Security Industry Career Pathways Guide

PRACTITIONERS AND SUPPLIERS

Prepared by:

McKinley Advisors

ASIS INTERNATIONAL
Advancing Security Worldwide®

SIA
SECURITY INDUSTRY ASSOCIATION

Security Industry Career Pathways Guide

Practitioners and Suppliers

Prepared by: McKinley Advisors

Table of Contents

Overview and Methodology

ASIS International (ASIS) and the Security Industry Association (SIA) retained McKinley Advisors (McKinley) to conduct research to understand the career pathway of security management and supplier personnel, including their educational and professional backgrounds, job titles and responsibilities, required knowledge, skills, and abilities. The goal of the research is to develop an illustration that provides insight into the common ways in which professionals enter and advance through the security field and describe the level of preparation and experience that best ensures their success. McKinley Advisors (McKinley) supported this effort with an extensive and in-depth project that included the following key phases:

- **Engagement of Task Force:** As a first step in the project, McKinley convened a Task Force of representatives from ASIS and SIA to review its work. The Task Force served as critical in validating our work through the project, providing advice, counsel, and review as the project phases advanced. ASIS and SIA thank the Task Force members for the hard work and dedication to this project.

  Ms. Kathy Lavinder
  Security & Investigative Placement
  Bethesda, MD

  Mr. Donald E. Knox, CPP
  Sears Holdings Management Corporation
  Peoria, IL USA

  Mr. Bernard D. Greenawalt, CPP
  Securitas Security Svcs USA
  Chicago, IL USA

  Mr. Michael Brzozowski, CPP, PSP
  Symcor
  Toronto, ON CANADA

  Mr. Michael S. D'Angelo, CPP
  Secure Direction Consulting LLC
  Miami, FL USA

  Mr. Malcolm C. Smith, CPP
  Qatar Museums Authority
  Doha, QATAR

  Ms. Angela J. Osborne, PCI
  Guidepost Solutions
  Decatur, IL USA

  Mr. Edward J. Batchelor, PSP
  Guidepost Solutions
  Chicago, IL USA

  Mr. Scott Dunn
  AXIS Communications
  Chelmsford, MA USA

  Mr. Martin Huddart
  ASSA ABLOY
  New Haven, CT USA

  Mr. Phil Aronson
  Aronson Security Group (ASG)
  Renton, WA USA

- **Literature Review:** McKinley next conducted a literature review of industry sources that included industry white papers, career websites, government sources, and other publications.

The literature review created a basis for identifying the elements to be tested and validated through an electronic survey (e.g., "*what types of fields do security management personnel come from?*" "*what kinds of traits do security industry suppliers need to perform their job functions successfully?*"). An important publication, the Enterprise Security Competency Model,[1] provided a conceptual framework for the project. Many of the concepts tested through the survey research were gathered through the document.

- **Telephone Interviews:** After completing the literature review, McKinley conducted telephone interviews with professionals in the security industry that included human resources staff, security managers, and executives. The interviews were a validation step to confirm the initial literature review phase of work as well as built on the concepts to be measured through the electronic survey.

- **Electronic Survey:** Finally, after gathering multiple sources of background data, McKinley developed a survey to administer to ASIS International and SIA members. The survey was reviewed by the project Task Force, and included questions relating to security professionals' background, experience, and skills.

The following report summarizes the findings from the survey and presents a graphic, or illustration, of the typical characteristics and career pathway for security professionals. The data presented has been analyzed in full according to the employer category (practitioner, supplier) and level of responsibility (professional, management/director, executive).

Demographics and Taxonomy

The electronic survey was deployed on December 12, 2017 and remained open through February 12, 2018. Survey respondents represented multiple geographic regions, with the bulk indicating primary residence in the United States (57%) and Canada (11%) followed by the regions of Europe (14%), Asia (5%), Latin America and Caribbean (5%), Africa (4%), Oceania (3%), and the Middle East (1%). The survey instrument was distributed to a total of 33,761 valid email addresses and was completed or partially completed by 2,435 individuals for an overall response rate of 7%.

Overall Response Rate	7%
Total Responses	2,435
Complete Responses	1,105
Partial Responses	1,272
Valid Email Addresses	33,761

[1] The Enterprise Security Competency Model was published in 2015 by ASIS Foundation and provides a thorough review of the professional skills and competencies needed in the security industry.

For the purposes of categorization and analysis, survey respondents were asked to self-classify their level of responsibility (professional, management/director, or executive)[2] as well as to identify their employer type according to the taxonomy below:

Employer	Aggregated and listed in report as:
End-user/practitioner of security services	Practitioner
Provider of security or protection services	
Distributor of security products	Supplier
Engineering or design consultant	
Integrator of security products	
Manufacturer of security products	
Law enforcement	Other
Instructor, faculty or academician	
Security or risk management consultant	

The level of responsibility and employer-type taxonomy are central to the information included in the report. Respondents were classified into peer segments, or groups, based on this classification scheme. Each group (e.g., executive level suppliers, management/director level suppliers, professional level suppliers) is constructed of professionals that may represent a variety of backgrounds (e.g., manufacturers, integrators) but are considered homogenous in the general nature of their work when compared to other professionals in the security field. Still, important differences may exist within these groups. For example, sales and business development responsibilities may be very common among "practitioner" professionals working in businesses that supply security services, yet almost unheard of for staff in end-user/client organizations. For this reason, a granular breakdown of survey responses is provided in the appendix of this report and provides an additional layer of detail to the data. In addition, supplier employer types may vary even more than the survey categorizations. While this report looks at job titles and trends among suppliers in aggregate, the varied company types can impact the work and focus professionals are required to have in a given company. Additional supplier employer categories may also include: access control product manufacturer, door/lock/hardware manufacturer, intrusion product manufacturer, camera product manufacturer (hardware/software), cyber security manufacturer, logical access manufacturer, specialty product/ software manufacturer, service providers (system integrators, security alarm dealer, locksmith), distributors and wholesalers.

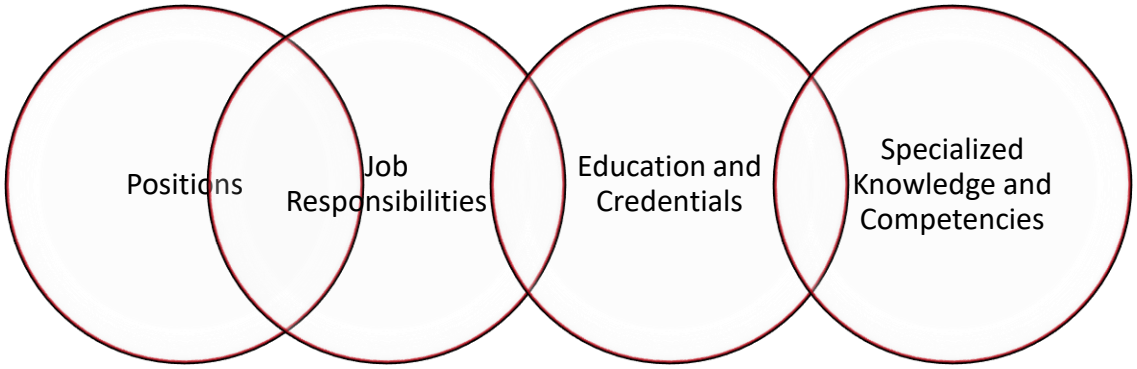
[2] Those that selected "manager" or "director" were grouped together into the "management/director" level of responsibility referenced throughout the report. This level of responsibility reflects a mid-point between "professionals" who are security task-focused, and executives who are focused very broadly on the strategy and operations of the organization.

Security Management Practitioners Career Pathways

Security Industry Suppliers Career Pathways

Executive Summary

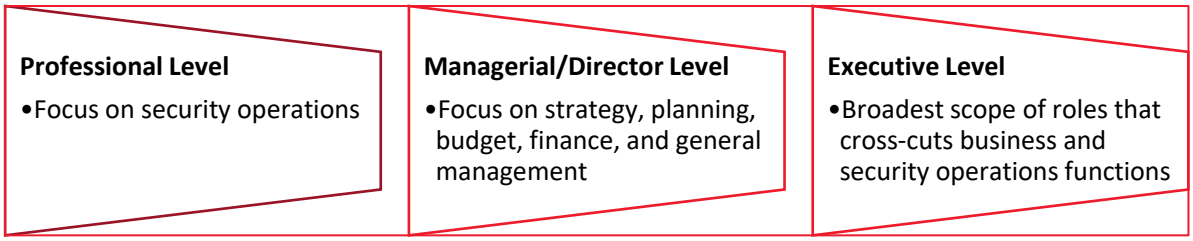
The following summary provides a brief overview of key themes uncovered through the research. It captures critical elements of the career pathways map, including:



- **Positions in Security Field: The diversity of roles in the field provides numerous ways for security professionals to identify a career pathway that fits their skills and interests. Professionals are categorized here into professional, managerial/director, or executive level positions. Each stage typically requires a general knowledge of security management coupled with specific expertise related to their role and position level.** There are many job titles and roles in the security field. They range from positions that hold a professional or technical focus to those that involve management/director or executive level responsibilities. Those with prior experience in the field tend, at the management/director level, to have at least seven-to-nine years of experience prior to taking their (current) positions. Executive level jobs may require 11 years of experience or more, on average. However, level of responsibility (professional, management/director, executive) tells only a part of the story. A security practitioner or supplier may have worked in the field for many years and gathered a very high level of expertise but chose not to pursue management/director roles in favor of a "professional level" position that requires their technical competency or expertise. In addition to the breadth of job titles and levels of responsibility, professionals in the security field may specialize in various sectors (e.g., public events, corporate security), domains (e.g., access control, investigations), or employer types (e.g., corporation, supplier of security services). It is worth noting that for suppliers, job titles can vary depending on the type of company. The supplier job titles presented in this report are primarily representative of mid to large companies based in the United States; supplier companies that are smaller in size and outside the United States may have slightly different job title structures.

- **Job Responsibilities: Security positions may involve complete enterprise-wise concern over the security function; oversight and leadership over a security department or teams; and/or responsibility for ensuring that the importance of security is communicated across the organization, with each employee being aware**

of their role in maintaining a safe and secure organization. Additionally, those on the supplier side of the security industry in particular may have responsibilities for sales and business development functions in addition to their role in providing or facilitating security. In accomplishing such a wide breadth of responsibilities, security professionals (practitioners or suppliers) may engage in a variety of specific business and operational roles, including strategy and planning, budgeting/finance, human resources, security operations and management, and many other role-specific tasks. To some degree, security professionals of all levels will have at least some responsibility in each of these areas. However, general areas of focus emerged by level for both practitioners as well as suppliers:



- **Education:** **The security field is made up of personnel with very diverse educational and professional backgrounds.** This is the result of an industry that requires a wide breadth of knowledge (e.g., current events, technology, security methodologies, cultural sensitivity, human resources, and budgeting) as well as a solid grounding in practical experience to foster good judgment and on-the-job creative problem-solving. However, certain courses of study may be helpful in preparing security professionals:
    - For practitioners, relevant academic disciplines include criminal justice, management, law, and/or social science disciplines.
    - Suppliers may also benefit from a background in these disciplines, or depending on their job responsibilities, may benefit most from a course of study in engineering or technology.

- **Credentials:** **In addition to education, there are several popular ways for security professionals to increase their expertise and credibility. Certifications and relevant credentialing opportunities may help to ensure a security professional's competency.** The most popular credentials for security management professionals include the Certified Protection Professional (CPP) and Physical Security Professional (PSP) certifications. Suppliers also commonly obtain the CPP and PSP but may also earn a project management credential (e.g., Certified Security Project Manager [CSPM], Project Management Professional [PMP]). Additionally, volunteering with an association or serving as a mentor to a less experienced professional are popular ways for security professionals to engage with the industry.

- **Career Pathway into Security Field:** **Security professionals come from all varieties of occupations. However, the most popular pathways into the security field for**

practitioners tend to be law enforcement, military service, or business. Suppliers may transition into the field through technology, manufacturing, and/or construction backgrounds, in addition to law and military. Law enforcement and military service provide an excellent primer for careers in security by offering direct experience, a vital network of connections, and expertise in working with external organizations that provide security. Similarly, business administration provides skill in navigating a corporate environment as well as experience in many of the crucial business functions performed in a security management position (planning and strategy, budgeting/finance, human resources, etc.). While law enforcement and military are the most popular previous careers overall, a background in business is particularly common among those in executive positions. Similar to practitioners, suppliers also frequently come from law enforcement, military, or business backgrounds. However, perhaps due to the technical, scientific, and engineering focus of many supplier roles, it is also very common for this group to transition to the security field through jobs in information technology, manufacturing, and architecture and construction.

- **Competencies and Specialized Knowledge:** **Security professionals require many different competencies and specialized knowledge to perform their jobs optimally. However, perhaps no knowledge is more important to security personnel of all employer types and levels of responsibility than broad-based knowledge of security fundamentals, risk management, and crisis management.** The background concepts, theories and application of these fundamental areas are critical to supplying security personnel with a knowledge base to understand the challenges faced by their organization and/or clients, and to know the methods, approaches, tools, and ways of preparing to manage and respond to threats. When it comes to professional skills, project management expertise is considered important by many security professionals and may be an area where they're most lacking in confidence and expertise.

- **Challenges:** **Security professionals may face additional challenges based on their specific role and level of responsibility.** For example, management/director level practitioners may have come from a background without wide exposure to core business functions such human resources, budgeting, and finance, but may require business acumen in their roles. Likewise, security industry suppliers at the executive level may benefit from specific knowledge and training related to their roles, such as executive management, relationship management, and even technical knowledge.

