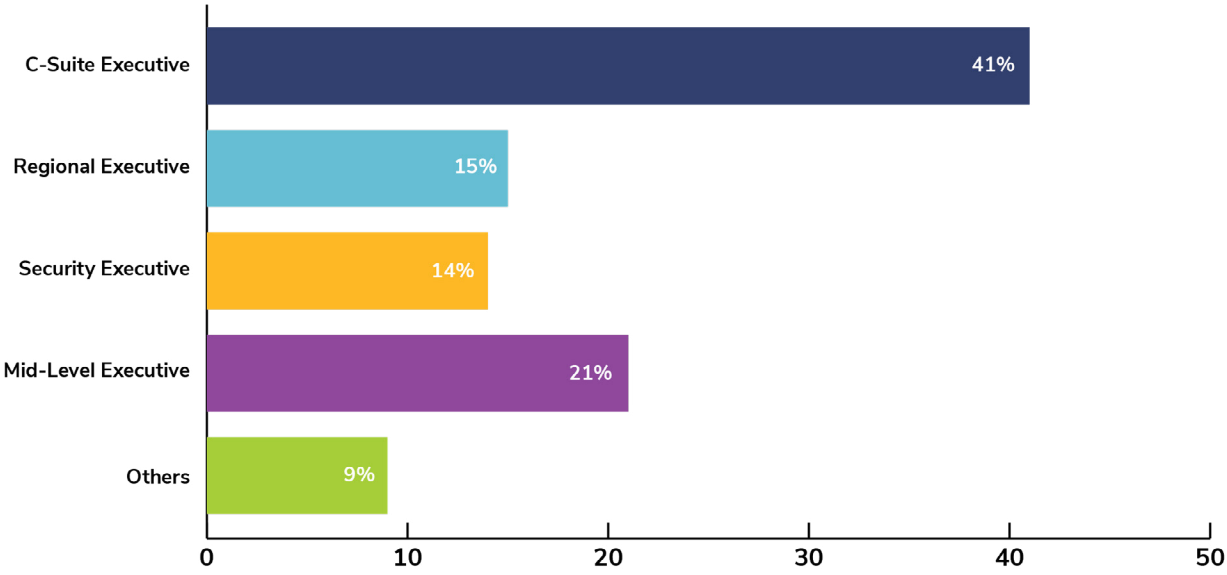


English Speaking Respondents

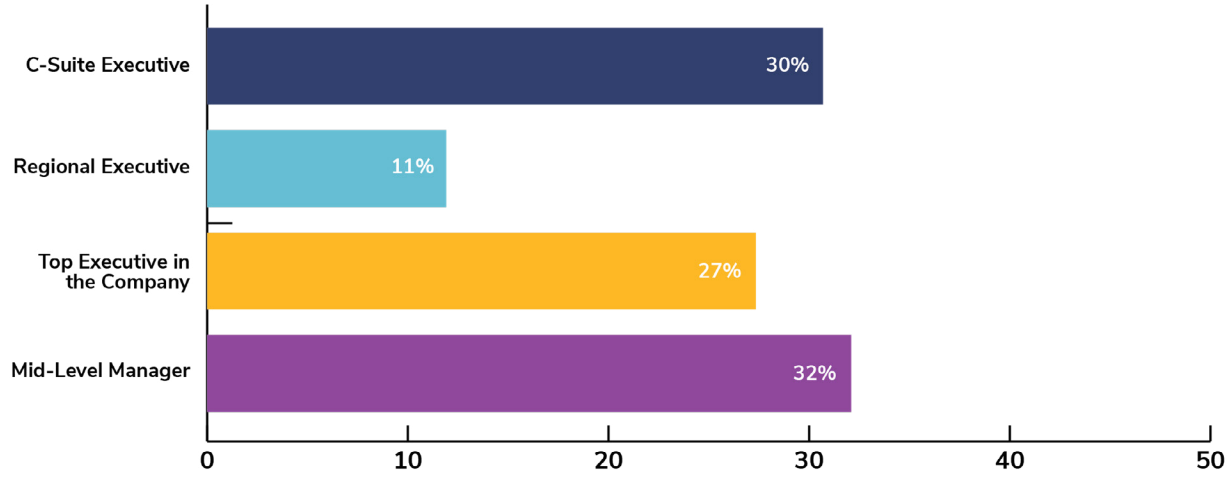


Spanish Speaking Respondents

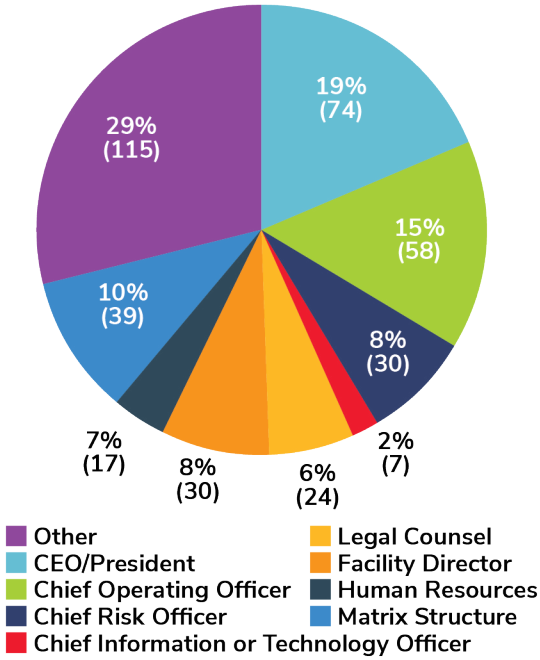
To the question, "At what level of the organization do you operate?", the following shows the various levels the English-speaking respondents stated they operate with. 41% of survey respondents operate at the C-suite executive level. The second largest at 21% work at the mid-level executive level.



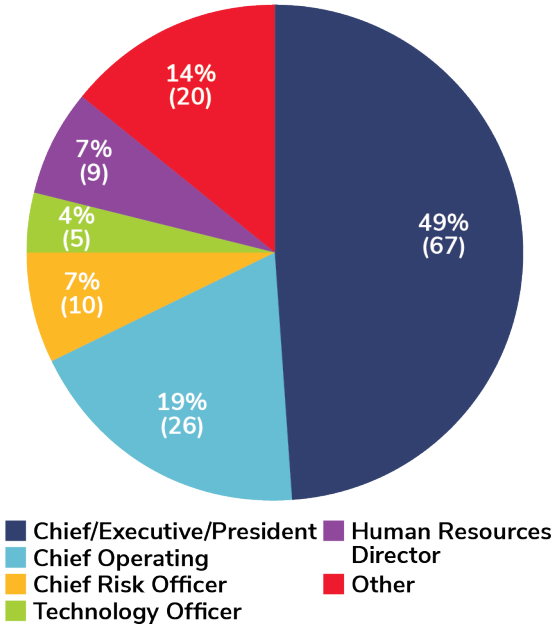
The Spanish-speaking respondents answered the same question as shown below. There is no 'other' category and the percentage of respondents who stated that they operate at the C-suite level and mid-level managers are 30% and 32% respectively. The top executive refers to senior executives at 27%. Security management professionals who completed the survey indicate that most of them work with C-suite/top executive and mid-level executives. This data meets with the expectation that this function is a top-level function within a firm.



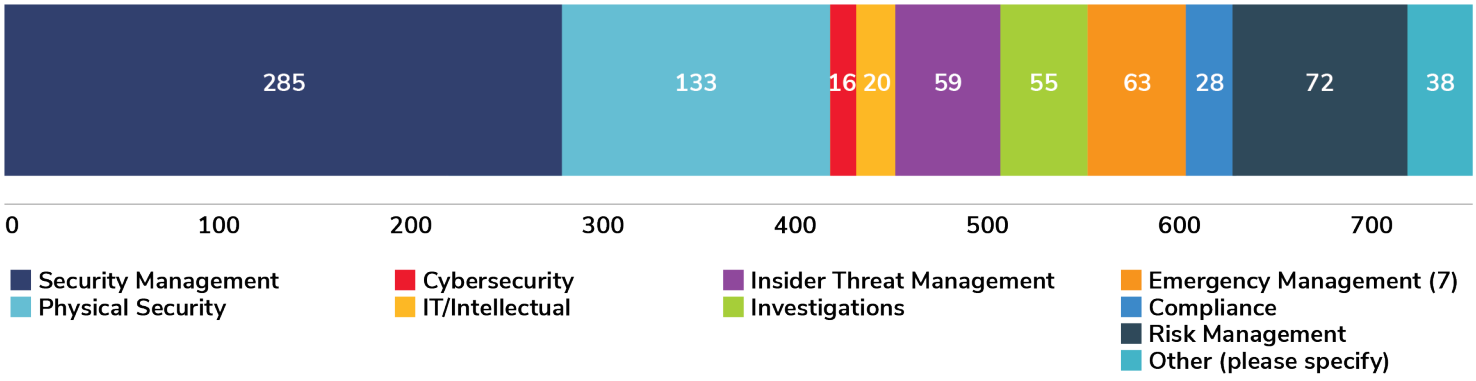
To the question, "What level and function of the organization do you report to?", the English-speaking respondents answered as shown below. The 'other' category at 29% can be interpreted as an indication that the field is evolving, and new structures are being tested. The Spanish-speaking respondents also indicate that besides the top-level executives, 29% report to others.



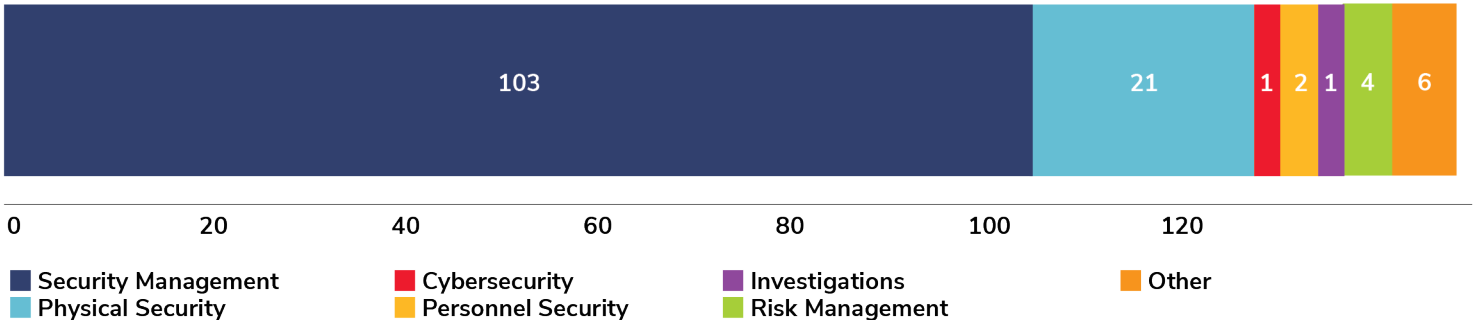
The Spanish-speaking respondents answered the same question as shown below. As indicated a larger percentage of respondents are reporting to the CEO/President. It is also important to note that the matrix structure is not prevalent with Spanish-speaking organizations.



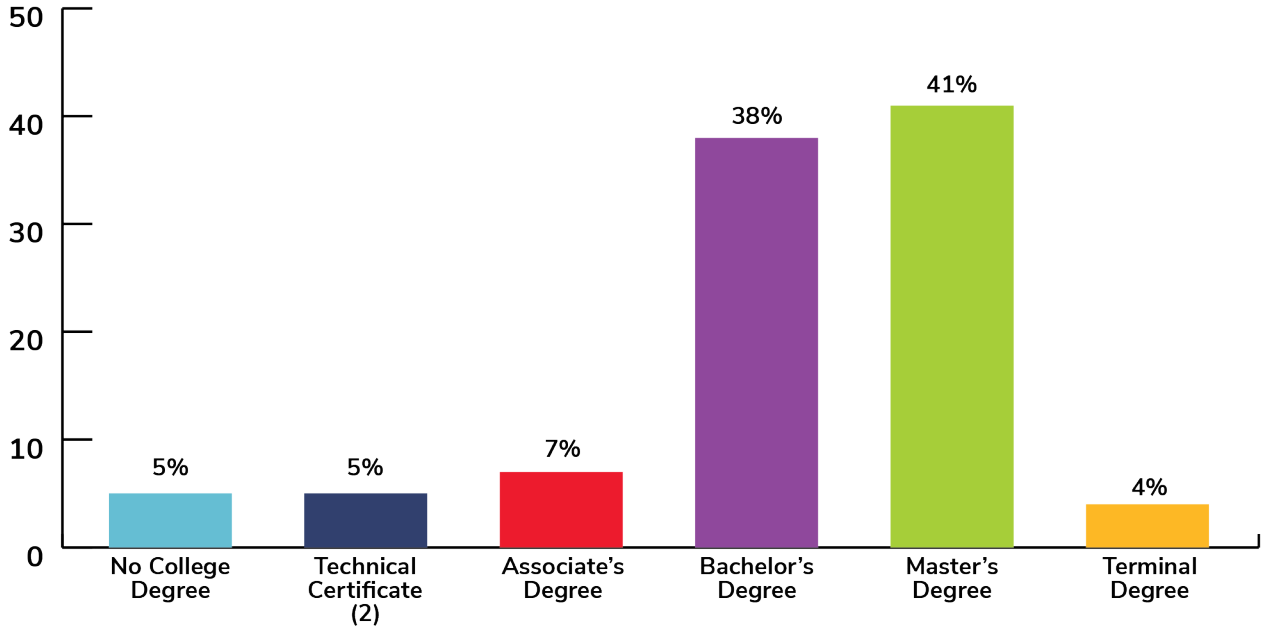
To the question, "What is your personal specialty or discipline?", English-speaking respondents answered as shown below. A majority indicated security management or physical security. Risk management and emergency management and insider threat were cited along with investigations as personal specialty.



