Key Findings from

THE STATE OF SECURITY MANAGEMENT

A Baseline Phenomenological and Empirical Study

Funded by

ASIS FOUNDATION™

MODULE 1:

Overview and Recommendations

This project provides a snapshot in time. It explores a field that is global in scope and affects peoples' lives, commerce, and governance daily. The target year for the study, 2020, included global upheaval on several fronts, from pandemic and civil unrest to natural disasters and supply chain disruptions. The year saw major changes in the practice and perception of security, security management, and risk management that will have lasting impact.

RESEARCH APPROACH

This global study views security management through the lens of a senior security executive or chief security officer in a public- or private-sector organization of any size or type. It treats security management as both a field and a profession and distinguishes it from a security discipline, such as physical security, information security, cybersecurity, or personnel security.

Researchers conducted an online survey of mid-level to senior security executives and professionals and excluded security service or product providers, vendors, and integrators. Demographic questions collected data on industry sector, reporting level, geographic region, ASIS member status, and gender. Substantive questions asked about the challenges faced by security executives, skills they seek, management tools they use, whom they collaborate with, and their views on enterprise security risk management (ESRM). The survey, offered in English and Spanish, generated 545 responses.

Researchers also interviewed 10 thought leaders in the profession, conducted a literature search, and made a special effort throughout to seek definitions for the term *security management*.

The research team had hoped to minimize discussion of the COVID-19 pandemic—to gather data based on as normal a condition as possible—but quickly learned that the pandemic and other world events were already reshaping some aspects of security management perception and practice during the research process.

FINDINGS

The data showed that the current state of security management is secure and positive, yet some concerns and challenges exist in the profession. The researchers made these eight key findings:

1. People matter (and by nature security management is a people function as well as a business function).

2. Security executives and management

professionals must embrace change.

3. The security management field lacks a clear definition.

4. Parochialism in the security management field is a challenge.

5. Enterprise security risk management (ESRM) is catching on and considered viable.

6. Security professionals need to broaden their perspectives on global threats.

7. The security profession's brand and reputation must be enhanced.

8. Security management metrics are an increasingly essential tool.

The study also developed several noteworthy themes (which are important but less significant than the findings). These themes provide a deeper understanding of security management as a profession and some of the issues that influence the perception and practices of the field. They are as follows:

- The profession's gender gap.

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

- The common practice of hiring former military or law enforcement members into senior corporate security positions.
- The trend toward security services providers diversifying their market as well as their service offerings to remain relevant and efficient in their business models.
- The divergence between the views of English-speaking and Spanish-speaking survey participants.

IMPLICATIONS OF THIS RESEARCH

The findings and noteworthy themes led researchers to make 14 recommendations, which are meant to be actionable steps for security professionals, employers, academics/researchers, C-suite executives, and relevant professional associations.

Following are some ways to translate the study findings into tangible benefits to enhance organizational safety and security. The recommendations are clustered in three groups: definitions, education and certification, and brand and reputation.

DEFINITIONS

One hindrance to the advancement of security management is the lack of consensus on definitions of key terms, such as *information security* and *security management*. A proposed definition of the latter combines the two most widely accepted answers in this project's survey and also the definition in *The Handbook of Security* (Gill, Ed., 2014): "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 1: After a consensus definition of *security management* is reached, it should be added to the ASIS Glossary of Security Terms and be incorporated into ASIS International educational and marketing materials. In this way it will seamlessly become a part of the security body of knowledge.

Recommendation 2: ASIS should initiate an effort to conduct round-table discussions on a common lexicon with professional associations in allied fields, such as Information Systems Audit and Control Association (ISACA), (ISC)2, International Security Management Association (ISMA), International Association of Privacy Professionals (IAPP), Society of Human Resource Professionals (SHRM), Association of Certified Fraud Examiners (ACFE), and International Association of Emergency Managers (IAEM). The effort could also include academic institutions offering graduate programs in security management and related fields.

EDUCATION AND CERTIFICATION

The study found a need to improve the image of the profession, increase the credibility of security professionals, and enhance their ability to influence decision makers. Education and certification programs will aid in meeting those objectives.

Recommendation 3: 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.

Recommendation 4: Further efforts should be made to encourage institutions to improve crossflow among security management, homeland security, cybersecurity,

emergency management, intelligence, and business courses. Approaching the issue from an ESRM perspective will help facilitate mutual respect and understanding among the various academic communities.

The Wharton School at the University of Pennsylvania has collaborated with ASIS International since 2004 on the Program for Security Executives. This five-day intensive course caters to senior security executives and chief security officers seeking greater exposure to business and management perspectives.