- **Domain-Specific Knowledge and Skills:** **Security professionals may have a wide-breadth of responsibilities over total enterprise risk, or, may act more as specialists within one more disciplines (e.g., access control, executive protection). Each domain may require prior experience and/or training as well as knowledge, skills, and abilities.** For example, professionals that provide executive protection may require tactical experience whereas those in security technology may need a background in computers or technology systems. However, regardless of their specific security domain(s),

all security professionals must develop an understanding of the enterprise, its assets, and the available solutions and approaches to risk or threat mitigation.

Positions in Security Field

Professionals typically work at executive, management/director, or professional levels within the field. The security field offers many unique job roles for security practitioners, suppliers, and other stations within the field. Although it is difficult to develop a precise taxonomy of job titles due to the wide variety of occupations, certain themes exist. For example, titles such as specialist, operator, and advisor are most common at the professional level. Those that have management/director responsibilities often hold manager, senior manager, director, or senior director titles. At the executive level, common titles may include c-suite positions (e.g., chief executive officer, chief security officer, president), vice president, executive director, and managing director. Each career level (professional, management/director, executive) denotes certain responsibilities:

- *Executives* are generally strategists that lead the organization through vision and broad policy decisions
- *Management/Director* occupations may be responsible for directing others' work and ensuring operations are performed at a consistent, high-level of performance.
- *Professional* level may be the broadest in the typology - it includes those who may be very highly skilled and experienced as well as entry-level professionals with comparatively junior responsibilities.

The following classification is a framework for understanding the security field. However, the level of seniority reflected in titles may vary across organizations. For instance, an advisor might hold management/director responsibilities at one company or may function more as a professional level specialist at another. This section of the report connects specific job titles to levels of responsibility based on self-reported survey data from security professionals. Oftentimes, professionals with the same job title may describe varying levels of job duties, management responsibility, and level of seniority.[3]

[3] It is interesting to note that approximately 70% -80% of all practitioners and suppliers, regardless of their level of responsibility indicated that their previous job (prior to assuming their current role) was in the security field. An additional 15% reporting holding their previous job in a related field, with about 5% coming from an unrelated field.

PRACTITIONERS

Security management practitioners that participated in the ASIS International-SIA Career Survey commonly reported titles such as security advisor, account manager, security manager, director of security, or director of public safety. However, these may be further categorized according to level of management responsibility.

Professional Level Job Titles: At the professional level, security management staff may have come into their positions at an entry-level point or may have previously had many years of experience in security management. Common overarching (broad/generic) titles include officer, specialist, advisor, coordinator, and analyst. A sampling of job specific titles includes:

- Corporate Security Advisor
- Corporate Security Analyst
- Facility Security Advisor
- Private Investigator
- Project Manager
- Protective Security Advisor
- Security Advisor
- Security Coordinator
- Security Officer
- Security Operations Assistant
- Security Specialist
- Supervisor

Management/Director Level Job Titles: According to results from the ASIS International-SIA Career Survey, approximately 85% of those with prior experience in the field have had at least nine years of experience in security management prior to assuming their current role at the management/director level[4]. Common generic titles at this level include manager, director, and general manager. A sampling of specific titles includes:

- Account Manager
- Assistant Director of Security
- Associate Director of Security
- Branch Manager
- Business Development Manager
- Client Services Manager
- Corporate Security Manager
- Director of Global Security
- Director of Loss Prevention
- Director of Security
- General Manager
- Manager of Security
- Regional Security Manager
- Security Manager
- Senior Security Director

Executive Job Titles: Those at the executive level tend to have the greatest amount of experience. Nearly 85% of executives with prior experience in security have had at least 11 years of experience in the field prior to assuming their current role. Common titles at the executive level include c-suite titles (e.g., CEO, CSO), executive director, and vice president. A sampling of titles includes:

- Chief Executive Officer
- Chief Operating Officer
- Chief Security Officer
- Executive Vice President
- Head of Global Security Services
- President

[4] Note that even within the "Management level" positions may vary according to seniority. A Security Manager may hold less responsibility than a Director of Security, and thus require fewer years of industry experience.

Although seniority level may differ across companies, respondents participating in the ASIS International Career Survey provided information regarding a typical career progression as a security management practitioner, illustrated below:

Typical Practitioner Career Progression

SUPPLIERS

Compared to practitioners, suppliers in security management tend to hold technical focused titles, such as technician or engineer. However, suppliers also utilize a similar framework in terms of level of responsibility (i.e., manager, director, c-suite).

Professional Level Job Titles: The most common professional level titles for suppliers tend to be account-management focused (e.g., consultant) or technical (e.g., engineer). Similar to practitioners, these professionals may be entry-level in nature or very experienced with advanced technical skill sets. Because of this, professional level security management suppliers may have no prior experience or very long tenure in the field. A sampling of specific titles among this group includes:

- Electronic Security Systems Technician
- Programmer
- Sales Engineer
- Account/ Sales Associate
- Security Consultant
- Security Project Engineer
- Systems Engineer

Management/Director Level Job Titles: The majority, around 85%, of suppliers with prior experience in security have had at least seven years of experience in the field prior to taking their current management/director level position. This is similar, but slightly less than security management practitioners of an equivalent level. Common broad or generic titles for staff at this level include manager and director. Examples include:

- Business Development Director
- Business Development Manager
- Director
- Project Manager
- Sales Team Manager

Executive Job Titles: At the executive level, security management suppliers with prior field experience tend to hold about the same level of expertise prior to assuming their positions as those on the practitioner side of the industry. About 85% had 11 or more years of experience in the

security field by the time they were hired into their current role. Common broad or generic titles among this group include vice president and c-suite positions:

- Chief Executive Officer
- Executive Director
- President
- Principal
- Vice President of Engineering
- Vice President of Sales

Typical Supplier Career Progression

Professional	Manager/Director	Executive
•Engineer	•Project Manager	•Vice President
•Account Executive	•Manager	•C-Suite
•Coordinator/ Associatge	•Director	

Occupational Roles and Responsibilities

As previously mentioned, security professionals are responsible for a broad set of concerns that generally span the following:

- Having accountability over enterprise-wide risk issues (e.g., physical security, personnel, information security, brand and intellectual property)
- Leadership over the security function, including management and training of security staff
- Communicating with, and educating, other non-security personnel about the importance of security and their role in facilitating safety and security within the organization

PRACTITIONERS

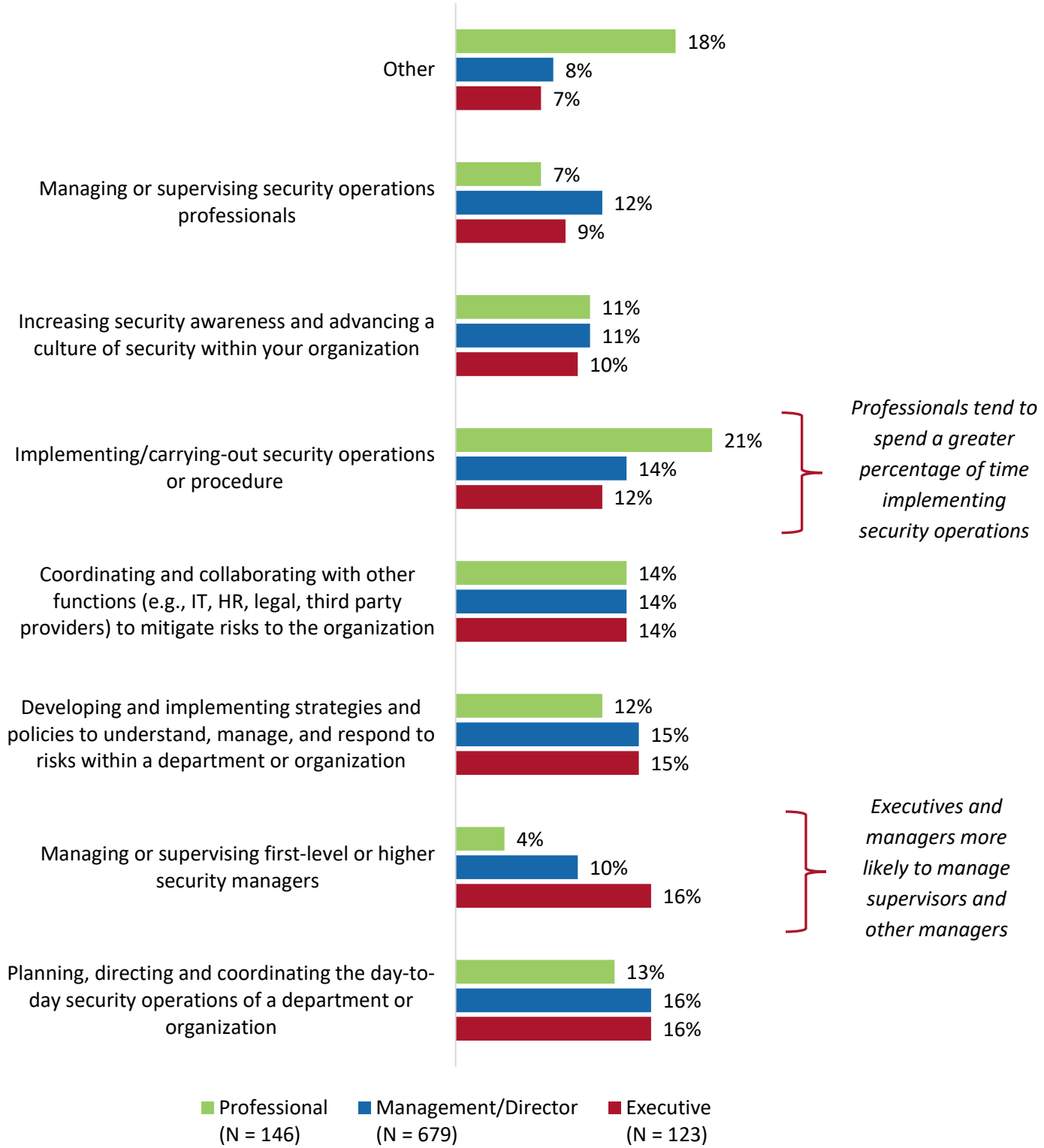
RESPONSIBILITIES

Practitioners at all levels divide their time, to varying degrees, between operations, planning, management, and coordinating. Security management practitioners directly implement security procedures, techniques, and approaches within their own organization or for a client organization. They may specialize or focus on one domain in the security role (e.g., investigations) or may hold a broader focus (i.e., as in the case of a chief security officer who oversees and coordinates security efforts across the enterprise). Regardless of their level of responsibility, security management practitioners have a diverse set of concerns and are likely to divide their time across many different tasks, including planning, directing, and coordinating security operations, developing and implementing security strategies and policies, and coordinating among different functions in their organization. Although security practitioners' tasks may vary according to their level of responsibility (e.g., managers and executives are more likely to manage first-line or higher managers, while professionals are most likely to be involved with implementing security operations), all practitioners nonetheless experience a role in each type of responsibility regardless of their station within their company or organization. The chart on the following page illustrates findings from the survey, and describes the way security practitioners devote their time, segmented by their level of responsibility:

- *Professionals* tend to spend about 21% of their time implementing security operations or procedures; however, they are similar to managers and executives in having responsibility for developing security strategies, planning/coordinating procedures, coordinating with other functions and departments, and even in having responsibility for increasing security awareness throughout the organization.

- *Managers* and *executives* spend the greatest share of their time on development and implementation of strategies as well as operations. While managers and executives may spend about one-third of their time focused on planning, directing, or coordinating security operations (16% of their time, on average) and developing and implementing strategies to understand and manage risk (15% of their time, on average); they, nonetheless, devote a portion of their time to implementing or carrying-out security operations.

Percentage of Time Spent Performing Job Functions
Security Management Practitioners



BUSINESS FUNCTIONS

Business functions become increasingly important as a practitioner moves from professional level to executive – offering a glimpse at the skills development required throughout the course of a career. In addition to allocation of time spent performing certain tasks, survey respondents were asked to review a list of job responsibilities that ranged from core business functions (e.g., strategy and planning) to security management functions (e.g., investigations and intelligence) and identify which functions they are responsible for in their current role. Consistent with findings reported above, while executives and managers were more likely to have responsibility over business functions, professional level staff were most likely to spend their time focused on security operations.

- *Executive level responsibilities:* Executive level security management practitioners tend to have a full plate when it comes to their responsibilities. This applies to both business functions as well as security operations. However, this group is unique in that they are most likely to have the core business functions of budget and finance, strategy and planning, and general management as part of their portfolio. They are also much more likely than staff at other seniority levels to hold responsibility over sales and business development (if relevant according to their employer-type), human resources, procurement and contracting, and marketing and/or marketing research/analytics. However, these responsibilities may be much more common in organizations that provide security services than in end-user/client organizations[5]. The wide scope of responsibility illustrates the range of accountability and demands on executives' time. Consequently, executives in security management positions may be challenged in determining how to best prioritize their time.