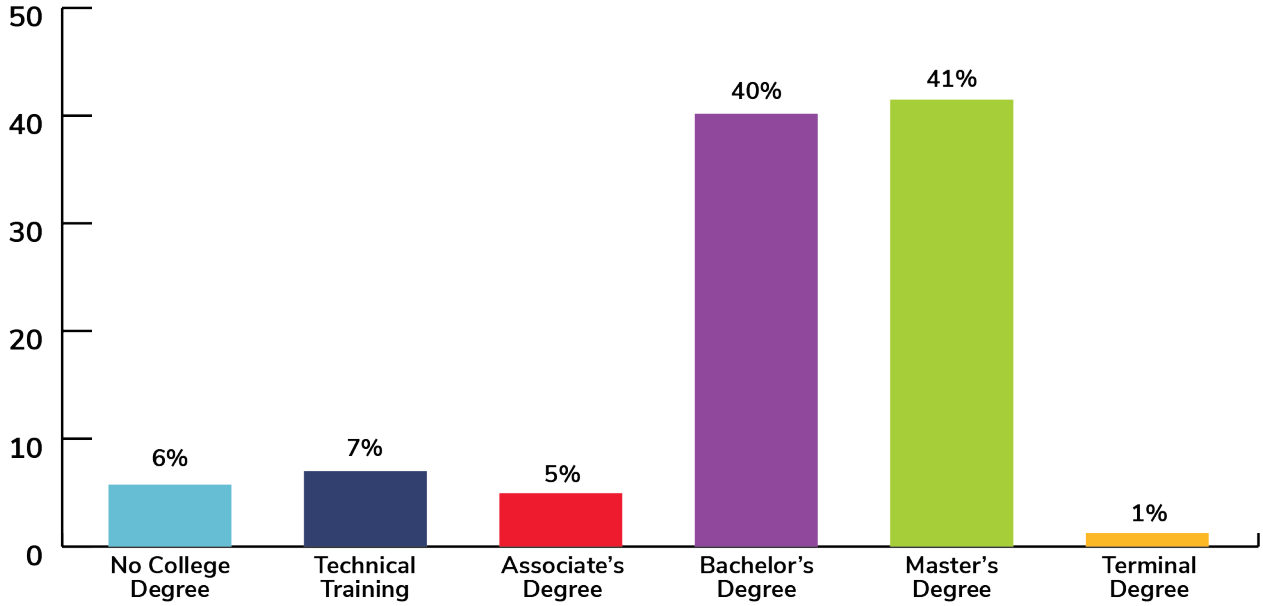
To the same question, the Spanish-speaking respondents answered as follows. Security management and physical security are identified by both groups as the first and second personal specialties by both groups of respondents. The Spanish-speaking respondents were less focused on other specialties.



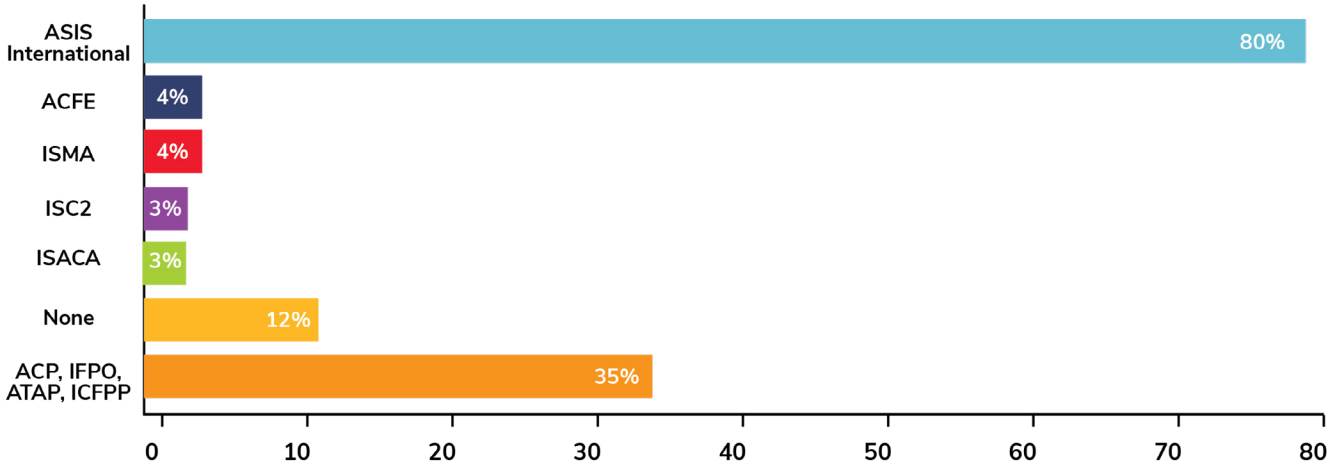
To the question on education level, the English-speaking respondents answered as shown below. A majority of them have a master's or bachelor's degree.



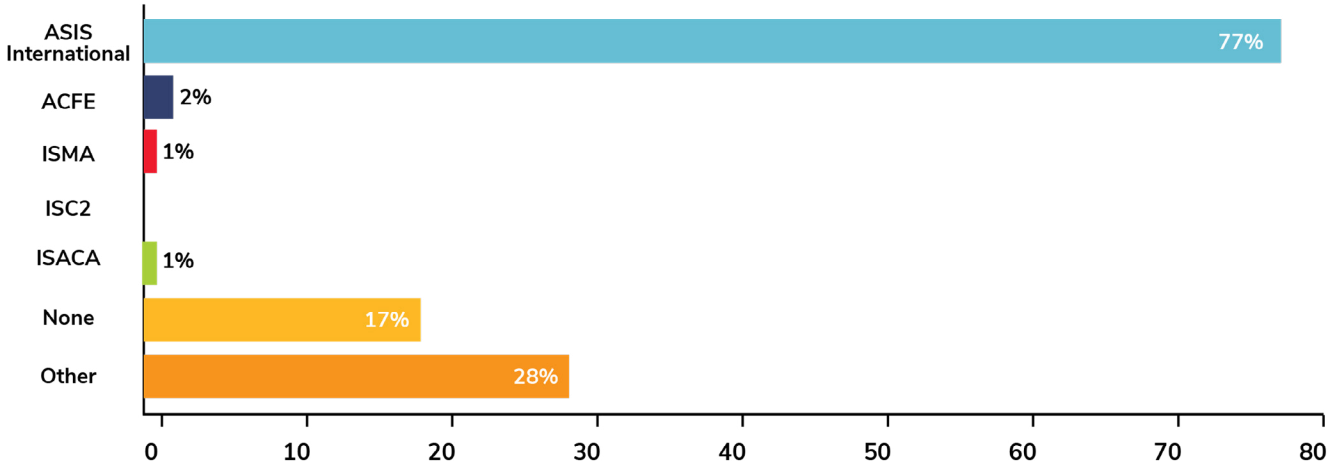
To the same question, the Spanish-speaking respondents answered as shown below. It is interesting to note that these groups answered the question similarly. The difference seems to be with technical certificate for the English-speaking group when compared to the Spanish-speaking respondents.



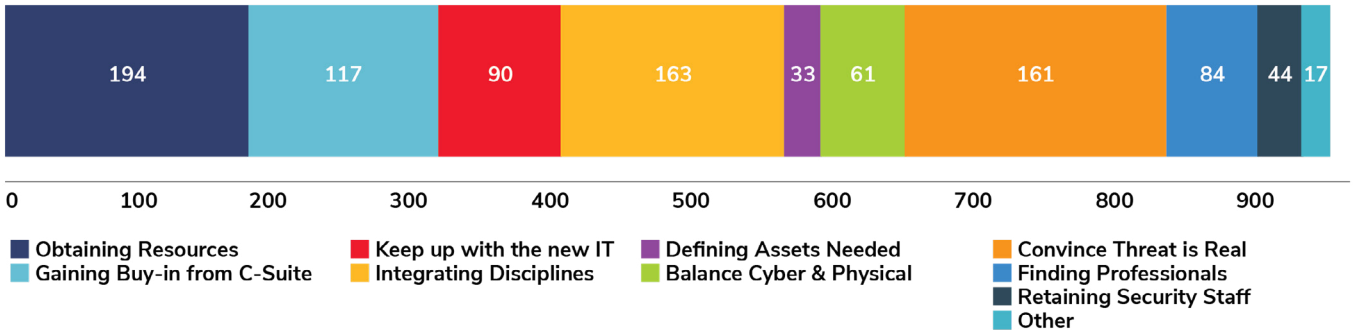
To the question, which professional association they belonged to, the English-speaking respondents answered as follows.



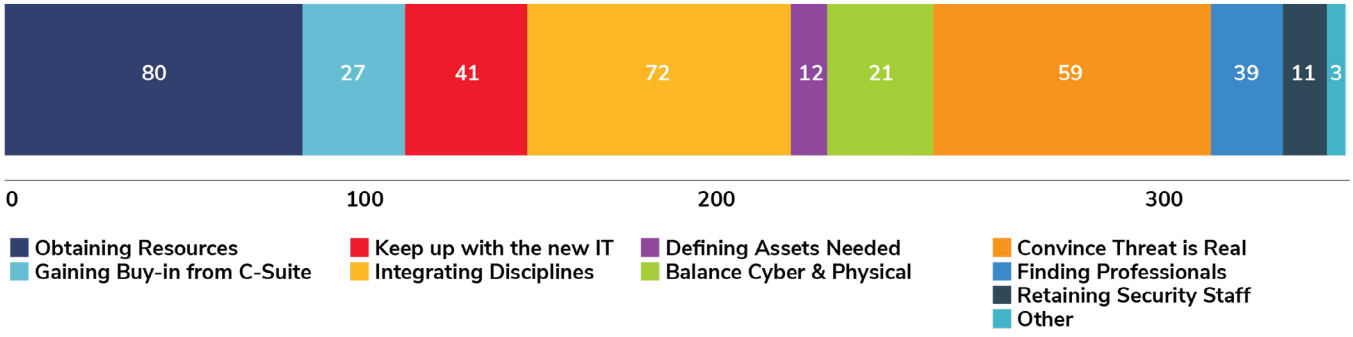
To the same question, the Spanish speaking respondents answered as shown below. Clearly ASIS is the dominant association that both groups of respondents belong to. However, this is likely a function of the fact that ASIS members were the focus of this survey. Regardless, as a global organization, ASIS certainly is the leading association for security management professionals.



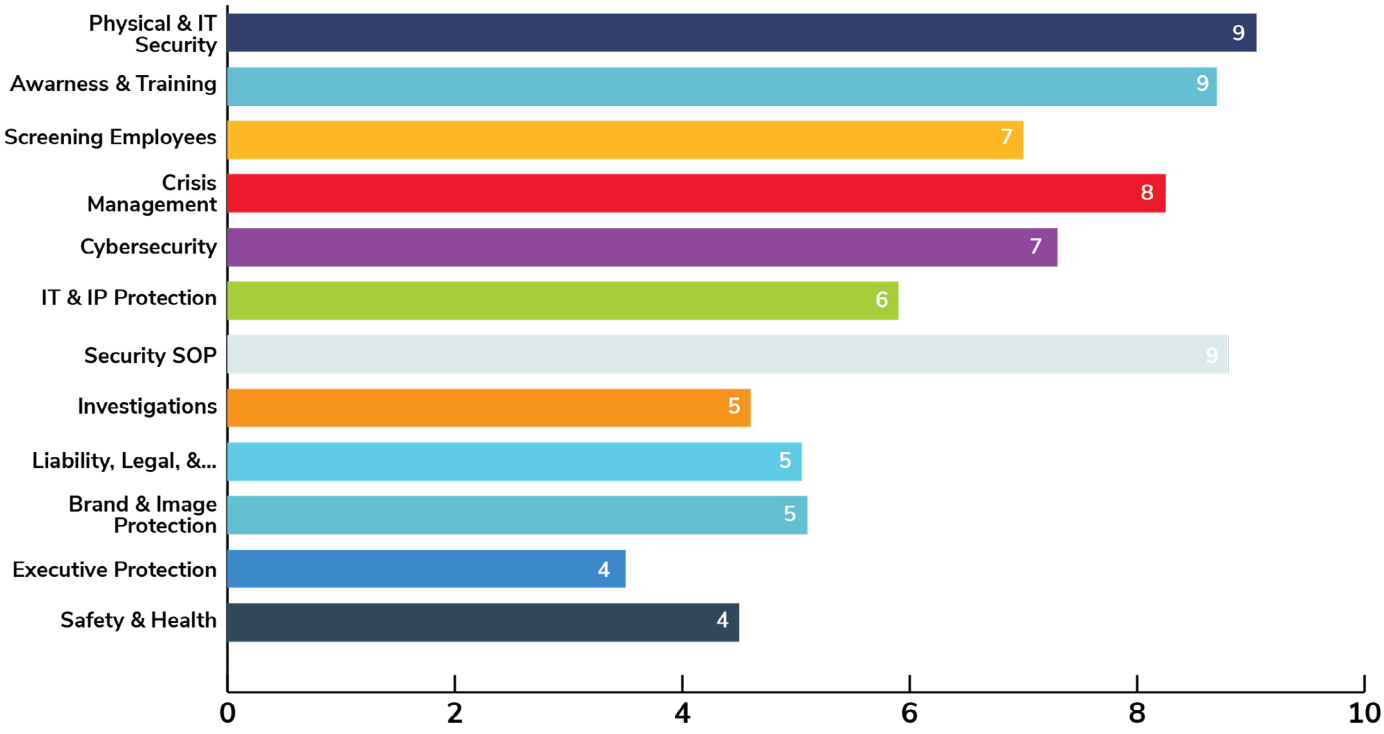
To the question "Identify key challenges in performing your roles as Security Managers," the English-speaking respondents answered as shown below.