Recommendation 5: New programs with objectives similar to those of the Wharton Program should be developed. Ideally, several 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.

Online and informal learning platforms provide lessons globally and in many languages. Some offer full university courses that can be taken on a credit or noncredit basis under different pricing models.

Recommendation 6: Security professionals should explore new venues for learning, such as LinkedIn Learning, Udemy, or Coursera, and develop more educational content for such platforms. A course on security management would be extremely valuable.

BRAND AND REPUTATION

Individuals, organizations, and professions carry with them a brand (something they attempt to portray to others) and a reputation (the way others view them based on information or experience).

Recommendation 7: Security professionals should study ways of encouraging employers to focus on education and certification when recruiting, hiring, and advancing security professionals and to support ongoing professional development.

Recommendation 8: ASIS International should work with 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 (electronic security systems, robotics, mobile and aerial surveillance systems, etc.) programs;

SECURITY THOUGHT LEADER PERSPECTIVE:

Consistent, Holistic Risk Assessment Needed

"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 risk assessment methods and present their results in different ways? We need a holistic methodology for assessing risk using a common platform that depicts risks across domains and functions. Security professionals can be viewed as trusted risk advisors by coordinating with other disciplines to develop a shared risk picture in a manner and design preferred by executive stakeholders."

–Whit Chaiyabhat, CPP, MBCI, CBCP, CEM

and security systems installation, design, and development programs. Successful graduates would raise the professionalism of their career field and the perception and brand of the security field as a whole.

One issue hampering the profession's image is the lack of a unified risk assessment approach in most organizations.

Recommendation 9: Security professionals should work with professionals from other staff functions to develop consistent risk assessment and display protocols so senior decision makers are presented with a holistic view of the risks they face.

Recommendation 10: Security professionals should 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 prime sources of risk.

Recommendation 11: Security professionals should encourage appropriate use of data analytics and decision making technologies as tools in strategic planning. At the same time they should strive for continual improvement in developing and applying metrics for security management.

The following recommendations are meant to enhance the brand and reputation of the profession through better recruiting and onboarding of mid- and senior-level security executives and staff.

Recommendation 12: Job descriptions for security positions should accurately describe the roles and responsibilities envisioned by the sentior executives. For example, does the position involve strategy development, strategy implementation, strategy monitoring, or some combination of those? They are distinct functions, and the candidate and hiring organization should be aligned in their understanding of the role. Job descriptions should also be clear about whether the position involves cybersecurity responsibility and, if so, the nature and extent of those responsibilities. Misunderstandings over such issues may lead to a poor fit between the security professional and the position being filled. A poor fit degrades the quality of security management for the organization and may harm the image of security and the individual.

Marketing and collaboration across the security field can bring further respect to the security management profession, enabling security professionals to be more effective organizational partners and advisors.

Recommendation 13: A deliberate, aggressive marketing and branding strategy should be orchestrated for the security management profession. This project should involve marketing experts and security professionals around the globe, and campaigns should be tailored to different cultures and languages. This effort would focus less on marketing security associations and more on marketing the profession as a whole.

Recommendation 14: ASIS should work with other associations to make the security profession more collaborative, holistic, and oriented toward ESRM. Associations' educational programs, materials, publications, and communications should avoid terminology conflicts and help the profession's elements stop operating in silos. The profession can improve its image and reduce negative perceptions by presenting a united and responsible story to the C-suite, stakeholders, and the general public.

ADDITIONAL USES OF THE STUDY

This project may also be used for other purposes, such as:

- Developing position descriptions for security professionals and practitioners.
- Developing and updating educational programs and curricula related to security management and functions.
- Defining skill sets and training necessary to implement security programs.
- Defining interrelationships among organizational functions or departments.
- Identifying distinctions in security practice between the public and private sectors and among various industry sectors to benefit professionals transitioning from one sector to another and to improve relationships among sectors with respect to security management.
- Planning for security program development and strategy relative to strategic plans of the organization.
- Conducting trend analysis and metric development (and refinement) for security management.
- Facilitating conversation among security professionals operating in different industry sectors, disciplines, and global settings.

The first in a series of nine modules, this paper explores the findings of an ASIS Foundation study conducted by Kevin E. Peterson, CPP, CIPM II and Joe Roberts, Ph.D. in 2020 and 2021. To download the full ***State of Security Management*** report, visit *asisfoundation.org*.

The ASIS Foundation, an affiliate of ASIS International, helps security professionals achieve their career goals with certification scholarships, practical research, member hardship grants, and more. The Foundation is supported by generous donations from ASIS members, chapters, and organizations. Online at *www.asisfoundation.org*.