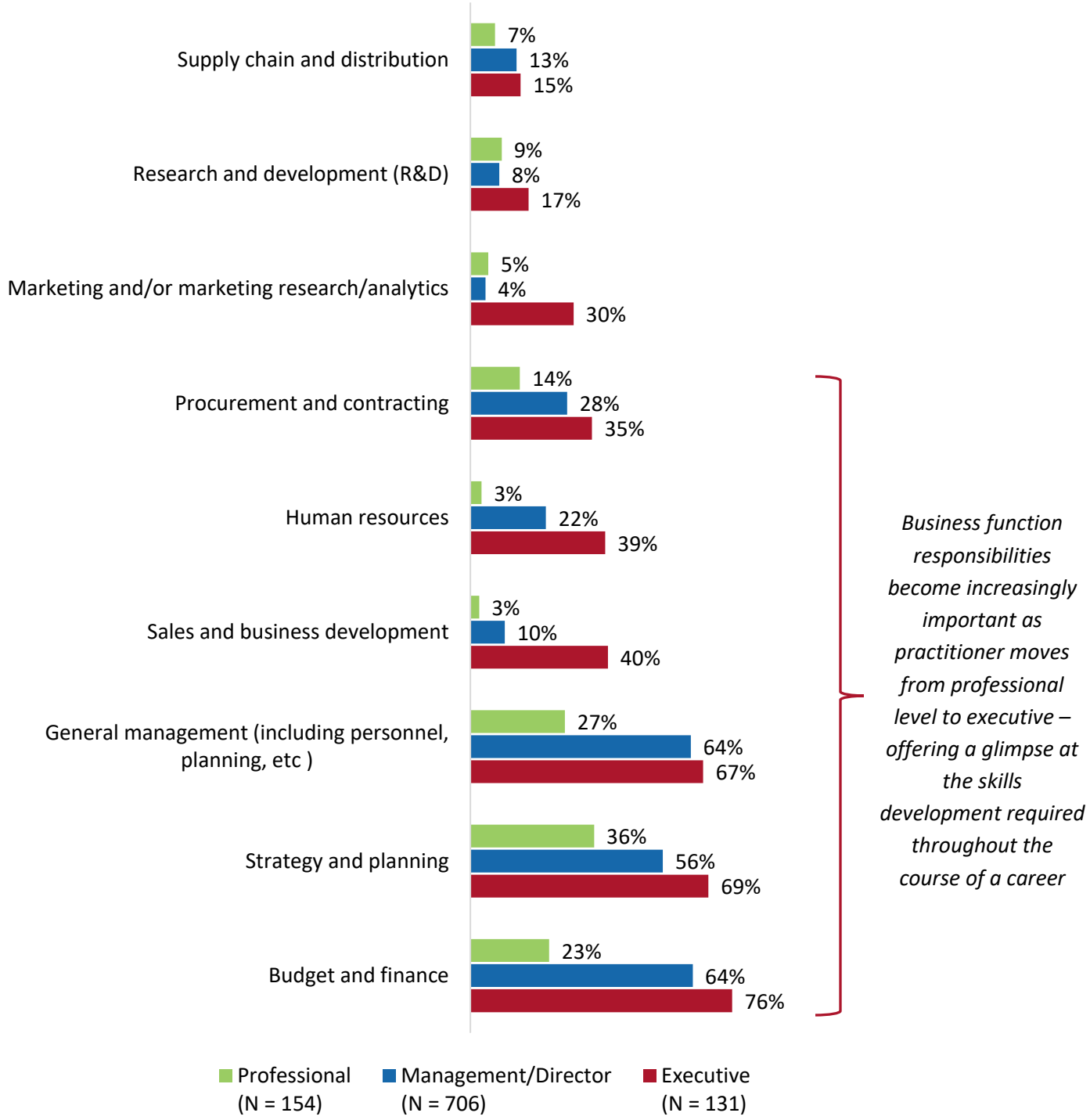
- *Management/director level responsibilities:* Management/director level practitioners tend to have slightly fewer diverse responsibilities than their executive counterparts. Instead of the wide breadth of business-related functions, they may be more likely to focus on a few important responsibilities that correspond to their job, including budgeting, strategy, and general management.

- *Professional level responsibilities:* Professional level staff are much less likely to have business-related tasks and functions as part of their role, focusing instead on security management operations.

The chart on the following page illustrates the breakdown of these responsibilities. Those in management/director or executive roles tend to have very widely distributed business roles, while only around one-third (capped at 36%) of those at the professional level hold responsibilities over business functions.

[5] The security management practitioner category encompasses both end-users (e.g., security management personnel employed by corporations for internal security operations) as well as providers of security management services (e.g., investigation company). Employees at provider organizations are significantly more likely to have business management responsibilities such as sales, human resources, and marketing analytics than those at end-user organizations.

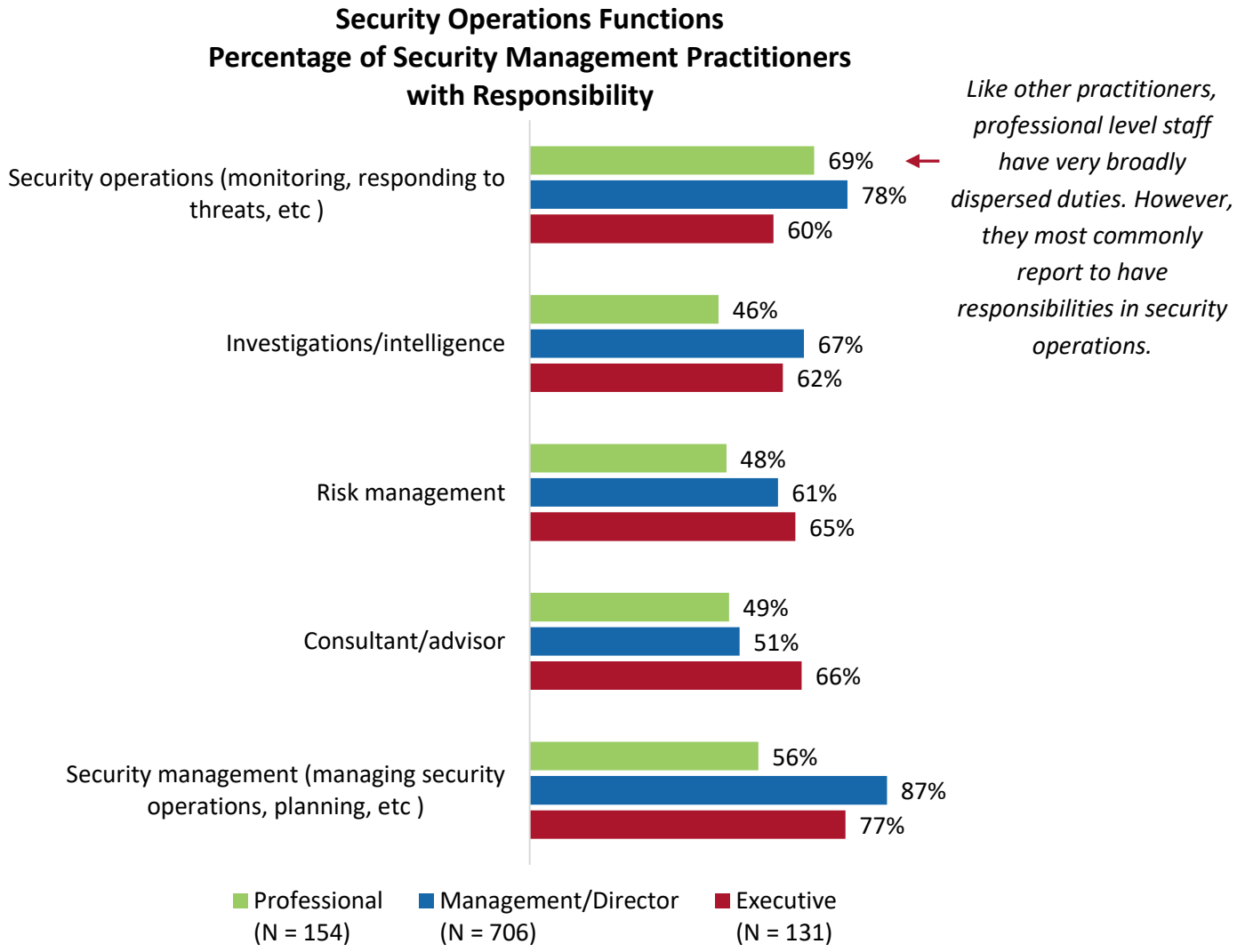
Business Functions
Percentage of Security Management Practitioners with Responsibility



Business function responsibilities become increasingly important as practitioner moves from professional level to executive – offering a glimpse at the skills development required throughout the course of a career

SECURITY OPERATIONS

Security operations, the implementation and oversight of security techniques, approaches, and methods, is the responsibility of all security management personnel, regardless of their level of seniority; however, some important role differentiators do exist. While executives are more likely than others to hold a consultative/advisory role in the security function, managers are somewhat more likely to report holding responsibility over the actual security management function (operations, planning). Perhaps not surprisingly, those at the professional level are most likely, compared to any other task or responsibility, to indicate that they spend time in the rubber-meets-the-road security operations function (e.g., monitoring, responding to threats).



MOST CHALLENGING AND REWARDING ASPECTS OF JOB

While practitioners at different levels of responsibility may experience similar categories of responsibility (e.g., management, strategy and planning, security operations), there are key differences in the scope of their responsibilities, focus, and top professional challenges. Participants in the ASIS International-SIA Career Survey provided further explanation about their day-to-day work through a series of comments describing their job role. The quotes reported below help to illustrate how a practitioner's focus may differ according to their level of responsibility.

Professional Level:

- *"I design and implement video surveillance." (End user of security services)*
- *"I coordinate all aspects of security with (my employer), contractors, and various stakeholder elements." (End user of security services)*

Management/Director Level:

- *"My primary duties have included the investigation of all forms of loss, assessment of compliance with applicable policies, procedures, and regulatory requirements, and providing guidance as needed regarding appropriate preventative measures to mitigate losses due to operational, criminal, or safety concerns. I have significant involvement in investigating allegations of misconduct, hostile work environment, etc. in support of employee relations"' (End user of security services)*
- *"I am (at a senior level of responsibility) of a (large) privately contracted guard force. I keep abreast of all aspects of the security industry…manage a (specific) security program and co-managing my client's program. I create all security plans for special events involving (specific individuals), keeping track of all goals, accomplishments and metrics, how to optimize utilization of our guard force, keep our business continuity plan up to date, and maintain most of our documentation of our personnel." (Provider of security services)*

Executive Level:

- *"I ensure that the company's people and assets are protected, and that we are ready and capable of responding to an emergency or crisis." (End user of security services)*
- *"My principal role is to strategically add value to our clients through innovation and diversification." (Provider of security services)*

Practitioners also weighed-in on the most difficult aspects of their job. They described that major challenges in security management include educating internal and external stakeholders to the importance of the security function, collaborating among different departments and functions, and the challenge of resource constraints and limited time to accomplish their goals.

Selected Quotes – Most Difficult Challenge

Professional Level

- "The number of "hats" I must wear throughout the aspect of the job."

Management/Director Level

- "Time management, with such broad scope of responsibilities it is difficult to commit quality time to each area of responsibility to deliver our very best for each program."

Executive Level

- "The most challenging aspect is dealing with buy-in and the complexities of security in general. The importance of the position is swept under the rug until something major occurs."

Despite these difficulties, security management practitioners expressed job satisfaction with respect to a job well done (e.g., "*working with our team to provide practical and useful guidance that we see is valued by our internal client teams the world over.*"), great degree of purpose ("*I find that what we do as security professionals is very noble*"), variety of work *('there are new and interesting challenges everyday'*), and problem solving aspects of the work ("*being able to solve a…complex security need within budget in innovative ways.*")

SUPPLIERS

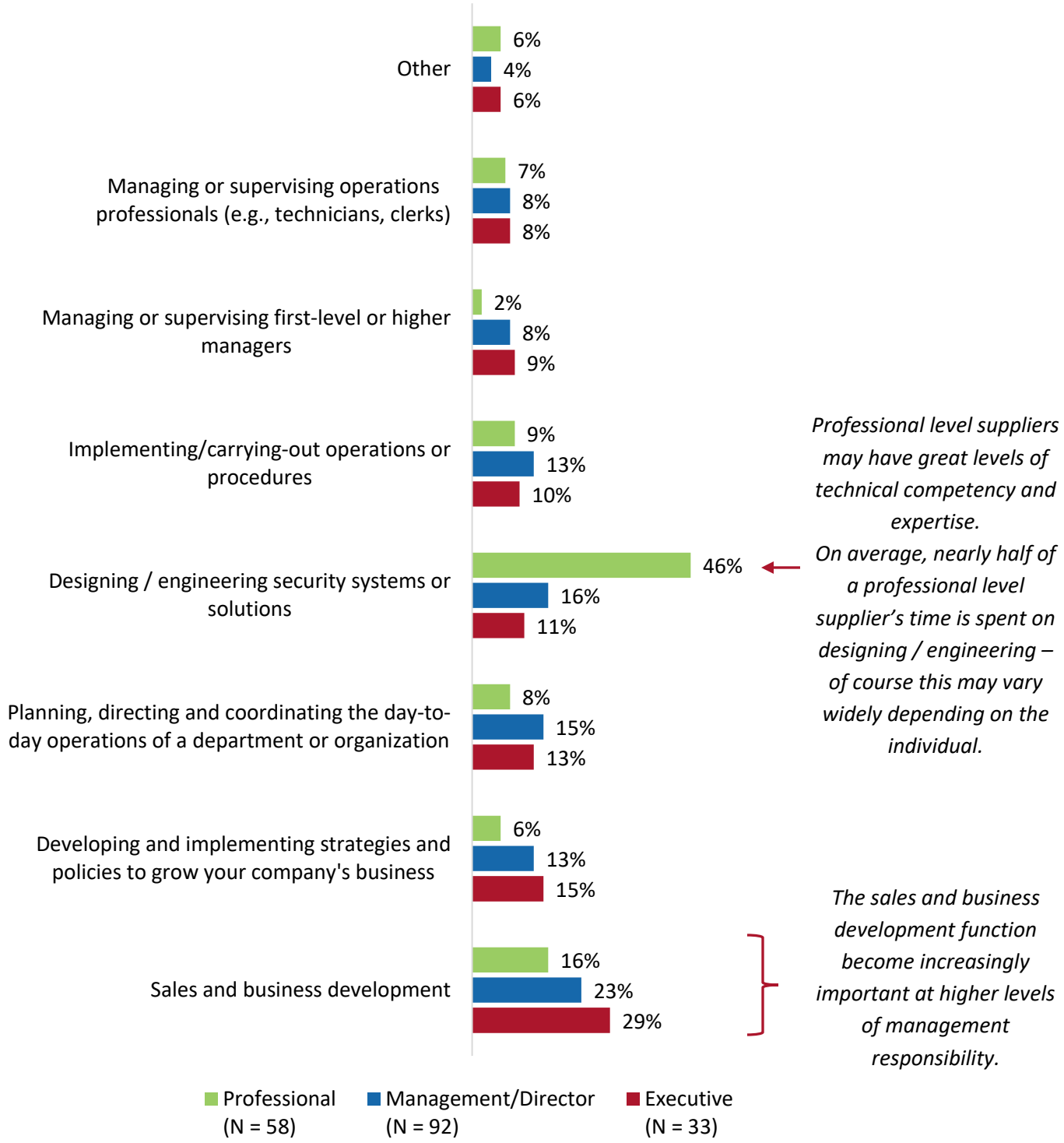
RESPONSIBILITIES

Suppliers may hold job responsibilities that reflect a very specialized role in one or more components of an organization's enterprise security scheme (e.g., selling technology, providing installation services) or may hold a broader organizational focus towards a client enterprise (e.g., providing general consulting services and assessments). Regardless of their role, supplier personnel require much of the same knowledge possessed by security practitioners regarding approaches and methodologies for identifying, prioritizing, and preparing for security threats. This is particularly important due to the very rapid pace of development of new technologies as well as technological threats to security. Depending on their role, suppliers may also devote a portion of their time and efforts towards the business development and sales function.