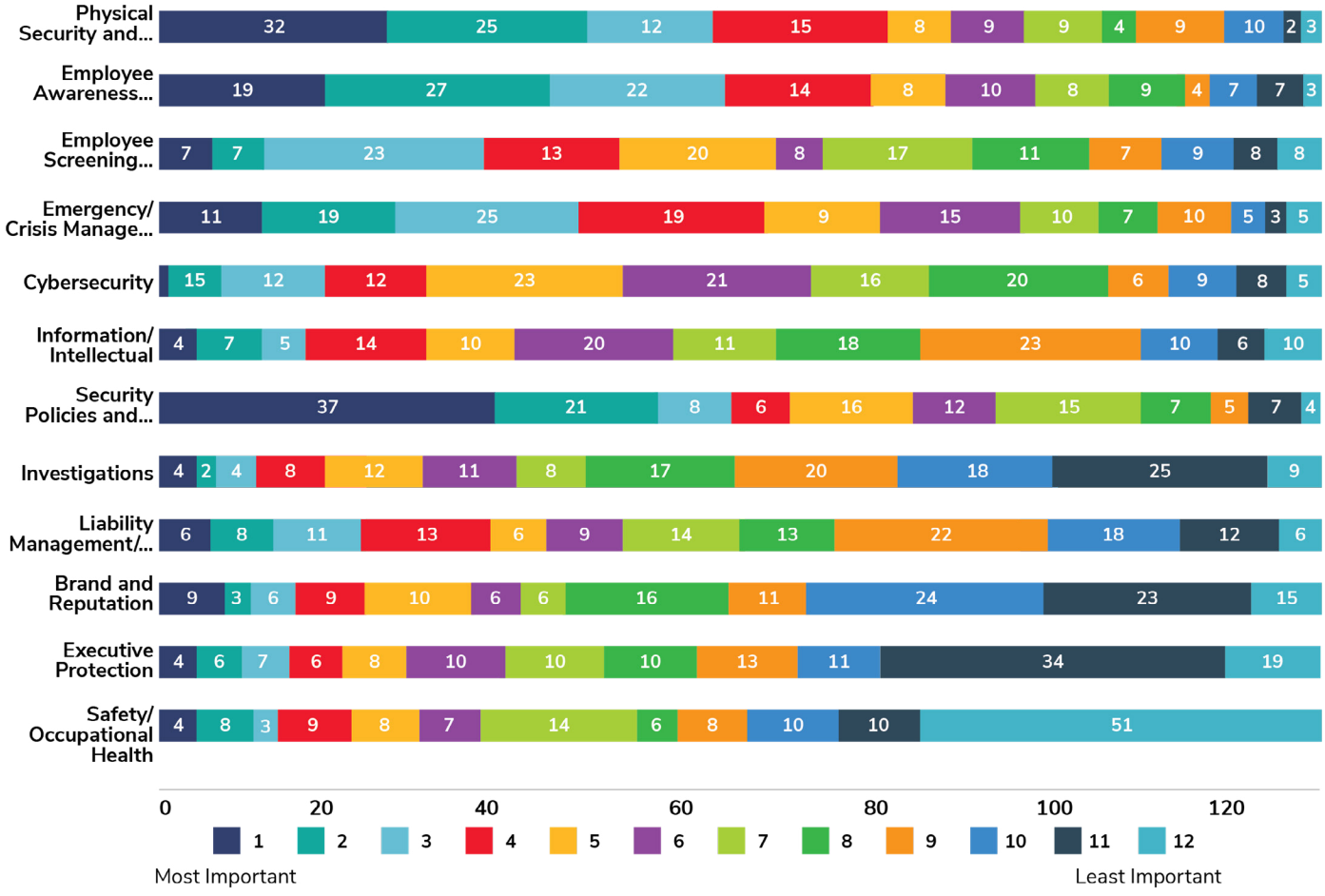
The same question was answered by Spanish-speaking respondents as follows. 'Obtaining resources, and integrating disciplines' stand out along with 'convincing threats are real' stand out as challenges. Finding trained security management professionals is also cited as a challenge by both groups.



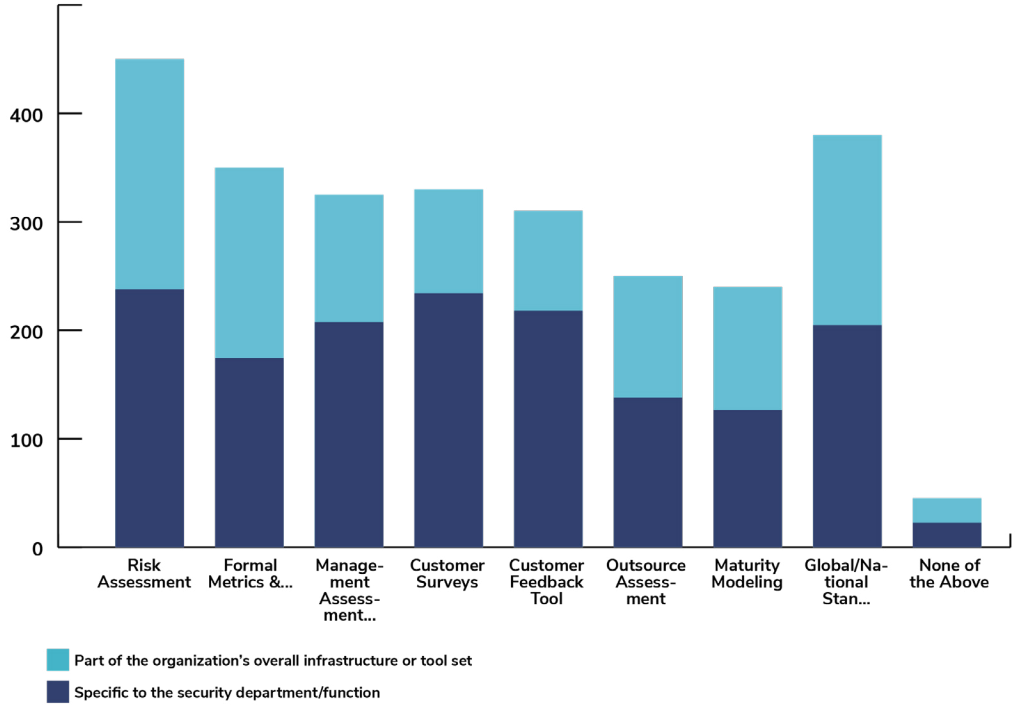
To the question, 'Please rank the importance of the functions that you believe comprise security management (1 = most important, 12= least important)," the English-speaking respondents answered as shown below. (Number indicates weighted averages). The functions that are listed below as most important are physical and IT security systems, awareness and training, security standard operating procedures. Crisis management are some of the other functions that are noteworthy.



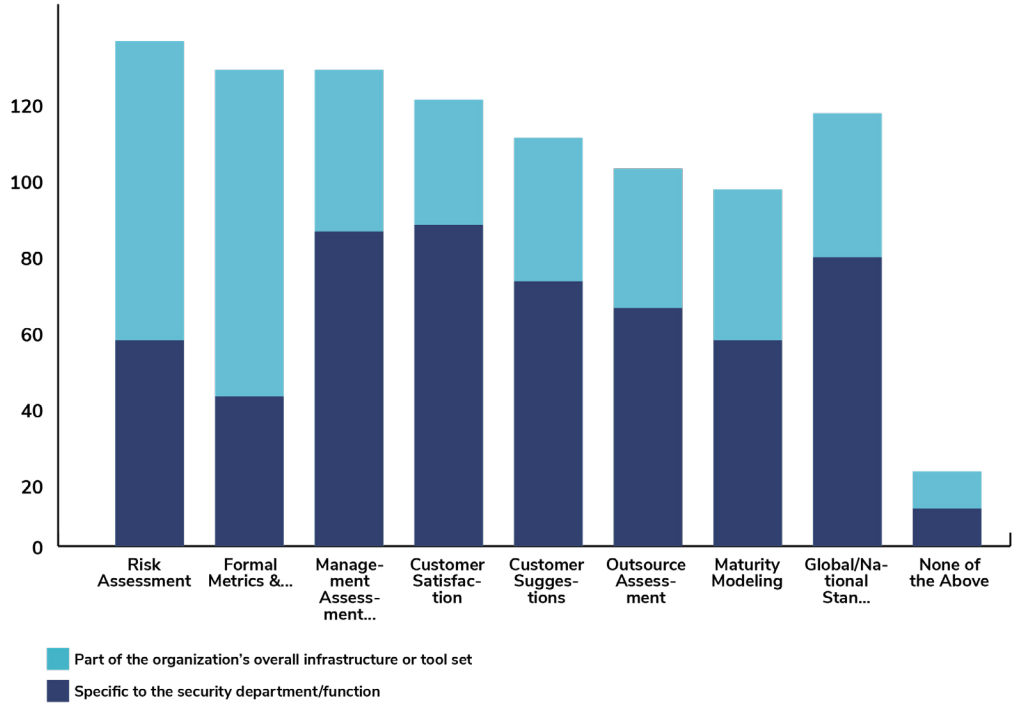
To the same question, the Spanish-speaking respondents answered as follows. Differences worth noting are, safety and occupational health and executive protection are more important. This stands to reason because in countries like Mexico, Argentina, Chile, Columbia, Costa Rica, and El Salvador, security management professionals are called on for protection of executives more than in the United States, Europe, and other nations.



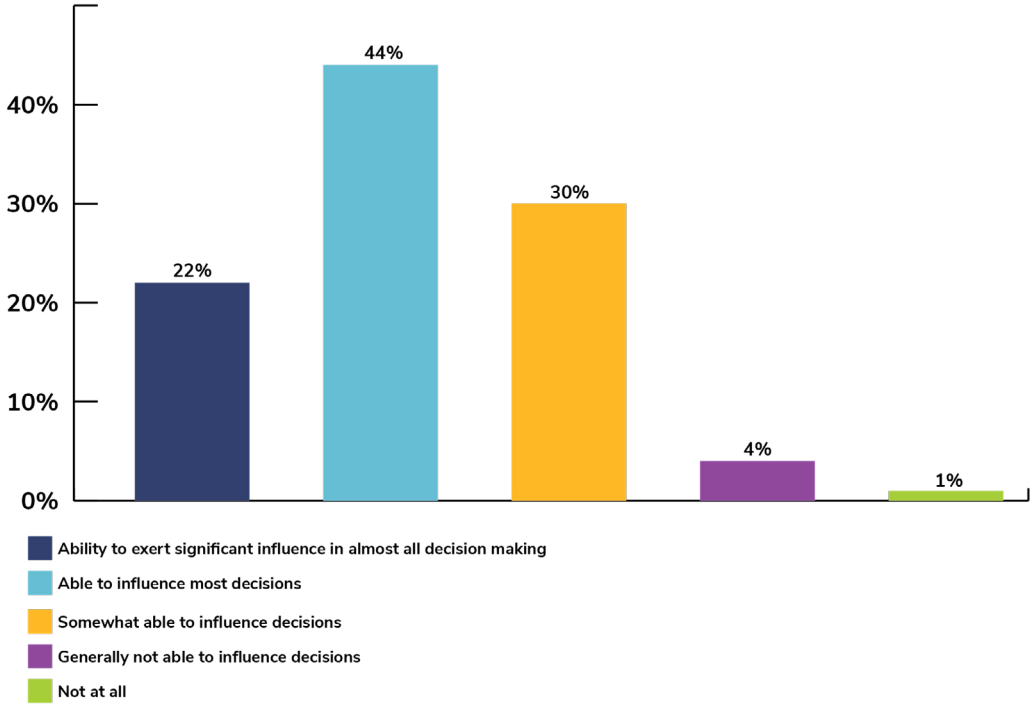
To the question, "What tools do you use to assist in performing your security management mission? (please check all that apply and indicate whether the tool is an organizational one or a separate one only used by the security function)," risk assessment was identified by 64% of the respondents as the important tool and part of the overall organizational structure. Customer feedback and surveys along with management assessment were identified as important tools needed to perform as a security manager.



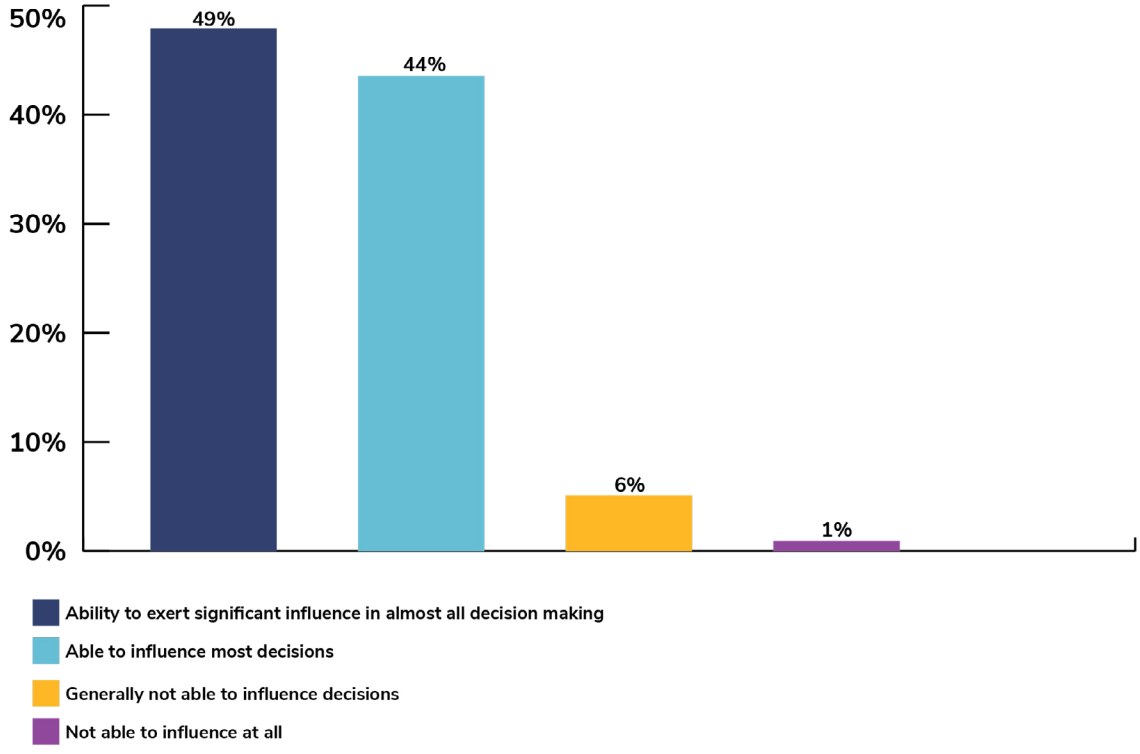
The same question was addressed by the Spanish-speaking respondents in the following manner: Outsourced assessment and global/national standards are seen as important in addition to customer feedback.



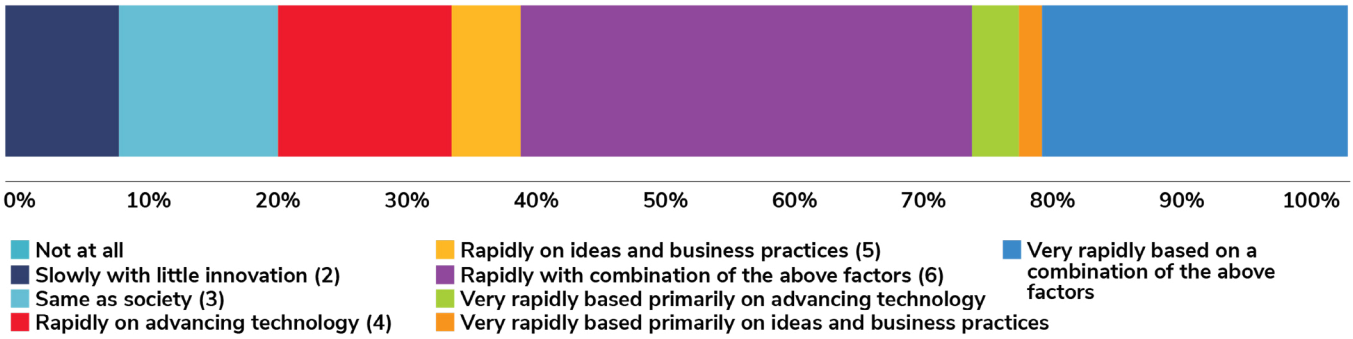
We asked respondents to rate their ability, as a security executive, to influence decisions in their organization and among its executive management. The English-speaking respondents answered as follows.



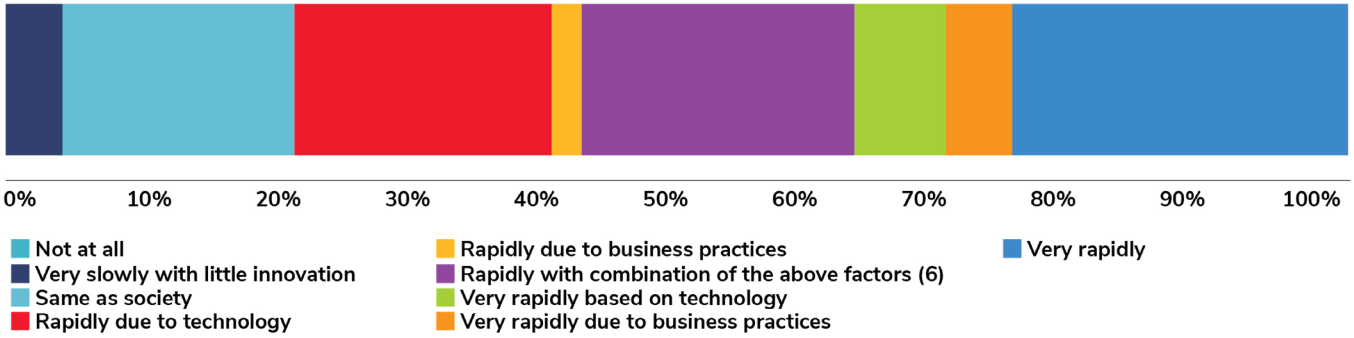
The same question elicited responses from the Spanish-speaking respondents as shown below. Both groups indicated they feel confident that they can influence most decisions made by the organization with respect to security management.



To the question, "To what degree do you think that security management as a field is changing?", the English-speaking respondents stated the following: All of the respondents indicated that the field is changing. There are minor differences about how the field is changing.

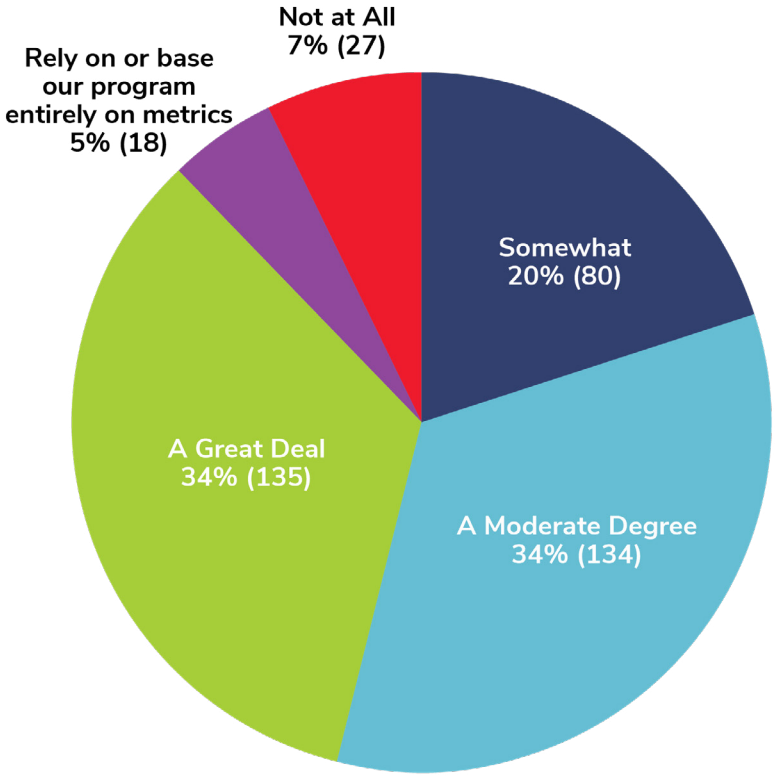


To the same question Spanish-speaking respondents stated the following.

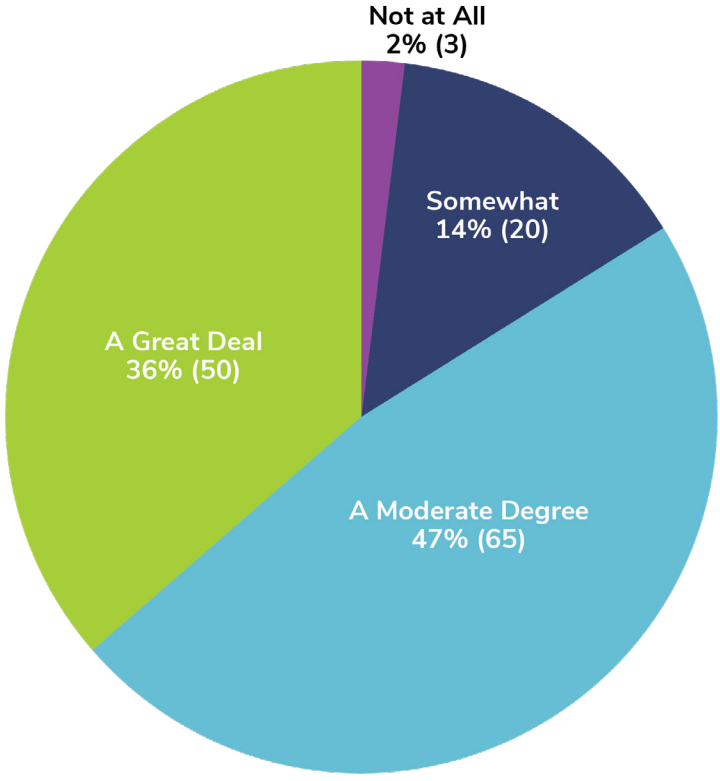


Both groups of respondents agree that security management is changing rapidly or very rapidly. There are small variations as to what is driving the change. However, the overwhelming evidence is that the field is changing.

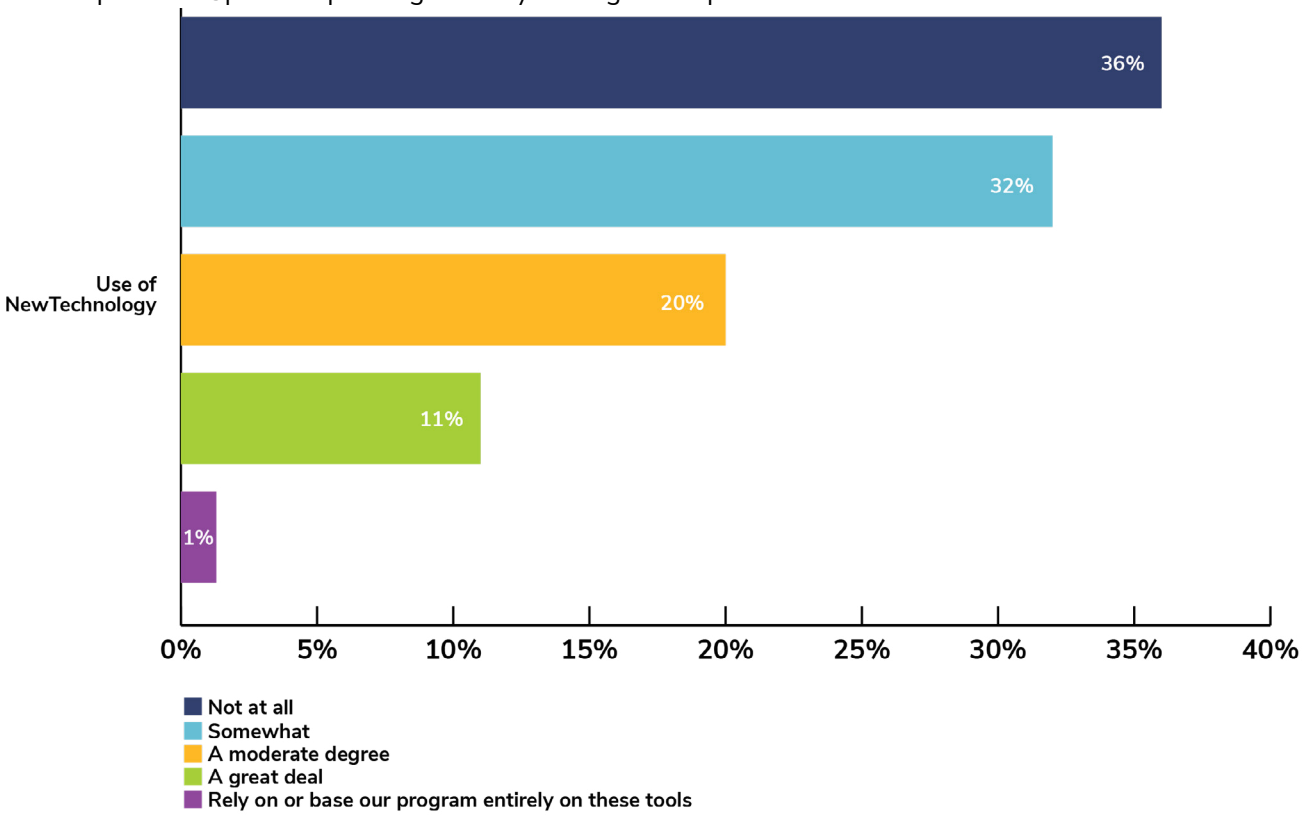
To the question, "To what degree do you use metrics and statistical analysis in performing your security management roles and responsibilities?", English-speaking respondents result below. 68% mentioned that they use metrics a great deal or to a moderate degree.