Security industry personnel on the supplier side of the industry are likely to have slightly more differentiated responsibilities according to their level of responsibility than their practitioner counter-parts. For example, the average professional level employees at a supplier company is likely to spend around 46% of his or her time in designing / engineering security systems or solutions, compared to executive level staff which might spend about 11% of their time on the same tasks. Similarly, executives in supplier companies are more likely than professionals to devote a greater share of his or her time to the sales, or business development, function. The greater amount of delineation in their roles may result in a more challenging transition from one level to the next for staff in supplier organizations – and thus require more support from the employer in terms of training and professional development resources.

The graph on the following page illustrates the average percentage of time that suppliers at each level of responsibility (professional, management/director, executive) may expect to spend on each job function. However, those in very specialized / focused roles, particularly at the professional level, may find that their responsibilities are much more heavily focused in one category or another.

Percentage of Time Spent Performing Job Functions
Security Industry Suppliers



Professional level suppliers may have great levels of technical competency and expertise.

On average, nearly half of a professional level supplier's time is spent on designing / engineering – of course this may vary widely depending on the individual.

The sales and business development function become increasingly important at higher levels of management responsibility.

BUSINESS FUNCTIONS

Professionals on the supplier side reinforced differentiated roles between professional level and executive level positions, varying in focus on operations versus business function. Industry suppliers that participated in the ASIS International-SIA Career Survey identified tasks that they perform related to business and security operations. Survey results were consistent in that supplier personnel described highly differentiated roles at the professional versus executive level, the former being more highly specialized in design and engineering, while the latter are much more likely to hold business development and sales responsibilities.

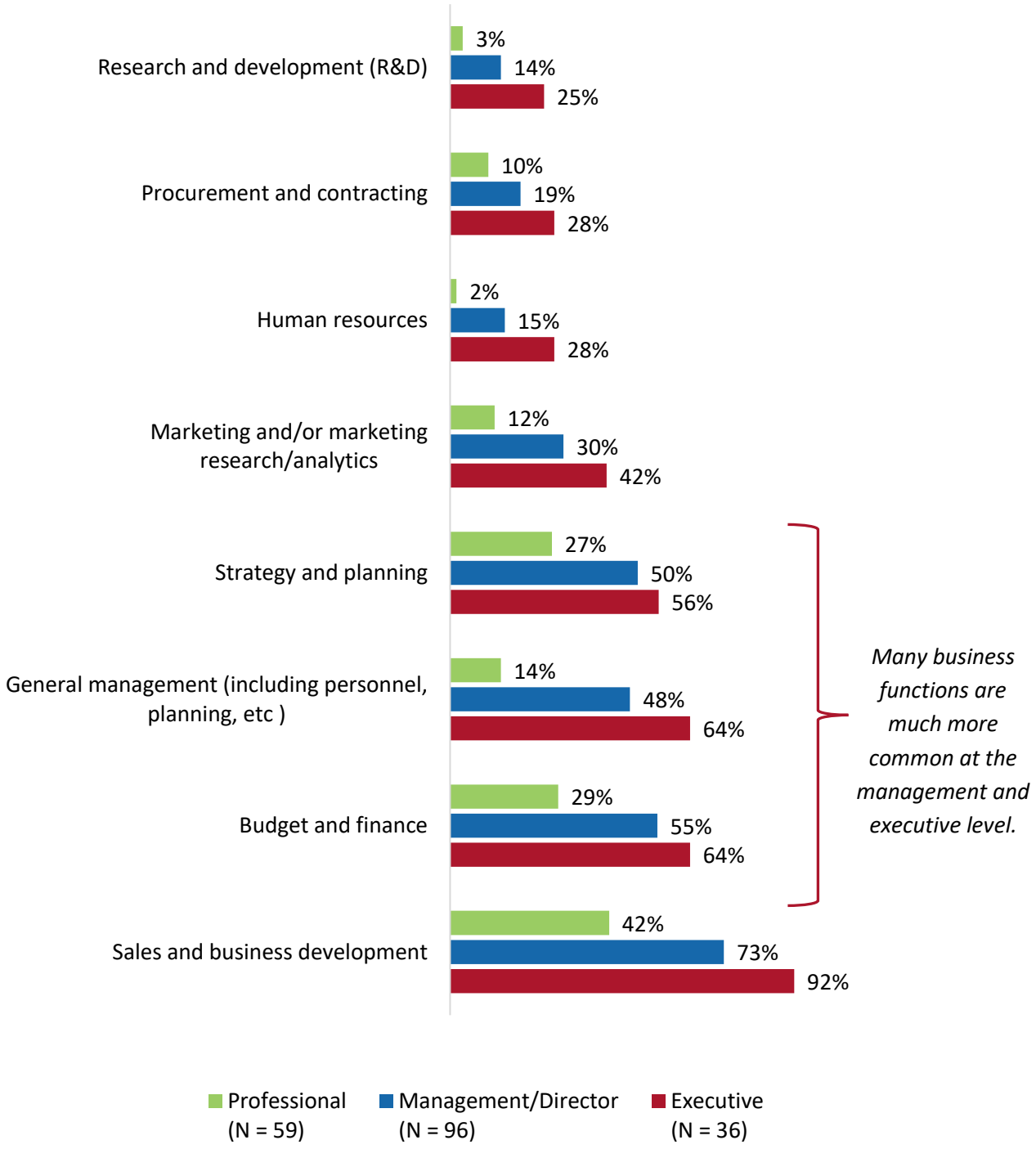
Sales and business development comprise a core "business function" responsibilities for suppliers. Security management professionals in supplier roles are similar to practitioners in that they hold diverse responsibilities according to their level of seniority, however; the sales function takes on much greater importance among suppliers. In additional to sales, other areas that job titles may focus on among supplier companies include: finance, HR, IT, compliance, legal, technical support, quality control, customer service, marketing, supply chain management and product management.

- *Professional Level Responsibilities:* Professional level security management supplier staff are less likely to hold responsibilities in core business functions than security management operations, but many did nonetheless indicate having sales and business development responsibilities – perhaps due to their oftentimes client-facing roles.

- *Management/director Level Responsibilities:* Those in management/director are also likely, although somewhat less than executives, to be involved in each of these business functions as well as the other core business tasks (e.g., marketing or marketing research/analytics, human resources, procurement and contracting, and R&D).

- *Executive Level Responsibilities:* Nearly all executives in supplier companies hold sales/business development responsibilities. They are also very likely to be involved in budget and finance, general management, and strategy and planning.

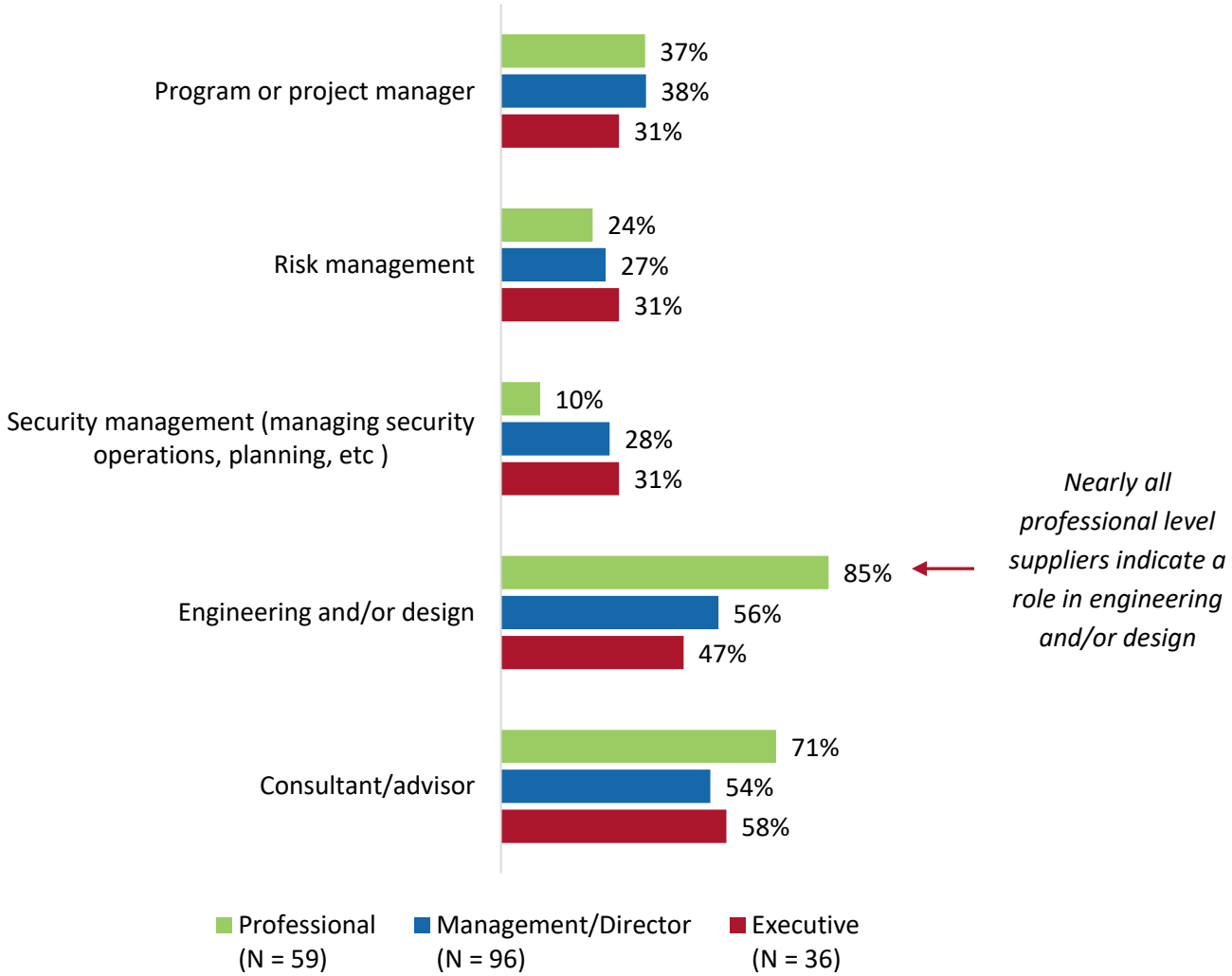
Business Functions
Percentage of Security Industry Suppliers
with Responsibility



SECURITY OPERATIONS

In terms of security operations, executive and management/director positions in security industry supplier organizations are very similar to one another in their likelihood to involve operations-focused responsibilities, such as consultative/advisor roles, engineering and/or design, security management, risk management, and project or program management. Although these senior personnel may have similar patterns in involvement in these tasks, their actual responsibilities and day-to-day tasks may depend on their exact position in the organization. Conversely, professional level staff in these organizations, oftentimes the front-line in terms of technical expertise and know-how, indicate a much greater focus on engineering and design and even consultation/adviser services.

Supply Operations Functions
Percentage of Security Industry Suppliers with Responsibility



MOST CHALLENGING AND REWARDING ASPECTS OF JOB

Security industry suppliers described the breadth of their role and responsibilities in a similar manner to practitioners, however; their focus was more oriented towards the implementation of technical solutions. The quotes below were selected to illustrate how suppliers at different levels of responsibility may each experience a different job focus.

Professional level:

- *"I provide design and specification of security infrastructure."*
- *"I act as a design and consulting engineer and project manager for (specific systems)."*

Management/director level:

- *"I provide end users and partners with resources to successfully utilize my products."*
- *"I oversee the day-to-day operations and overall performance of (my department)."*

Executive level:

- *"I'm responsible for all day-to-day operations, contract management, and design engineering."*
- *"I focus on seeking new business and growing and maintaining existing business. I'm also engaged in highlighting areas of avoidable exposure to risk, advising on new or improved technology, or practices that may reduce or eliminate exposure to loss or risk to businesses assets, including its human resources, and those with which it interacts."*

Security industry suppliers expressed a variety of concerns when considering the most challenging aspects of their work. In fact, similar challenges exist regardless of the supplier's level of responsibility, including the demands on their time and the challenges in educating clients about optimal solutions.

Selected Quotes – Most Difficult Challenge

Professional Level

- "The need to be in more than one place at a time."

Management/Director Level

- "Preconceived beliefs on cost effective & effective security countermeasures."

Executive Level

- "Staying focused among multiple disciplines and responsibilities."

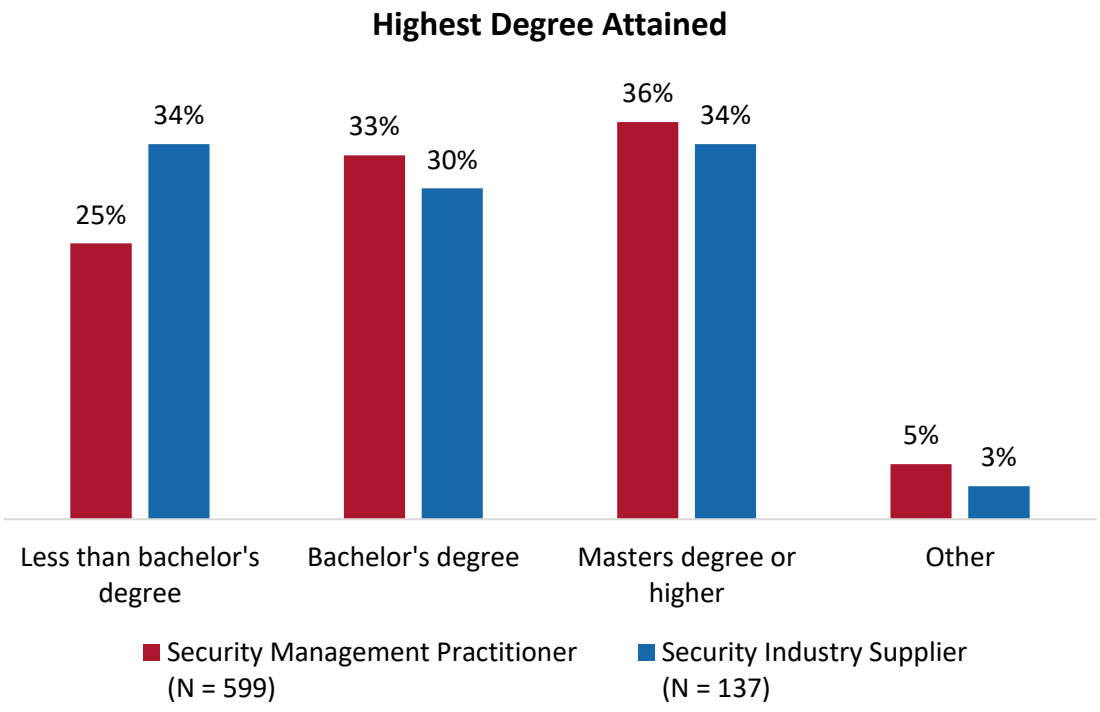
Similar to security management practitioners, suppliers find great reward in their job, including the challenge of the work ('*being able to give vision and set strategy goals for sales, culture, and overall business environment*'), the satisfaction of a job well done *('[when we are able to] obtain a result of the physical security system that exceed the initial plan'*) and truly creating an impact ('*we are able to help people save lives*').

Education and Credentials

Professionals in the security field come from diverse professional and educational backgrounds. While there is no required educational pathway for entry into the field, many security personnel have a background in courses of study that correspond to their job responsibilities. For security management practitioners, this includes criminal justice (e.g., criminal justice, law, sociology), business (e.g., management, finance), and/or courses of study in the social sciences (e.g., political science). Suppliers also have benefited from these academic disciplines, but many have chosen to focus on technical training (e.g., technology, engineering). In addition to education, many industry professionals have elected to acquire relevant credentials and/or participate in professional service.

EDUCATIONAL ATTAINMENT

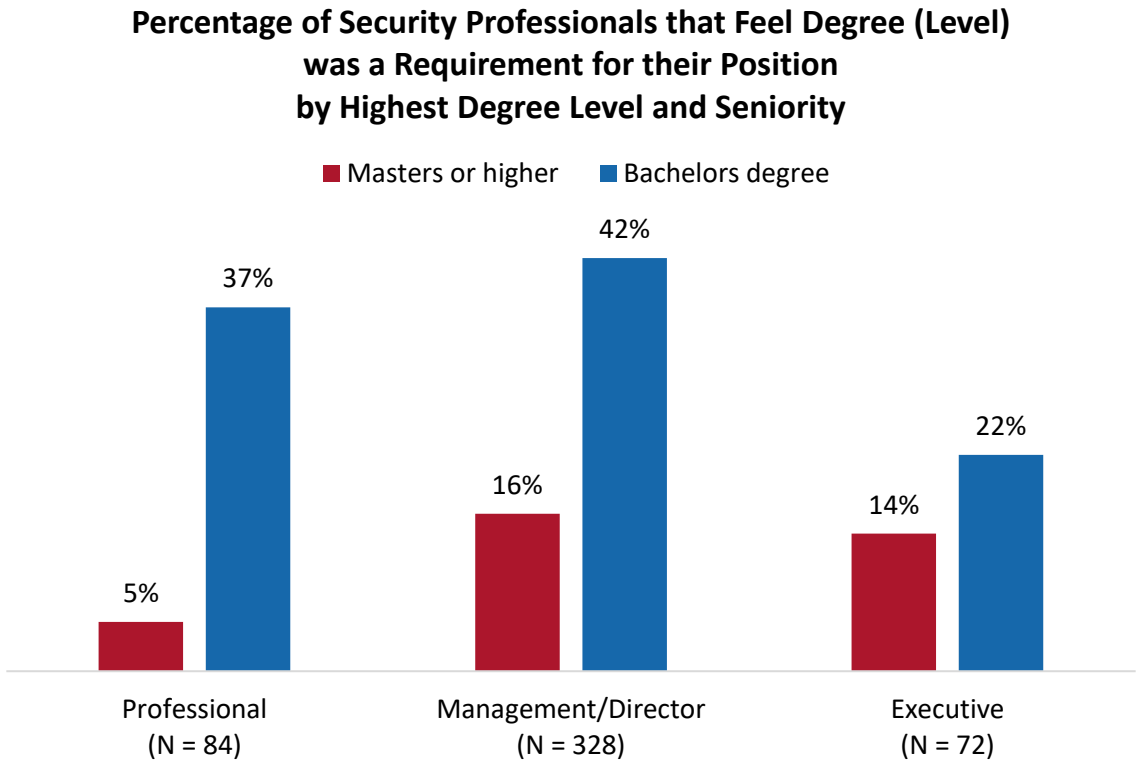
Both security management practitioners as well as security industry suppliers hold similar levels of education, with about one-third representing less than a bachelor's degree (e.g., associate's degree, some college, or high school diploma), one-third holding a bachelor's degree, and slightly over one-third having obtained a master's degree or higher. In general, educational levels do not differ substantially between those at the professional, management/director, or executive levels.



VALUE OF DEGREE LEVEL

Degree requirements appear to be more important at the management/director level than professional or executive level. Nearly half of participants (42%) in the ASIS International-SIA Career Survey that serve in a management/director role and have acquired a bachelor's degree described their educational attainment as a requirement for their position. Sixteen percent with a masters or higher indicated the same.

This educational requirement at the management/director level may reflect the desire from employers to pre-qualify their hires at the management/director level, whereas technical abilities or professionalism may be more important for those as the professional level. On the other hand, many executive positions may not face strict educational requirements, either because they are held by company owners/founders, or, because the most important qualifications for the positions may rest on experience and demonstrated accomplishments.



It is also worth noting that, even in cases where survey respondents felt their degree was not a requirement, the vast majority of those with at least a bachelor's degree at the professional, management/director and executive levels did note that their degrees helped to demonstrate their qualifications or set them apart from other candidates.

MOST POPULAR COURSE OF STUDY

Degrees that are most directly connected with the security field (e.g., criminal justice, law enforcement) are seen as most valuable. Interestingly, most security professionals feel that their specific course of study was more helpful to them in qualifying them for their current position than their first job in the field. Security management practitioners are most likely to have majored at the undergraduate level in criminal justice and business administration and management, although political science, law enforcement and corrections, and economics are also popular courses of study. This trend is mirrored at the graduate degree-level, where the most popular programs of study for practitioners are management and administration, criminal justice, and security technologies.

Security industry suppliers also tend to major in business administration and management and criminal justice at the bachelor's level, however; several of the most popular degree programs for this segment of the industry are electrical engineering, engineering science, and information sciences and technology. In terms of the value of their education, a strong majority (70% - 81%) of security management practitioners and security industry suppliers indicated that their area of study was important in qualifying them for their current position.

	Security Management Practitioner	Security Industry Supplier
Bachelor's or associate's course of study	1. Criminal justice (27%) 2. Business administration and management (24%) 3. Political Science (11%) 4. Law enforcement and correction (10%) 5. Economics (6%)	1. Business administration and management (28%) 2. Electrical engineering (19%) 3. Engineering science (9%) 4. Criminal justice (9%) / Information sciences and technology (9%) / Marketing (9%) [tie]
Masters degree or higher course of study	1. Management (14%) 2. Administration (9%) 3. Criminal justice (8%) 4. Law (4%) 5. Security technologies (4%)	1. Engineering (22%) 2. Administration (17%) 3. Management (13%) 4. Marketing and communications (7%) 5. Security technologies (4%)
% indicating background area of study important in qualifying for current position	Executive (73%) Management (81%) Professional (71%)	*Executive not reported due to low sample size Management (79%) Professional (80%)

The table below illustrates the percentage of security professionals that feel their background area of study was important in qualifying them for their first and current positions in the security field. Degrees that are most directly connected with the security field (e.g., criminal justice, law enforcement) are seen as most valuable. Interestingly, most security professionals feel that their specific course of study was more helpful to them in qualifying them for their current position than their first job in the field.

	% Indicating Important for First Job in Field	% Indicating Important for Current Job
Bachelors or Associates		
Criminal justice (N = 66)	80%	89%
Law enforcement and corrections (N = 25)	76%	88%
Economics (N = 16)	50%	87%
Business administration and management (N = 67)	58%	82%
Electrical engineering (N = 13)	69%	79%
Political science (N = 27)	59%	64%
Graduate		
Engineering (N = 15)	93%	88%
Management (N = 33)	52%	88%
Criminal justice (N = 17)	76%	80%
Administration (N = 26)	42%	72%

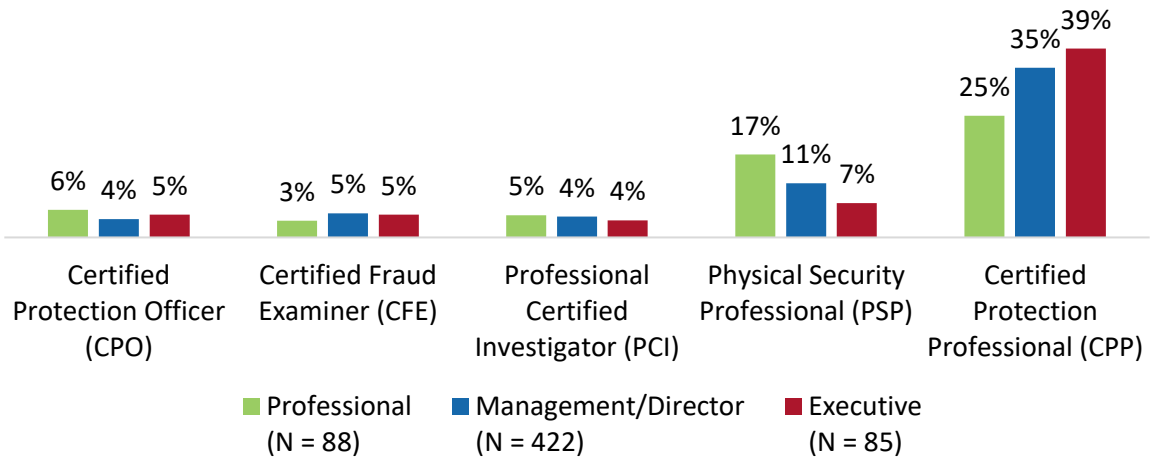
CREDENTIALING AND PROFESSIONAL SERVICE FOR PRACTITIONERS

Although not necessarily required by employers, credentials and involvement in professional associations contribute to career growth and opportunity. Security professionals have a wide variety of credentials available to them to test and affirm their knowledge, competency, and skills. Acquiring certifications and other forms of credentialing can often help demonstrate qualification for jobs but may also function to challenge the professional to evaluate and grow their own skill set. **Consequently, nearly all security professionals who acquired ASIS International and SIA certifications indicated the credential was "very" or "somewhat" important for professionals in their role, including CPP (93%), CSPM (93%), PSP (88%), and PCI (74%).**

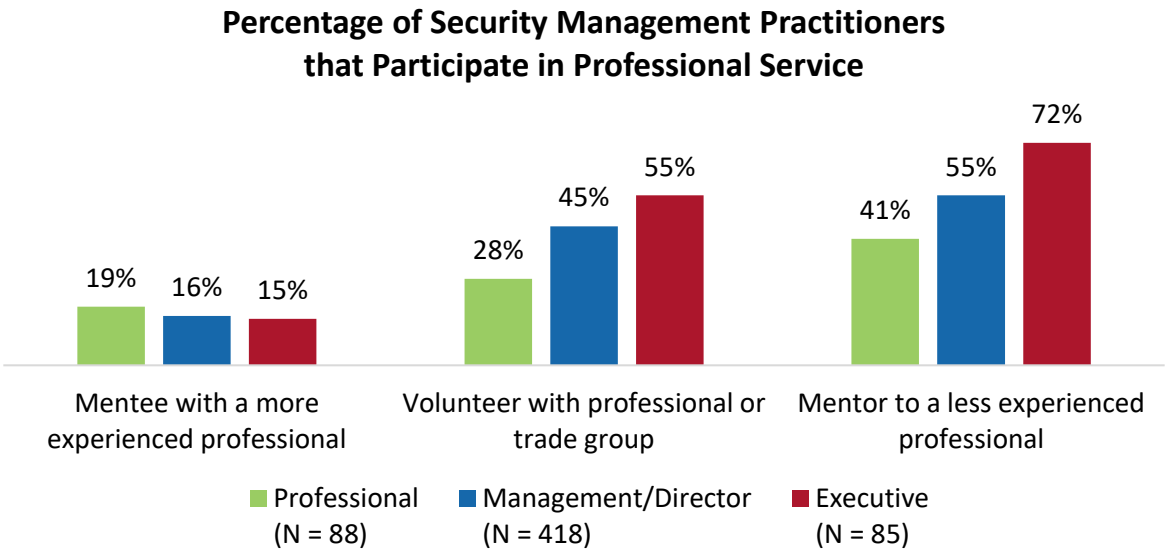
Participants in the ASIS International-SIA Career Survey possessed a range of different certifications, designations, and other credentials. However, the most popular certifications among

security management practitioners were the Certified Protection Professional (CPP) and Physical Security Professional (PSP) certifications. While the CPP tends to be most popular among those with greater levels of seniority (management/director and executive level staff), the PSP holds greater attraction at the professional level. The chart below illustrates the percentage of security management practitioners that possess the five most common certifications.