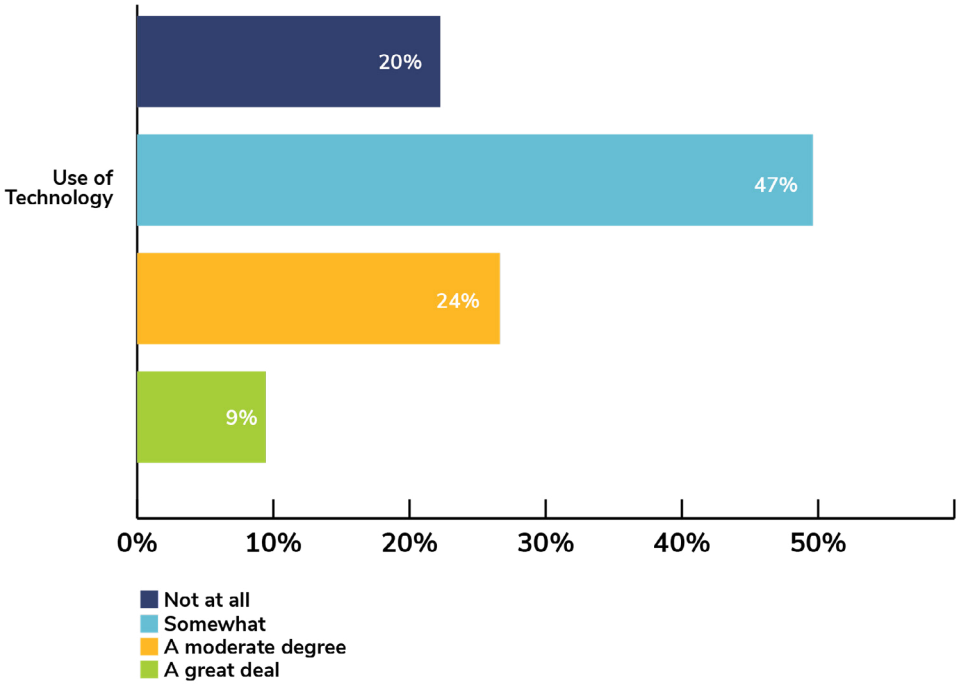
Spanish-speaking respondents results are below. A majority of both groups agreed that they use metrics a great deal or moderately.



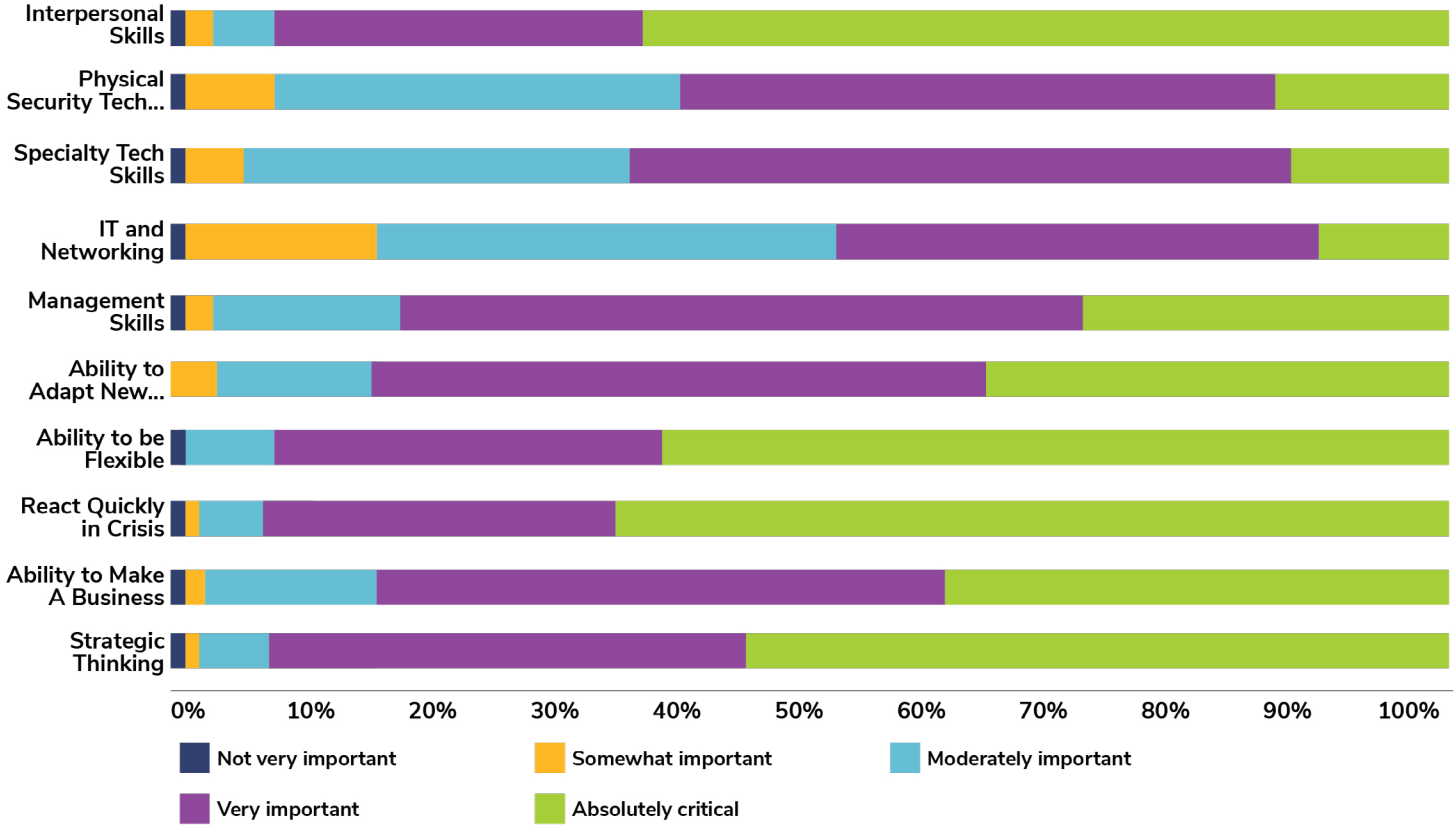
To the question, "To what degree do you currently use advanced technologies such as Artificial Intelligence, Machine Learning or Data Analytics to aid in decision making or p program management?", 36% of English-speaking group indicated that they do not use AI and ML tools; 20% of their counter parts with Spanish-speaking indicated that they do not use such tools. It is interesting to note that a larger number of English-speaking professionals did not use these tools when compared to Spanish speaking security management professionals.

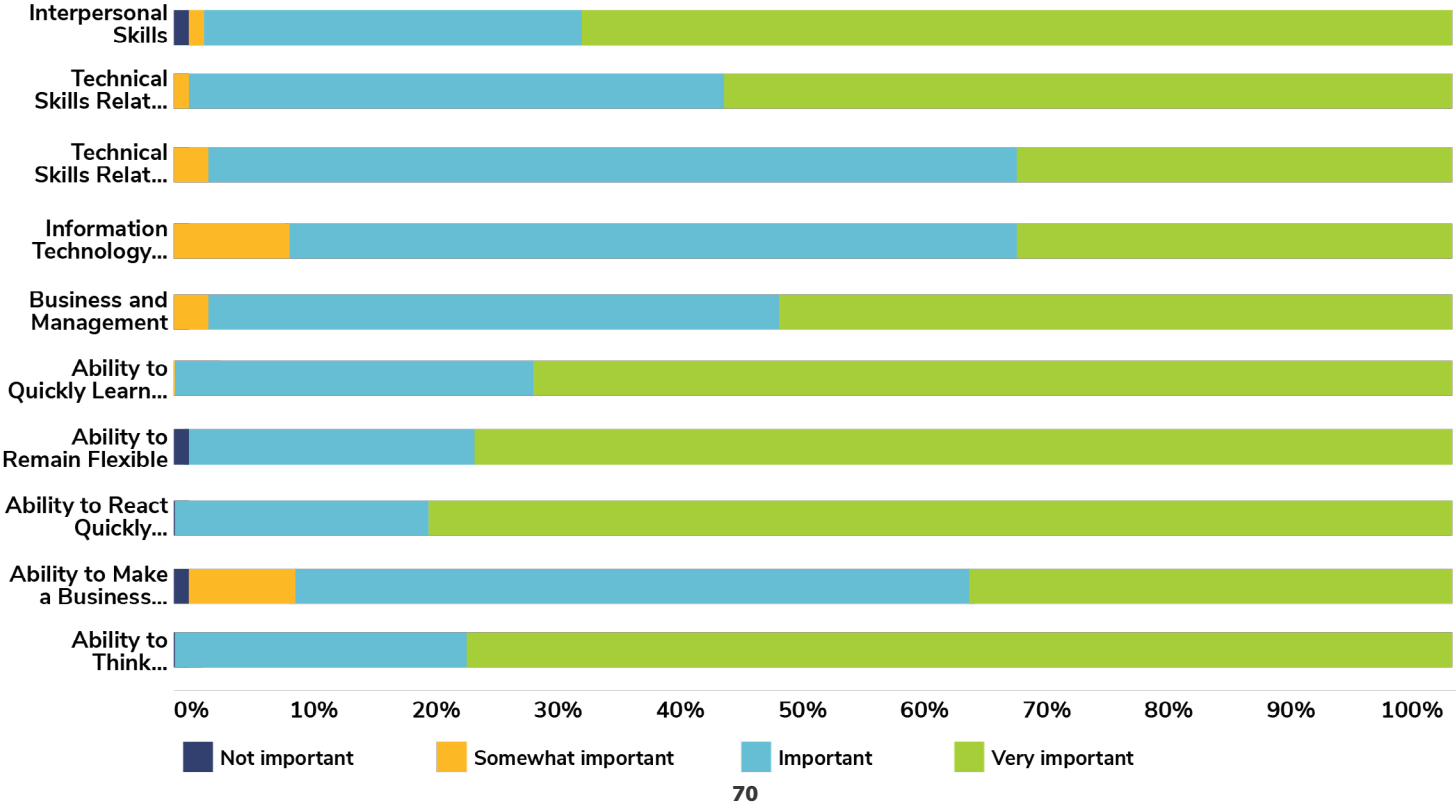


Spanish-speaking respondents answers are below.

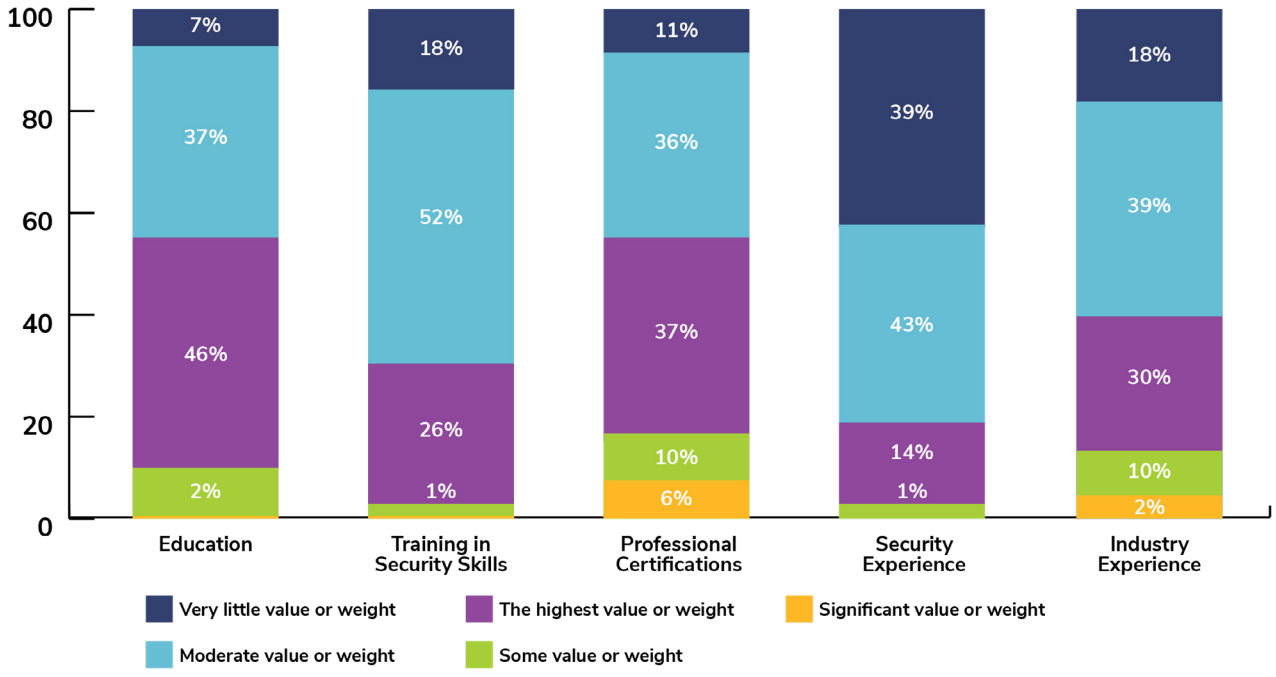


To the question, "What skills and qualifications do you feel are needed in the successful security professional today and in the future?", people skills were indicated as critical by both groups. This finding affirmed the earlier finding that security management as a profession was driven by the people in the profession. Notwithstanding the language nuances between English and Spanish there was overwhelming evidence that people skills drive the success of this profession.