Percentage of Security Management Practitioners who Attained Certification (Most Popular Shown)

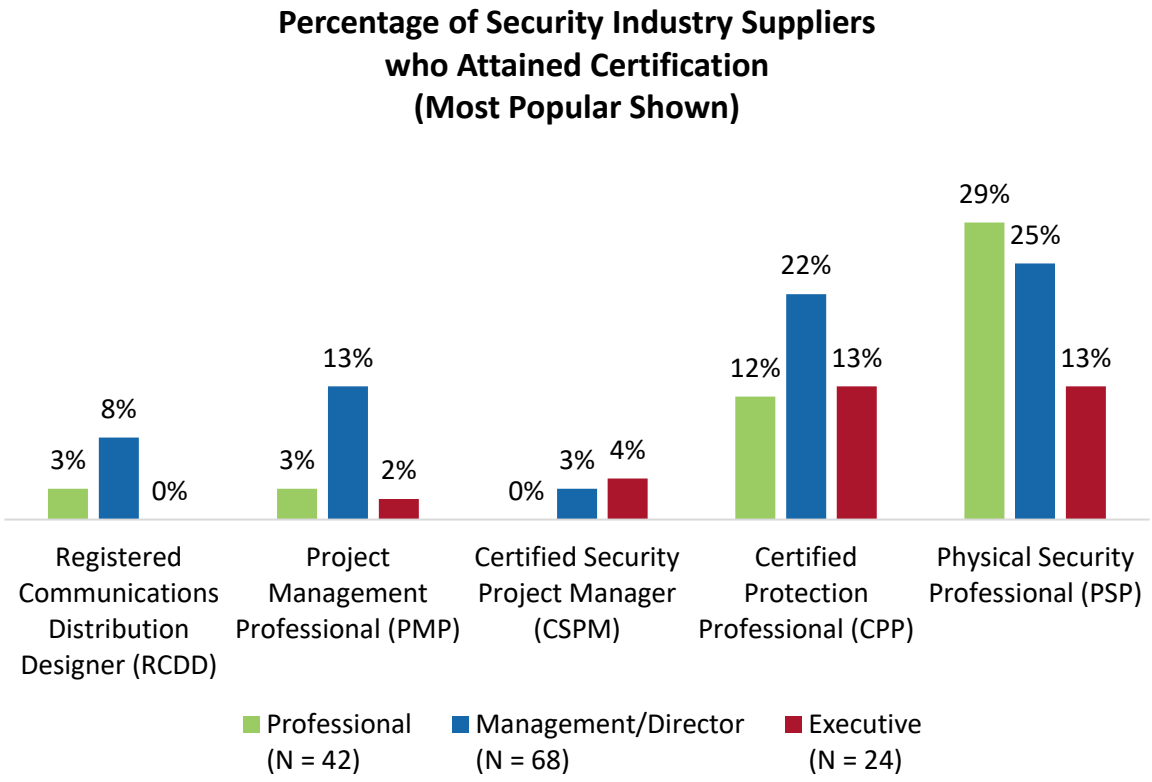


In addition to acquiring certification, another popular method of professional development is participation in activities such as volunteering with professional associations and mentoring programs. These types of opportunities are common among security management practitioners. While nearly three-quarters of executives noted that they serve as a mentor to less experienced professionals in the field, about half also volunteer with a trade or professional society. Likewise, nearly half of all management/director level practitioners act as mentors and/or volunteer with their association. Professional level staff, who may still be working up the "career ladder" are less likely to be involved in these types of activities. Nonetheless, they may represent an important growth opportunity for them as they progress to higher levels of responsibility.

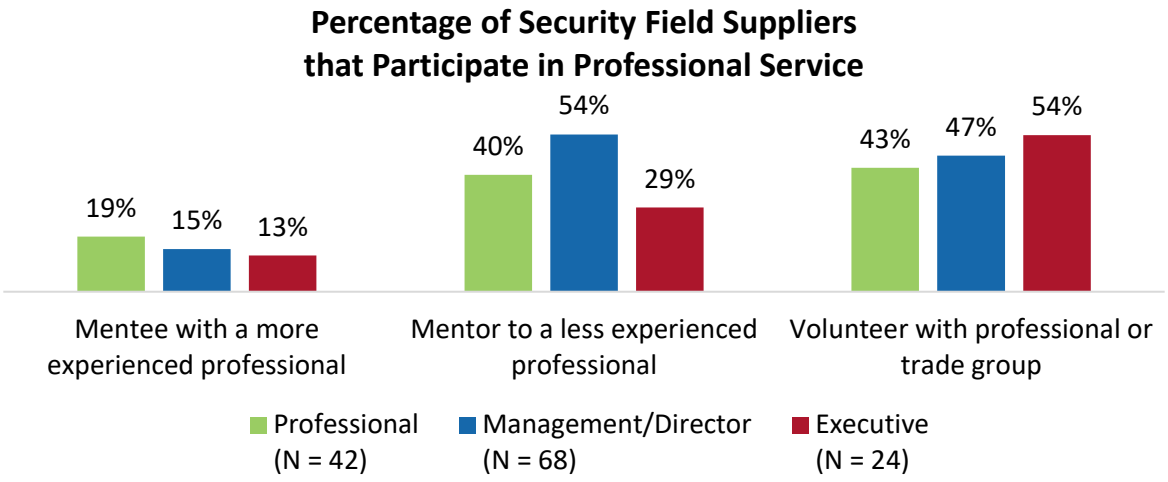


CREDENTIALING AND PROFESSIONAL SERVICE FOR SUPPLIERS

The CPP, PSP and several other certifications (CSPM, PMP, and RCDD) are common among suppliers, and suppliers at all career stages are likely to be involved in industry associations. Similar to security management practitioners, many security industry suppliers have acquired the Physical Security Professional (PSP) and/or Certified Protection Professional (CPP) certifications. However, also noted among suppliers are project management certifications such as the Certified Security Project Manager (CSPM) and Project Management Professional (PMP) certifications, likely due to the increased importance of project management in the role of suppliers (particularly at the management/director level). The Registered Communications Distribution Designer (RCDD) certification was also held by almost 10% of suppliers.



As in the case of security management practitioners, many security industry suppliers have participated in the field as volunteers and mentors. Interestingly, nearly half of suppliers, regardless of their level of seniority are involved in their professional or trade association. While this level of involvement is common at the management/director level or higher for practitioners, even professional level suppliers tend to engage in their industry groups. This may be due to the increased technical focus among supplier professionals as well as the wide responsibility for sales and business development common among supplier responsibilities.


Percentage of Security Field Suppliers that Participate in Professional Service
19%
15%
13%
40%
54%
29%
43%
47%
54%
Mentee with a more experienced professional
Mentor to a less experienced professional
Volunteer with professional or trade group
Professional (N = 42)
Management/Director (N = 68)
Executive (N = 24)

Career Pathway into Security Field

Security management practitioners and suppliers that participated in the ASIS International-SIA Career Survey indicated the field they came from prior to entering the security industry. **Although the most popular points of entry were from law enforcement, military or business, there were examples of security professionals hailing from many different professional backgrounds.**

PRACTITIONERS

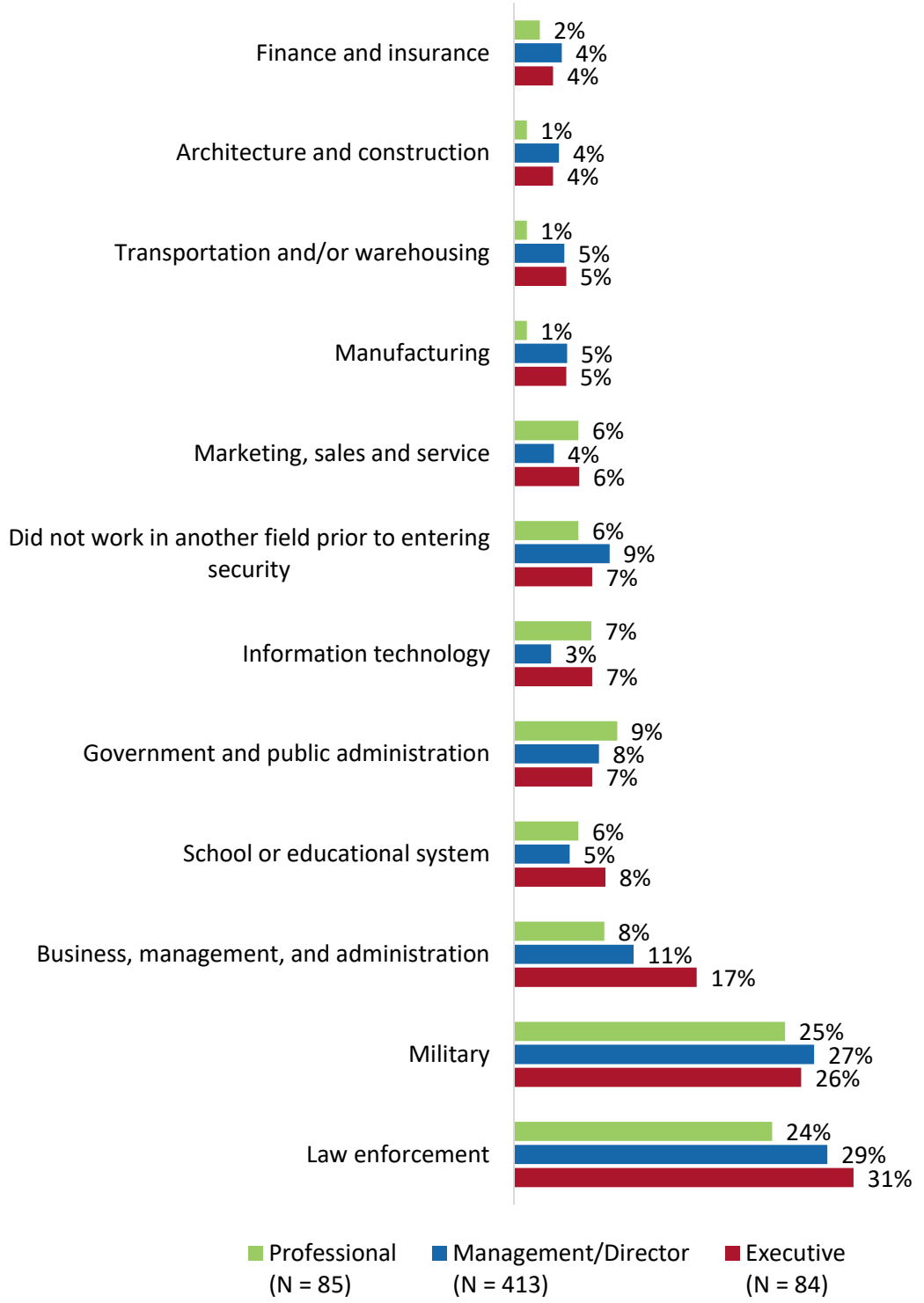
The most popular fields for practitioners to have originated from include law enforcement, the military, or business. As prior occupations, both law enforcement and military service offer direct experience in security and may provide a network that can assist in obtaining a security position. Additionally, since many security positions may require forming and maintaining relationships with other entities in the community (law, military, first responders, and the public) – having a background in law enforcement and/or military can provide an essential understanding of how best to work with external stakeholder organizations.[6]

Business, management, and administration was also identified by survey respondents as a frequent prior occupation, particularly among those in senior level positions. Such careers may be helpful in preparing security managers to navigate a corporate environment, as well as assist them in understanding and identifying various areas of risk. Moreover, business experience may be crucial in understanding many of the business-related roles and responsibilities in senior-level security positions (e.g., strategy and planning, budgeting/finance, human resources).

The graph on the following page illustrates the occupational fields that ASIS International-SIA Career Survey respondents came from prior to entering to security. Notably, while law enforcement and military careers were most popular overall, those at the executive level were more likely than others to come from business backgrounds.

[6] Survey participants from the United States provided additional information regarding their background. Overall, all levels of law enforcement were popular among respondents from the United States, including local law enforcement (27%), Federal (10%), and state (6%). Additionally, out of the 24% with a military background, 42% came from the Army, 21% from the Air Force, 17% from the Marines, and eight percent from the Navy. The remaining 12% hailed from a reserve group.

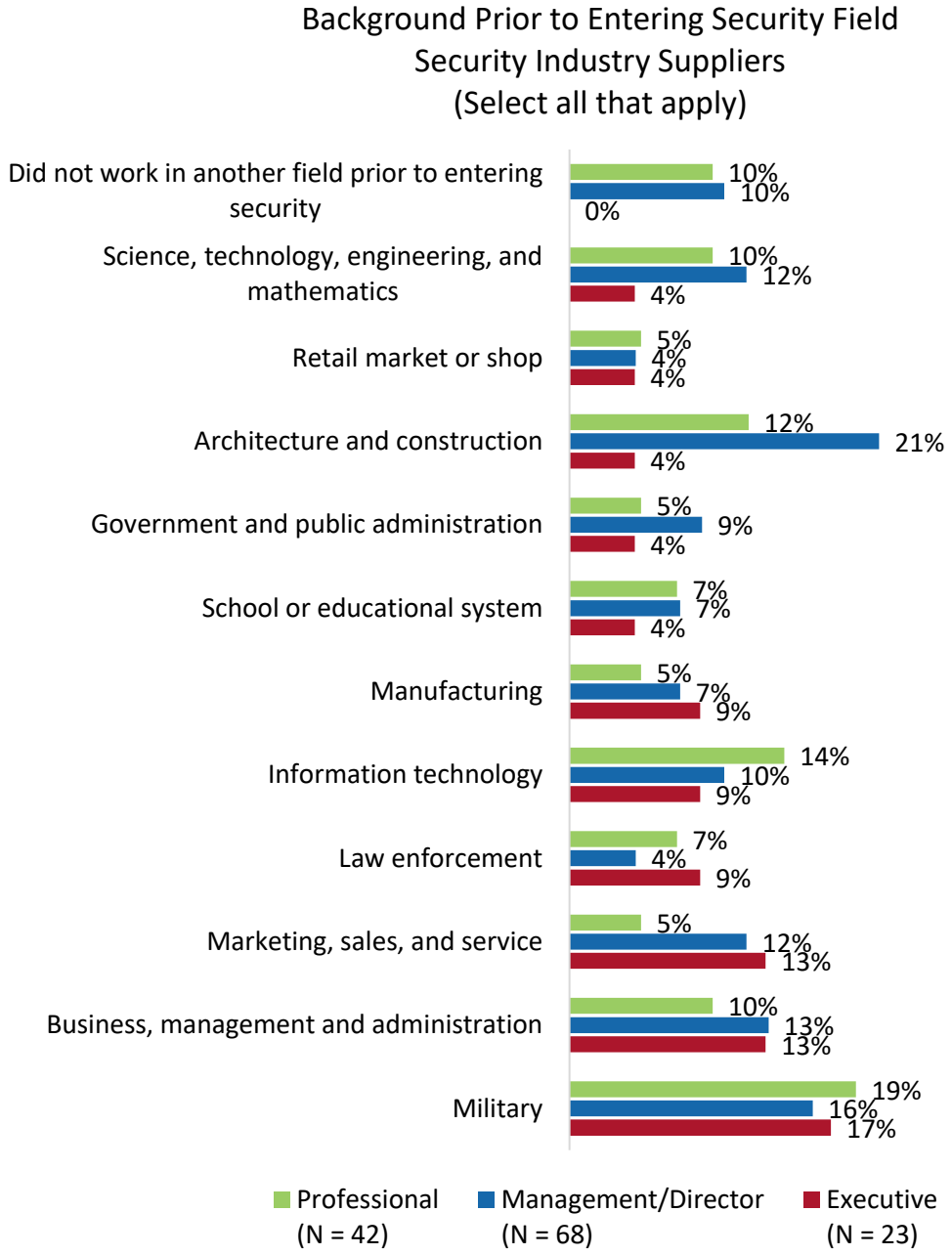
Background Prior to Entering Security Field
Security Management Practitioners
(Select all that apply)



The most popular fields overall include law enforcement, military, and business. Notably, executives appear more likely than others to have originated from law enforcement or business

SUPPLIERS

Compared to security management practitioners, security industry suppliers tend to come from a wider range of prior occupations. For example, although law enforcement, military occupations, and business remain important pipelines into the security industry, so too are technical and engineering fields such as information technology, manufacturing, and architecture and construction. The wider breadth of prior occupations is not surprising given the mix of generalist versus technical-specialist roles found on the supplier side of the security field.



Suppliers at the management level are more likely than others to have entered the field from architecture and construction occupations. However, care must be taken in interpreting this statistic due to relatively low survey sample sizes.

Competencies and Specialized Knowledge

Broad-based knowledge of security fundamentals is critical across all career stages, sectors and positions, but nuances and differences in required competencies and skills exist within segments. Participants in the ASIS International-SIA Career Survey were asked to review and identify crucial skills and traits[7] related to their current position.[8] In general, there were many consistencies across employer types (practitioners, suppliers) as well as levels of responsibility (professional, management/director, executive). For example, it was very common for security professionals of all backgrounds to identify the importance of broad-based general knowledge of security fundamentals. These findings are not surprising in that the security field is very diverse in its focus and a professional's success may depend on having a great breadth of knowledge of the issues and threats that may impact their employer or client. Additionally, soft-skills and traits, such as teamwork, collaboration, leadership, and integrity were also very commonly identified as crucial qualities of security professionals in both practitioner and supplier roles.

At the same time, there were also several nuances between practitioners and suppliers, and across levels of responsibility. For instance, while practitioners were generally more likely to stress the importance of general security fundamentals, risk management, and crisis management; suppliers tended to focus more narrowly on specific subject-matter expertise, technical knowledge, and customer relationship skills. Likewise, those in professional roles tended to identify the importance of operational and tactical knowledge and traits, whereas management/director and executive level professionals gravitated towards executive and sales-oriented skills.

PRACTITIONERS

Security practitioners of all levels of responsibility most commonly identified security fundamentals, risk management, and crisis management as important skills needed in their jobs.[9] This is not surprising given that practitioners are required to have a very broad base of knowledge to understand the myriad of security threats that might affect an organization. They are also expected to know the methods and approaches utilized to prepare for, detect, deter, and respond to those threats. Project management, which reflects both a knowledge area as well as expertise in how work is performed, was also frequently identified as an important skill.

---

[7] The list of skills and traits provided in this section is truncated. Each graph illustrates only those skills and traits that were most commonly selected by respondents. Additionally, the graphs contain only the titles or headings pertaining to each skill and trait, whereas respondents were provided with a definition. A full description of each skill and trait is provided in the appendix of this report.

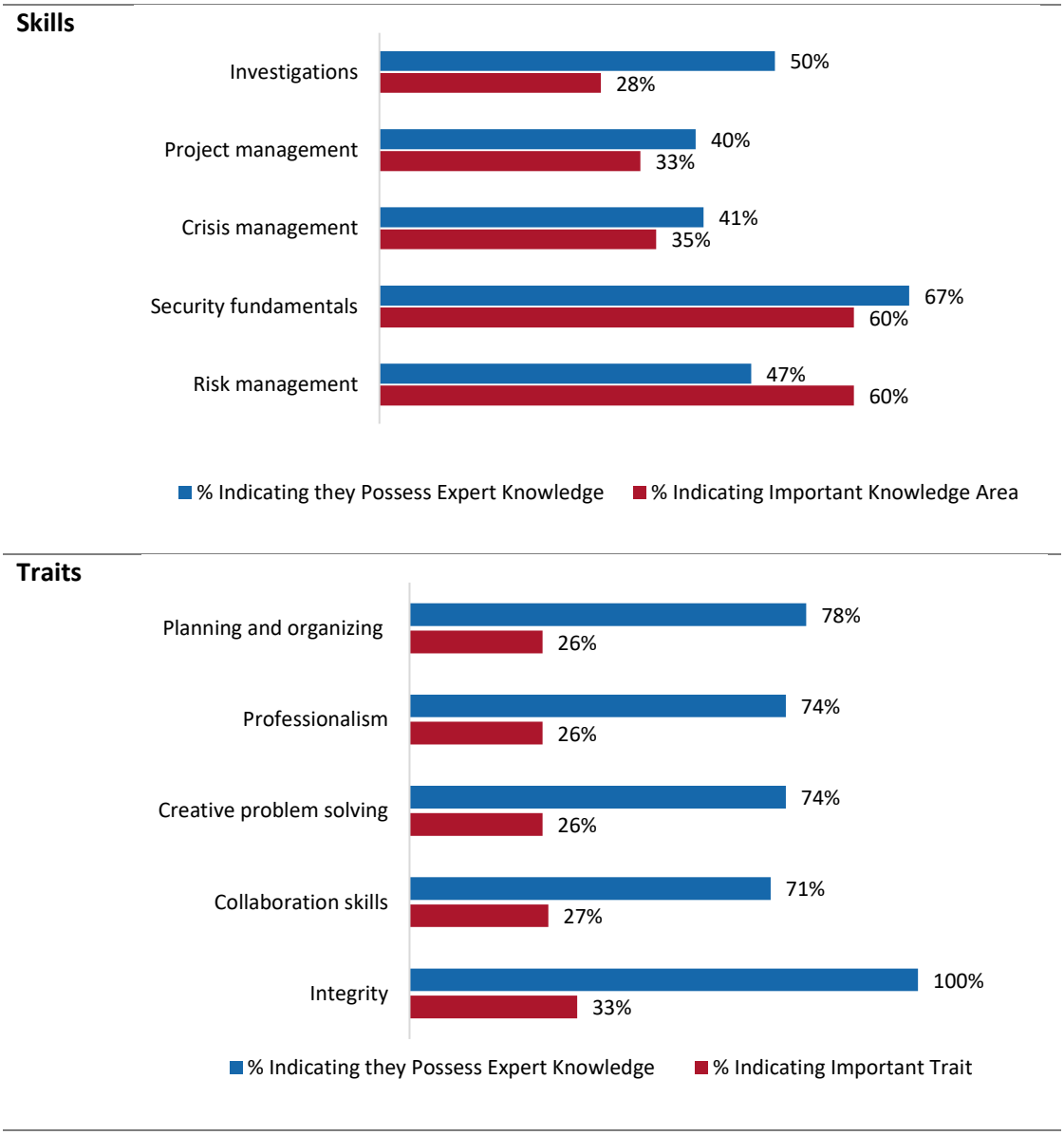
[8] Respondents were provided a unique list of skills and trait to rate according to their seniority level (professional, management/director, executive) as well as job role (practitioner, supplier). Although there was significant overlap between the lists, each list contained several unique items that was deemed relevant to the segment.

[9] Risk management was defined as "the ability to identify threats/risks and vulnerabilities taking into account the frequency, probability, speed of development, severity and reputational impact to achieve a holistic view across the enterprise." Security fundamentals was defined as "basic concepts involved in security and security management." Crisis management was defined as "understanding the process through which an enterprise deals with a critical incident or major event that threatens to harm the organization, its property, assets, systems, continuity or people." Project management was defined as "initiating, planning, executing, controlling, and closing the work of a team to achieve specific goals and meet specific success criteria at the specified time."

Additionally, practitioners identified integrity and leadership as important traits.[10] The selection and identification of these is not surprising, since they are tightly connected with the security field (and in many of the common occupational pathways into the field, such as law enforcement and military occupations). While integrity is required of any individual with access to sensitive information or tasked with protecting objects of value, it is also a cultural trait inherent in the security field. Additionally, strong leadership is required given the sometimes tense and chaotic environments and events in which security professionals may at times (frequently or occasionally) operate. The following section breaks down more specific competencies and skills by career stage/ position level.

Professional Level: Key competencies include knowledge of security fundamentals, investigation skills, integrity, collaboration, creative problem solving, professionalism, planning and organizing. Many (over 50%) indicate a knowledge deficit related to other key areas of project management, crisis management, and risk management skills. The graph below illustrates the skills and traits that practitioners at the professional level felt were most crucial. In terms of their own level of mastery, a majority felt as though they had expert knowledge of security fundamentals and investigations skills as well as traits that included integrity, collaboration skills, creative problem-solving ability, professionalism, and planning and organizing. The only top areas where less than 50% of professional level practitioners identified as experts included risk management, crisis management, and project management. It is notable that these three skills are considered crucial across all levels of responsibility. Practitioners at the professional level may benefit from professional development in these areas in order to increase their performance in their current roles as well as to help prepare those that intend to assume greater levels of responsibility in the future.

[10] Note that "risk management" was not included in the list of traits provided to self-identified executives, and "leadership" was not displayed as an option among practitioners at the professional level. However, both terms were among the most selected options by all others.



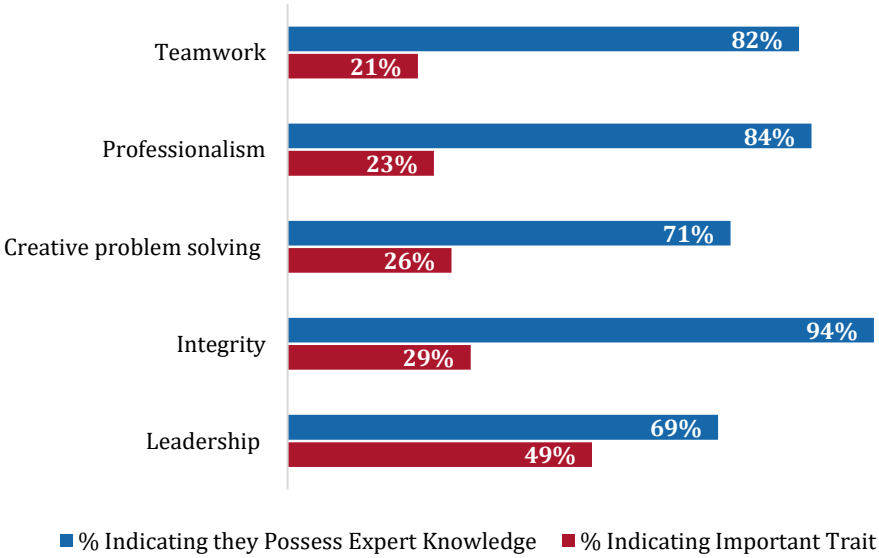
Management/Director Level: Key competencies include risk management, security fundamentals, subject matter expertise, executive management, leadership, and integrity. Many indicated a knowledge deficit in the areas of business acumen and compliance/ regulatory aspects. A majority of practitioners that hold jobs at the management/director level felt as though they possess expert knowledge in the crucial skill areas that are important in their roles. However, two important deficits surfaced: business acumen and compliance, legal and regulatory aspects.[11] Respondents were least likely to note mastery in these areas, and training may

[11] Business acumen was defined as "understanding of the business context of situations." Compliance, legal and regulatory aspects was defined as "developing and maintaining security policies, procedures, and practices, that comply with relevant elements of criminal, civil, administrative, and regulatory law to minimize adverse legal consequences)."