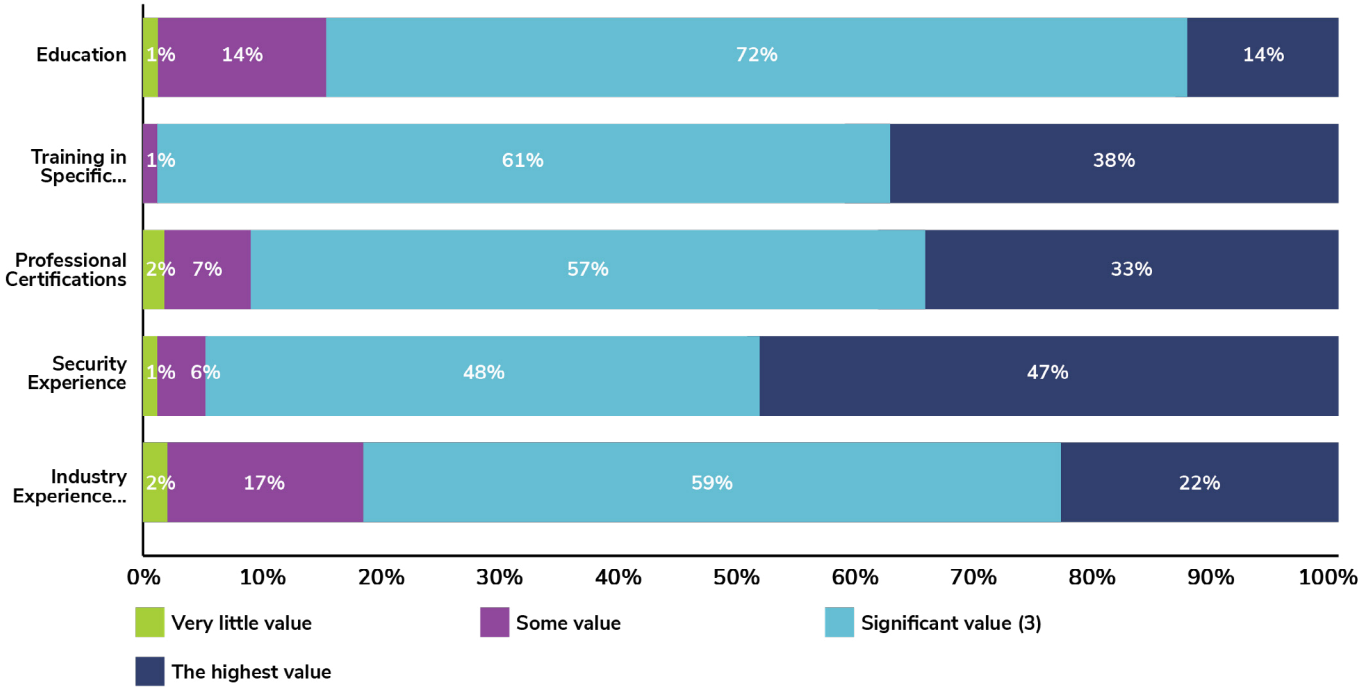




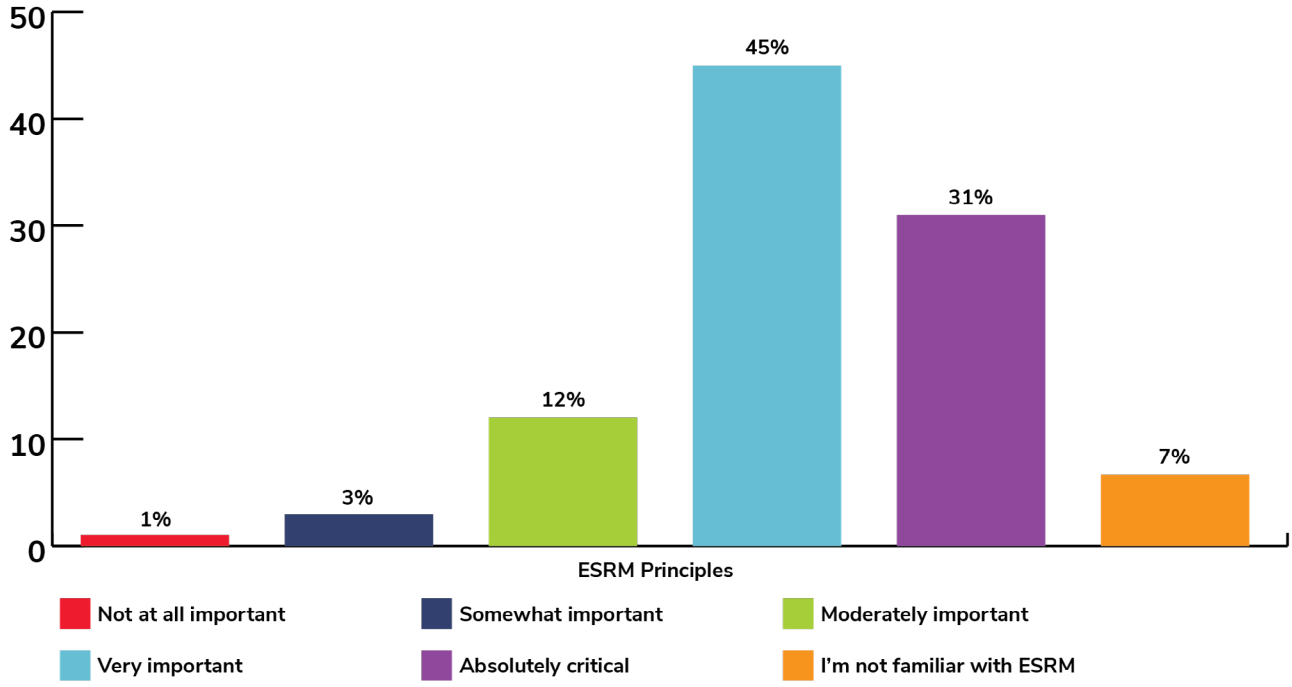
To the question, "What value do you place on each of the following components when seeking a candidate for a position on your professional security staff?", both groups of respondents indicated that education and training were more important than experience in the field. Collectively speaking, experience was considered important, but not as important as education, training, or certifications.



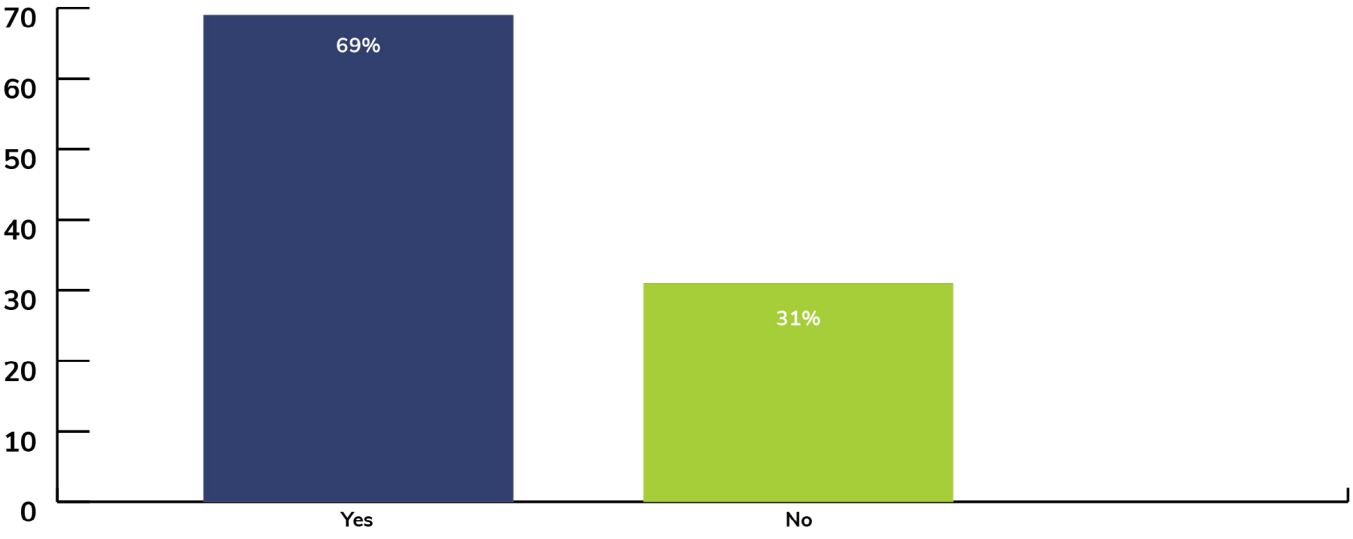
Spanish speaking



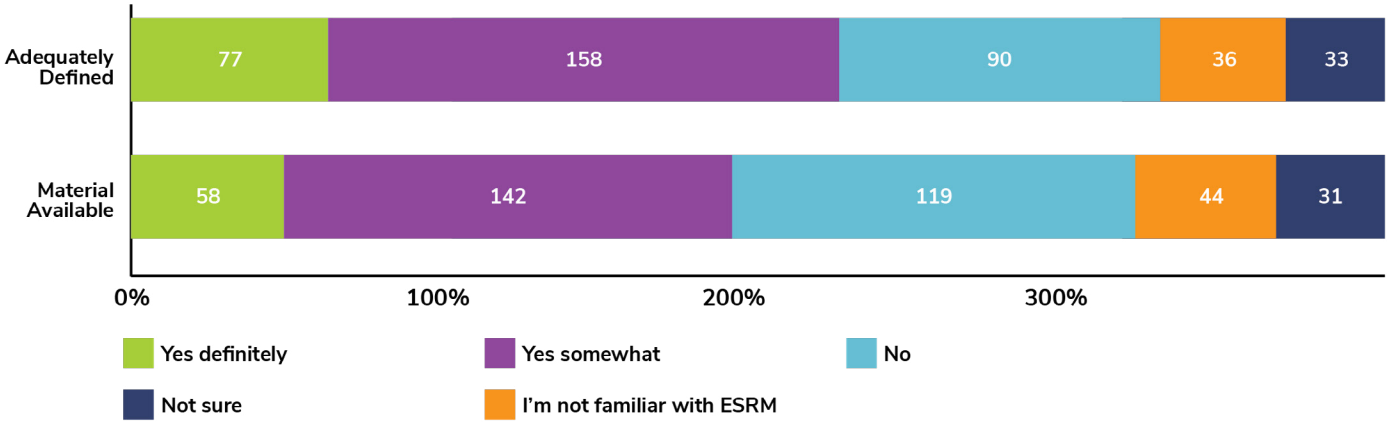
To the question, "How important do you believe it is to apply the principles of ESRM (Enterprise Security Risk Management) in performing your duties and how do you implement them?", a majority of the respondents stated that ESRM is important and indicated that ESRM will be part of the future landscape of security management.



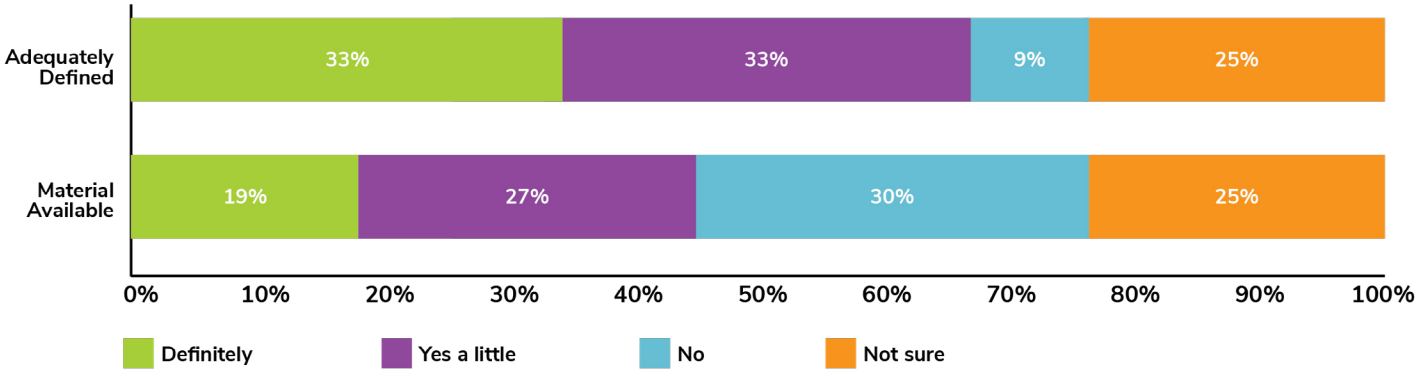
Spanish speaking



To the question, "Do you believe that ESRM is adequately defined as a concept and that enough useful reference material is available to successfully implement it?", both groups of respondents indicated that ESRM is somewhat defined but not adequately. There were approximately 35% of the respondents indicating that ESRM is not defined.



Spanish Speaking Responses below.



The consensus is that ESRM as a concept is gaining momentum and becoming popular. However, there is a lack of clarity of what ESRM is and how it is defined.

ASIS INTERNATIONAL
Advancing Security Worldwide®

FACT SHEET

Appendix B

ASIS INTERNATIONAL FACT SHEET

ASIS: A 65-YEAR COMMITMENT TO EXCELLENCE

Celebrating 65 years, ASIS is the leading association in advancing security worldwide, promoting excellence and leadership within the profession and is deeply committed to advancing and reinvesting in the industry. ASIS remains dedicated to expanding and enriching knowledge sharing, best practices and peer-to-peer connections so security professionals across disciplines—and at all stages of their careers—can easily access the information and resources they need to succeed. ASIS also manages the world's leading security trade conference and expo, Global Security Exchange (GSX), which unites the full spectrum of the industry: cyber, operational and physical professionals from private and public sectors.

ASIS BY THE NUMBERS

34,000
members in 158 countries

11,022
certificants worldwide

252
chapters in 87 countries

25+
webinars produced annually

35
subject area communities

10
Standards published

6
Guidelines published

4
globally-recognized certifications offered

NEWEST CHAPTERS (2020)

Ahmedabad, India
Chennai, India
Honduras
Kumasi, Ghana
Portugal
Pune, India
Takoradi, Ghana

MEMBERSHIP OPTIONS

Adjusted Rates for Emerging Markets: Available for qualified individuals living in countries classified as upper-middle, lower-middle, and lower-income by the World Bank

Reduced Student Rates: $20 student dues for full-time students pursuing a security related degree (includes all-access registration to GSX)

MILESTONES:

'50

1955 American Society for Industrial Security (ASIS) created; First Chapter recognized (Southern California)

1955 ASIS Annual Seminar holds first show

'60

1957 First issue of *Industrial Security* magazine published

1966 ASIS Foundation launched

1973 ASIS Annual Seminar added "and Exhibits" to its formal name

'70

1972 *Industrial Security* renamed *Security Management*

1977 Certified Protection Professional (CPP) certification launched

1978 ASIS reached 10,000 members

'80

1984 ASIS reached 20,000 members

1995 ASIS bookstore launched

1989 First woman president named to Board of Directors (Darlene Sherwood, CPP)

1999 ASIS reached 30,000 members

'90

2003 Professional Certified Investigator (PCI) and Physical Security Professional (PSP) certifications launched

2001 ASIS Commission on Guidelines launched

'00

2002 Name changed from ASIS to ASIS International; "Advancing Security Worldwide" tagline adopted

2008 ASIS Commission on Guidelines added "Standards" to its title, is it became an American National Standards Institute (ANSI) accredited Standards Developer

'10

2018 ASIS Annual Seminar and Exhibits re-branded as Global Security Exchange (GSX); Associate Protection Professional (APP) certification launched

'20

2020 Installed Global Board of Directors in transition to new global governance structure

'21

Appendix C

REFERENCES

ACFE (2020). Fraud in the wake of COVID-19: Benchmarking Report, Association of Certified Fraud Examiners, December 2020, Austin, TX

American National Standards Institute and ASIS International (2013). Chief Security Officer – An organizational model, ANSI/ASIS CSO.1-2013, National Standard, 8 Nov 2013, Alexandria, VA

American Society for Industrial Security (2000). Proceedings of the Academic/Practitioner Symposium held at The University of Oklahoma, Norman, OK, May 24-26, 2000
Aon (2019). "Global Risk Management Survey 2019," Aon Centre of Innovation and Analytics, London, UK

ASIS Foundation, et. al. (2005). Scope and emerging trends, ASIS Foundation, Alexandria, VA
ASIS International (2019). Enterprise Security Risk Management Guideline, ASIS-ESRM-2019, Alexandria, VA

Bamfield, Joshua (2006). Chapter 1, "Management," in Handbook of security, Palgrave MacMillan, New York, NY

Beaudry, Mark (2017). Chapter 7, "Security education and research," in Security in 2025, edited by Lawrence Fennelly, et. al., ASIS International, Alexandria, VA

BizVibe (2021). "What is the current state of the global security market?," https://blog.bizvibe.com/blog/top-security-companies, Toronto, ON, Canada, accessed 31 May 2021

Campbell, George (2018). " A Guide for Building Your Corporate Security Metrics Program," Security Executive Council

Chaiyabhat, Whit (2020). Interview by Laneisha Hayes, virtual, 4 September 2020

Coppoolse, Miranda (2021). personal electronic communication with the author, 14 April 2021

Crysler, Justin (2020). "Maintaining relevance in the next industrial revolution: what Chief Security Officers must do to co-exist with artificial intelligence and not be replaced by it," graduate research project, Webster University, St. Louis, MO, December 20, 2020,

Fagel, Michael (2021). personal electronic communication with the author, 9 April 2021

Fennelly, Lawrence, Beaudry, Mark and Perry, Marianna, eds. (2017), Security in 2025, ASIS International, Alexandria, VA

Gill, Martin, ed. (2006). Handbook of security, Palgrave MacMillan, New York, NY

Gips, Michael and Cook, A. J. (2020). The rising profile of the corporate security executive, Legal Executive Institute, July 24, 2020, https://www.thomsonreuters.com/en-_us/posts/corporates/corporate-security-executive

Gips, Michael (2021). "Checking in on the progress of ESRM," International Security Journal, March 9, 2021

Grand View Research (2021). "Security Market Size, Share & Trends Analysis Report," https://www.grandviewresearch.com/industry-analysis/security-market, San Francisco, CA, accessed 31 May 2021

Griffin, Joel (2021). "Corporate risk strategies shift as civil unrest rises," Security Infowatch, June 4, 2021, https://www.securityinfowatch.com/security-executives/article/21225521/corporate-risk-strategies-shift-as-civil-unrest-rises

Griffiths, Mel, Brooks, David and Corkill, Jeffrey (2010). "Defining the security professional: Definition through a body of knowledge," 3rd Australian Security and Intelligence Conference, 30 November 2010, Edith Cowan University, Perth, Western Australia

Hayes, Laneisha, CPP (2020). personal electronic communication with the author, 1 September, 2020

Hendricks, Wayne (2020). In "ISMA - Chief Security Officers Enable Business," (video), International Security Management Association, https://vimeo.com/434397508

Hough, Mary (2021). LinkedIn post, untitled, https://www.linkedin.com/posts/mary-hough-cpp-3b707a7_this-is-so-true-i-dont-understand-why-activity-6815289090976608256-U1uQ (accessed 25 June 2021)

Hribernik, Miha and Haynes, Sam (2020). "47 countries witness surge in civil unrest – trend to continue in 2020," Political Risk Outlook 2020, Verisk Maplecroft, 16 January 2020, Bath, United Kingdom

Jibilian, Isabella and Canales, Katie (2021). "The US is readying sanctions against Russia over the SolarWinds cyber attack," Business Insider, Apr 15, 2021

Johnston, Roger (2016). "Some unconventional security metrics," Asia Pacific Security Magazine, November 16, 2016

Kingston, Jennifer (2020). "Exclusive: $1 billion-plus riot damage is most expensive in insurance history," Axios, September 16, 2020, https://www.axios.com/riots-cost-property-damage-276c9bcc-a455-4067-b06a-66f9db4cea9c.html

Lasky, Steve (2020). "A GSX Q&A: 2020 may prove to be the security industry's defining moment," Security InfoWatch, September 24, 2020

Lee, Elsa (2015). Homeland Security and Private Sector Businesses, 2nd Edition, CRC Press, Boca Raton, FL

Mahoney, Santanya and Peterson, Kevin (2016). Perspectives on the historical foundations of risk management, manuscript, July 2016

Marquez-Tejon, Jose, et. al. (2021). "Security as a key contributor to organisational resilience: a bibliometric analysis of enterprise security risk management," Security Journal, 20 March 2021

Martinez, Liz (2017). Chapter 1, "History of women in security," in Women in the security profession, edited by Sandi Davies, Elsevier Butterworth-Heinemann, Kidlington, Oxford, UK

McCrie, Robert (2016). Security Operations Management, 3rd Edition, Elsevier Butterworth-

Heinemann, Kidlington, Oxford, UK

Meyer, Claire (2021). "Accelerating change: an interview with John Petruzzi, Jr., CPP," Security Management, 1 January, 2021

Michelman, Bonnie (2020). Interview by Laneisha Hayes, virtual, 7 August, 2020

Michelman, Bonnie (2017). Chapter 2, "Managing and escaping stereotypes and obstacles," in Women in the security profession, edited by Sandi Davies, Elsevier Butterworth-Heinemann, Kidlington, Oxford, UK

Navickas, Thomas (2021). personal electronic communication with the author, 6 April 2021

OBeirne, Sarah (2020). "Security industry to reset public's perceptions of security officers," Facilities Management Journal, June 24, 2020, Kent, UK

Ohlhausen, Peter, et. al. (2014). Persuading senior management with effective, evaluated security metrics, ASIS Foundation, Alexandria, VA

Padilla-Pagan Payano, Michael (2021). Electronic discussion with the author, April 3, 2021

Padilla-Pagan Payano, Michael (2021). LinkedIn post, May 20, 2021

Petri, Axel (2020). Interview by Laneisha Hayes, virtual, 28 August 2020

Pierini, Shirley (2017). Preface, in Women in the security profession, edited by Sandi Davies, Elsevier Butterworth-Heinemann, Kidlington, Oxford, UK

Purpura, Philip (2018). Security and Loss Prevention: An Introduction, 7th Edition, Elsevier Butterworth-Heinemann, Kidlington, Oxford, UK

Reece, Paul (2021). personal electronic communication with the author, 30 April 2021

Roberto, Michael (2009). The Art of Critical Decision Making – Course Guidebook, The Teaching Company, Chantilly, VA

Sawant, Mangesh (2021). "The chief security strategist in an age of uncertainty," Security Management, 17 February 2021, Alexandria, VA

Statista (2021). "Security services market size worldwide by region 2011-2020," https://www.statista.com/statistics/323113/distribution-of-the-security-services-market-worldwide, Hamburg, Germany, accessed 31 May 2021

Strom, Kevin, et. al. (2010). The private security industry: A review of the definitions, available data sources, and paths moving forward, RTI International, Research Triangle Park, NC

Stupp, Catherine and Rundle, James (2020). "Pandemic elevates security chiefs to corporate leadership roles," interview, https://www.wsj.com/articles/pandemic-elevates-security-chiefs-to-corporate-leadership-roles-11596706200

Swanson, Charles (2021). Professional security management: A strategic guide, Routledge, Abingdon, Oxon UK

Tal, Jonathan (2020). "Security stacking: how to address the challenges it is creating," Security, October 26, 2020, https://www.securitymagazine.com/articles/93398-security-stacking-how-to-address-the-challenges-it-is-creating?

Taylor, Rod (2013). "Understanding Metrics: How metrics will improve your physical security program," graduate project, Webster University, St. Louis, MO

TigerRisk Partners (2021). 2020 Catastrophe Snapshot, white paper by TigerRisk Partners, January 2021, Stamford, CT
University of Phoenix (2014). Security industry survey of risks and professional competencies, published by the ASIS Foundation, Alexandria, VA

Wolf, Torsten (2020). "Lock down your internal controls: ACFE survey identifies corruptions as another symptom of Covid-19," LinkedIn article, Nov 13, 2020

Woods, Andrew (2017). Chapter 11, "Opportunities and obstacles for women in security," in Women in the security profession, edited by Sandi Davies, Elsevier Butterworth-Heinemann, Kidlington, Oxford, UK

Appendix D

THOUGHT LEADER BIOGRAPHIC SKETCHES

Howard Belfor, CPP
Howard is President of Belfor & Associates, LLC a consultancy specializing in serving the security industry, providing services to commercial, industrial, and government clients and security product and service companies. He is a former member of the Board of Directors (2017-2019) at ASIS International, Council Vice President, and former Chair of the Physical Security Council. A frequent speaker at seminars and education sessions on topics associated with security controls and their application, Howard is also an ASIS faculty member and a subject matter expert in the areas of access controls, intrusion detection, surveillance, security management systems, and auditing. He has been a contributor to Protection of Assets, and was a Lead Contributing Author for "Physical Security Principles" (ASIS International, 2015). Howard has been an ASIS Member since May 1981.

Earl Biggett, CPP
Earl Biggett is a native New Yorker who divides his time between Louisville, Kentucky and Orlando, Florida. Earl is the Senior Director of Security for Churchill Downs Racetrack, LLC. Churchill Downs Racetrack is the Home of the Kentucky Derby and this event is the Most Exciting Two Minutes in Sports. Prior to this position, Earl served as the Assistant Security Manager for Orlando Venues, City of Orlando Florida (Amway Center, Camping World Stadium, and Mennello Museum of American Art). Earl has been married to his adoring wife for 33 years and has two wonderful daughters. Earl has a Master's Degree in Homeland Security Management, a Bachelor's Degree in Economics and is a Board Certification in security, Certified Protection Professional (CPP) from ASIS International. Earl has more than 25 years of service with the Federal Bureau of Investigation (FBI) and during his tenure, he held executive and managerial positions and conducted investigations related to Terrorism, White Collar Crime, Civil Rights, Public Corruption, Internal Affairs, and Employee Assistance Programs. In Earl's free time, he is a community volunteer, accomplished golfer, and movie enthusiast.

Inge Sebyan Black, CPP, CFE, CEM
Inge has been in Corporate Security Management and Investigations for 43 years, working in the areas of loss prevention, workplace violence, emergency management, investigations, fraud, and information security. Inge has held private investigation licenses in the US, Ontario, and Quebec. She has worked in both the US and Canada, specializing in security risk assessments, workplace violence assessments, and security audits. Inge is a published author on topics including investigations, interviewing, and other security subjects since 1995; most recently authoring the book Investigations and the Art of the Interview, 4th ed. She has been a frequent presenter at ASIS International conferences and trainings along with speaking at ACFE meetings.

She joined ASIS in 1983 and has since been an active member of the Physical Security Council, Women in Security, Vice-Chair of the Investigations Council and Chair of the Crime Prevention & Loss Prevention Council for ASIS.

Since 2018, Inge has served as CVP (Council Vice President) for ASIS International. Currently Inge is working as a Senior Information Security Consultant for a fortune 50 company.
Inge was awarded the Karen Marquez Award in 2014 for her lifetime contribution to Physical Security, an honor granted to an outstanding woman in security each year.

Whit Chaiyabhat, CPP, MBCI, CBCP, CEM
Whit is a senior leader with over 20 years in global security, safety, crisis/continuity management, intelligence analysis, behavioral/insider threat assessment and national security programs. He created and led programs for various organizations, industries and risk cultures including Fortune 500 corporations, U.S. government and intelligence agencies, small and large campuses (100 - 2,000 acres), 24/7 global operation centers (FBI) and highly secure locations (U.S. national security sites and military bases). A team-oriented leader recognized by DHS/FEMA, ASIS International, IAEM, Campus Safety Magazine and Security Director News, including being named to America's "Top 20 Under 40" by Security Director News (2012) and ASIS Phoenix Chapter's Security Professional of the Year (2015). National security roles include service as an FBI Security Specialist and Emergency Preparedness Coordinator, unique FBI crisis management roles, national security contingency planning projects at the U.S. National Counterterrorism Center (NCTC) and Department of Defense industrial security (NISP) programs***. FBI Protective Intelligence Threat Assessment (PITA) Program Manager. Whit worked with various FBI, intelligence and law enforcement partners regarding assessment of targeted threats to the*** U.S. Attorney General, FBI Director, their Deputies and families. He also served in various national security consulting roles with Booz|Allen|Hamilton, SAIC National Security Division and Eagle Security Group in Washington D.C. His private sector experiences include serving internationally recognized organizations in VP, Director and Manager positions with Raytheon, Washington National Cathedral, Georgetown University, FM Global and Takeda.

Kathy Macdonald, M.O.M, CPP
Kathy Macdonald is a former police officer with almost three decades of investigative and crime prevention experience. She regularly delivers keynote presentations at conferences on the topics of online fraud, Internet safety, and social engineering. Kathy instructs online through the University of Calgary, Faculty of Continuing Education, on subjects including Crime in the Workplace, Cybercrime Prevention and Personnel Security. Kathy's new book, Cybercrime: Awareness, Prevention, and Response, is the first comprehensive Canadian resource talking about how cybercrime affects individuals, businesses, governments, institutions, and organizations.

Kathy holds a Master of Science in Security and Risk Management, and is a Certified Protection Professional (CPP). In 2009, the Governor General of Canada invested Kathy with the Member of the Order of Merit of the Police Forces, M.O.M., in recognition of her commitment to cybercrime prevention. Kathy volunteers on the board of the Women CyberSecurity Society Inc. and she was named to the Top 20 Women in Cyber Security in Canada for 2020.

Bonnie Michelman, CPP, CHPA
Bonnie Michelman has extensive leadership and security management experience in diverse industries and is reputed to be a strong security expert nationally. She currently is the Executive Director of Police, Security and Outside Services at Massachusetts General Hospital and the Security Consultant for its parent corporation, Mass General Brigham, an organization comprising 17 hospitals, hundreds of offsite facilities, and a workforce over 100,000. She oversees a licensed Police Department in this role among other departments. She was formerly a senior executive at First Security Services Corporation (now Securitas) overseeing Security for 60 diverse operations and Assistant Vice President for General Services/Operations at Newton Wellesley Hospital managing 16 operational and support departments.

Bonnie is on the Board of Directors and Past President for the International Security Management Association (ISMA). Bonnie served as President in 2001 of ASIS-International, a 40,000-person organization, Chairman of the Board in 2002, and Foundation President from 2003-2005. She is Past President (2008 and 1995) as well as Chairman of the Board of the International Association for Healthcare Security and Safety (IAHSS). She has also been an Instructor at Northeastern University, College of Criminal Justice in the Graduate and Undergraduate program for over 25 years. Bonnie is on the Regional Board of Directors for the Anti-Defamation League (ADL) and chairs their National Security Committee.
Under Bonnie's direction, MGH won the Lindberg Bell Award for the nation's finest healthcare security program in 1999, 2007, and 2018 among numerous other awards and recognitions. She was appointed in 2010 by DHS Secretary Janet Napolitano to the Homeland Security Advisory Council (HSAC), holding that position until 2015 and chaired the DHS Faith Based Security Advisory Committee.

Bonnie also lectures and consults on areas of healthcare security, workplace violence, hate crimes, active shooter training, domestic violence, risk assessment/management, disaster planning, leadership, change management, strategic business planning and communications. She has many publications in various journals on safety, security, leadership, and management. She also does significant work in Executive Coaching, Management Engineering and Strategic Planning as well as conducting ESRM assessments and expert witness work for the past 25+ years.

Bonnie has an MBA, and MS in Criminal Justice and a BA in Government and Sociology. She holds her CPP and CHPA certifications, and was selected as an "IFSEC Global Influencer" in 2018 in the security executive category.

Axel Petri
Axel Petri, a German qualified lawyer, is Senior Vice President, Group Security Governance at Deutsche Telekom AG. As Group Security Coordinator he is responsible for assuring the holistic and groupwide security approach. This contains strategy, regulations, and control in all security domains as well as steering the groupwide cooperation of all security departments. He is also in charge of Information Protection and Economic Security as well as Investigations and Prevention. As Security Commissioner he is responsible for the fulfilment of the legal obligations in the field of Public Safety including strategy and steering of Lawful Interception and Data Provision in Germany.

Axel is co-author of the Rechts-Handbuch zum E-Commerce (Legal Compendium on E-Commerce) and author of further publications regarding Internet/Media Law as well as Security. As an educator, he is a visiting lecturer at the University of Applied Sciences 'Rheinische' Cologne. Axel is also the Past President of the Advisory Council at ASIS's CSO Center for Leadership & Development, and also serves on boards and committees in different associations including BDI and BITKOM. In addition, he was selected as an "IFSEC Global Influencer" in 2018 for the security management category.

Dave Tyson, CPP, CISSP
Tyson is the President of Apollo Information Systems, a Cyber Security consultancy and technology services firm. He is also the co-founder of Cyber Easy Learning, Cyber Security training program that teaches Cyber Security in plain English!

His previous roles include CISO for SC Johnson, PG&E, Nike, the Global Security operations lead for eBay, and the Chief Security Officer for the Host City of the 2010 Winter Olympics.
Mr. Tyson holds a Master's Degree in Business Administration specializing in Digital Technology Management. He is also a CPP - Board Certified in Security Management, and holds the CISSP certification.

Dave currently serves as a member of the Board at the GSRMA (Global Security Risk Management Alliance) and is Co-chair for the Strategic Council, the national Cyber Security Initiative, for the Private Director's Association. Dave is a Past Chairman of the Board and 2015 President of ASIS International.

Tim Wenzel, CPP
Tim Wenzel, Head of Global Security Privacy Protection at Facebook, is an emerging thought leader in the security industry. Tim has a passion to help transform the existing paradigms of leadership, risk management, and creating organizational value through well designed security programs.

Tim is noted in business and the industry for his problem-solving skills, which stem from his background in healthcare. By properly identifying the root causes of risk, Tim and his teams have created a bridge between opportunity and risk for the business and security.

Caroline Wong
Caroline Wong is the Chief Strategy Officer at Cobalt.io. Wong's close and practical information security knowledge stems from broad experience as a Cigital consultant, a Symantec product manager and day-to-day leadership roles at eBay and Zynga. She teaches cybersecurity courses on LinkedIn Learning and is a member of the Forbes Technology Council. Wong was named 2019 Cyber Educator of the Year in the 6th Annual Cyberjutsu Awards. She authored the popular textbook Security Metrics: A Beginner's Guide, published by McGraw-Hill. Wong graduated from U.C. Berkeley with a BS in electrical engineering and computer sciences and holds a certificate in finance and accounting from Stanford University Graduate School of Business.
Her primary areas of specialization include security metrics, security management, application security, and cybersecurity education.

Appendix E

COUNTRIES REPRESENTED IN THE SURVEY OF SECURITY EXECUTIVES

The following list identifies countries by geographic region from which individuals responded to our survey (see Figure 3). There are a total of 73 countries represented.

North America (6)
Bahamas
Canada
Dominican Republic
Jamaica
Mexico
USA

Latin America (15)
Argentina
Brazil
Chile
Columbia
Costa Rica
Ecuador
El Salvador
Guatemala
Honduras
Nicaragua
Panama
Paraguay
Peru
Uruguay
Venezuela

Europe (20)
Belgium
Bulgaria
Czech Republic
Finland
France
Germany
Greece
Ireland
Italy
Lithuania
Malta
The Netherlands
Norway
Poland
Romania
Spain
Sweden
Switzerland
Ukraine
United Kingdom

Asia & Oceania (13)
Australia
Bangladesh
Cyprus
Hong Kong
India
Indonesia
Malaysia
New Zealand
The Philippines
Pakistan
Singapore
Thailand
Viet Nam

Sub-Saharan Africa (7)
Ghana
Kenya
Mauritius
Mozambique
Nigeria
South Africa
Tanzania

Middle East & North Africa (12)
Algeria
Bahrain
Egypt
Iraq
Israel
Jordan
Kuwait
Morocco
Qatar
Saudi Arabia
Turkey
United Arab Emirates

Appendix F

PROJECT PARTICIPANTS

Principal Investigators
Kevin E. Peterson, CPP, CIPM II
Innovative Protection Solutions, LLC
Herndon, VA USA

Joe Roberts, PhD
Business QnA
St. Louis, MO USA

Research Associates
Laneisha C. Hayes, CPP
Palm Bay, FL USA

Miranda Coppoolse, CFIP
MC Global Security Consulting
Amsterdam, The Netherlands

Myrah Kirkwood, CPP, CFE
Lake Forest, CA USA

Research Assistants
Zena M. Culp, PMP
Woodbridge, VA USA

Timothy C. Glass
Phalanx Protection Solutions
Atlanta, GA USA

Data Analysis and Visualization
Reuel Sample
Knoxville, TN USA

Kristin Thompson
Belleville, IL USA

Megan Roberts
St. Louis, MO USA

We also express our sincere gratitude and appreciation to our Research Advisory Panel which was comprised of:

Mark H. Beaudry, PhD, CPP
North Billerica, MA USA

Michael J. Fagel, PhD, CEM
Sugar Grove, IL USA

Thomas E. Navickas, PhD, CPA
Austin, TX USA

About the ASIS Foundation The ASIS Foundation, a 501(c)(3) nonprofit affiliate of ASIS International, supports global security professionals through research and education. The Foundation commissions actionable research to advance the security profession. It awards scholarships to help chapters and individuals—including those transitioning to careers in security management—achieve their professional and academic goals. Governed by a Board of Trustees, the Foundation is supported by generous donations from individuals, organizations, and ASIS chapters and communities worldwide. To learn more or make a donation, visit www.asisfoundation.org.