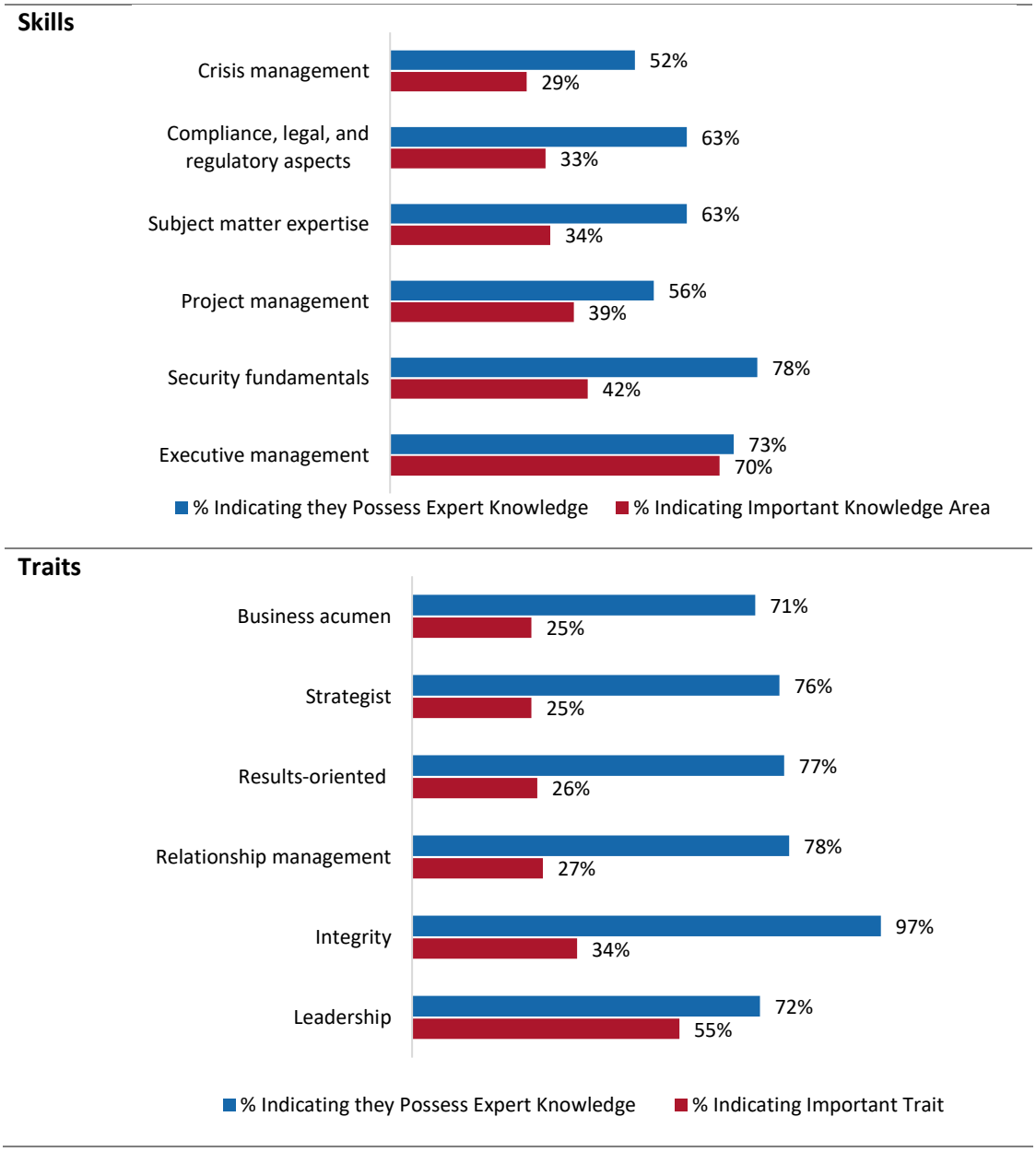
be beneficial since management/director level practitioners assume increasing levels of business-oriented responsibilities and may become engaged in a wider variety of organizational concerns.

Skills

Traits



Executive Level: Key competencies include executive management, security fundamentals, project management, leadership, and integrity. Executives may have opportunities to improve their project management and crisis management skills. Most executive level security management professionals felt as though they possessed expert-level knowledge for the top skills and traits required of their jobs. However, professionals in this group may appreciate additional resources to support their project management skills as well as knowledge of crisis management. It is worth noting that both skills are generally seen as important to practitioners of all levels of responsibility. In the case of executives, just over one-half of respondents that identified the skill area as important also felt as though they possessed expert knowledge.



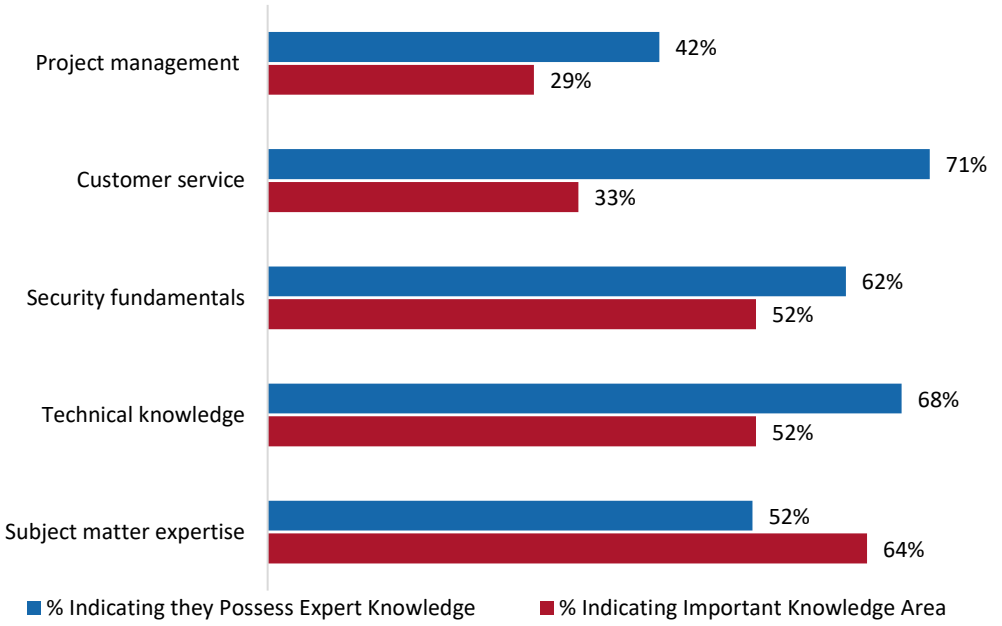
SUPPLIERS

Security industry suppliers identified many of the same essential skills and traits as practitioners: security fundamentals, project management, leadership, and integrity. However, they also pinpointed several skills that relate to their role in business development, including sales and business development, and customer service.[12] It is interesting to note that as the sales or business development function becomes increasingly important at higher levels of responsibility, there exists a corresponding level of importance placed on related skills.

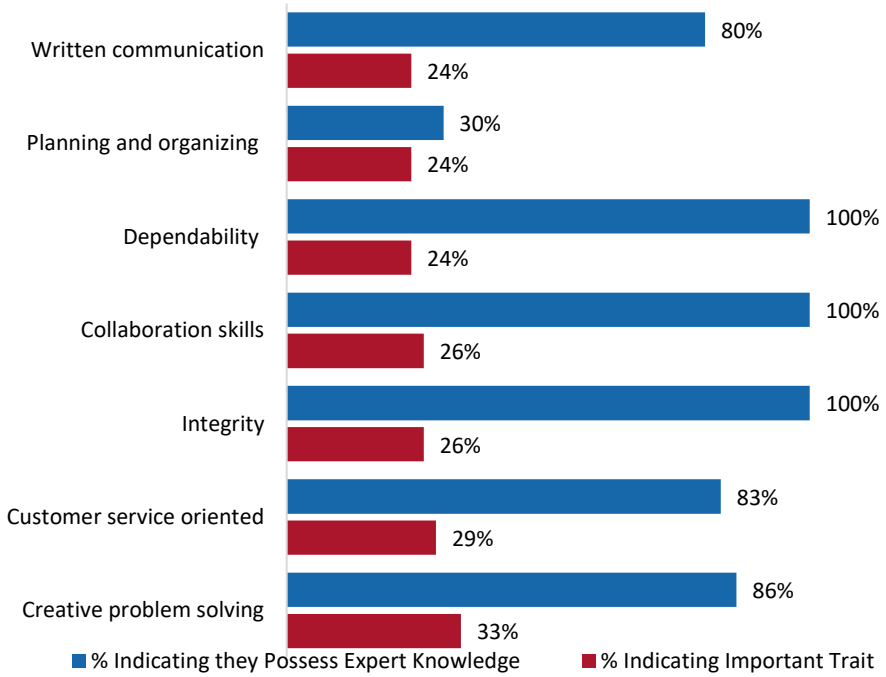
Professional Level: Key competencies include subject matter expertise, technical knowledge, security fundamentals, collaboration, and integrity. Knowledge deficits may occur related to project management skills as well as planning and organizational skills. A majority of security industry suppliers felt as though they had expert levels of knowledge in almost all areas they deemed as crucial to their jobs. However, only 42% felt as though they were proficient in project management – a skill not only seen as important to suppliers at various levels of responsibility but also for security management practitioners. Additionally, less than one-third (30%) felt that they possess expert planning and organizing skills. Taken together, professional level security industry suppliers, who may be in the position of managing multiple competing priorities and projects, may benefit from additional levels of project management training to perform at their best. Sales may also be part of the responsibilities required of a professional level supplier, depending on their area of focus.

[12] Sales and business development was defined as "ability to identify and prioritize sales targets and strategies, understand customer needs and respond with effective solutions/proposals." Customer service was defined as "the knowledge and ability to communicate and interact with customers and clients in a way that is sensitive to their situation, including their personality and needs)."

Skills



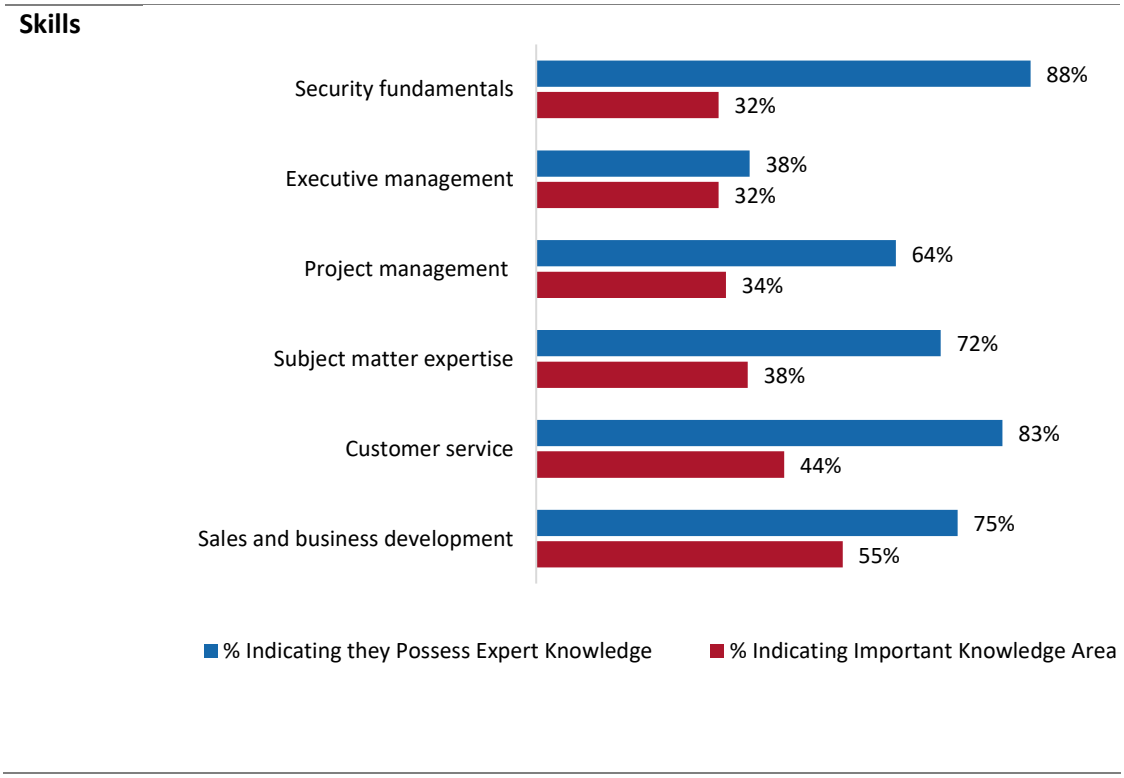
Traits



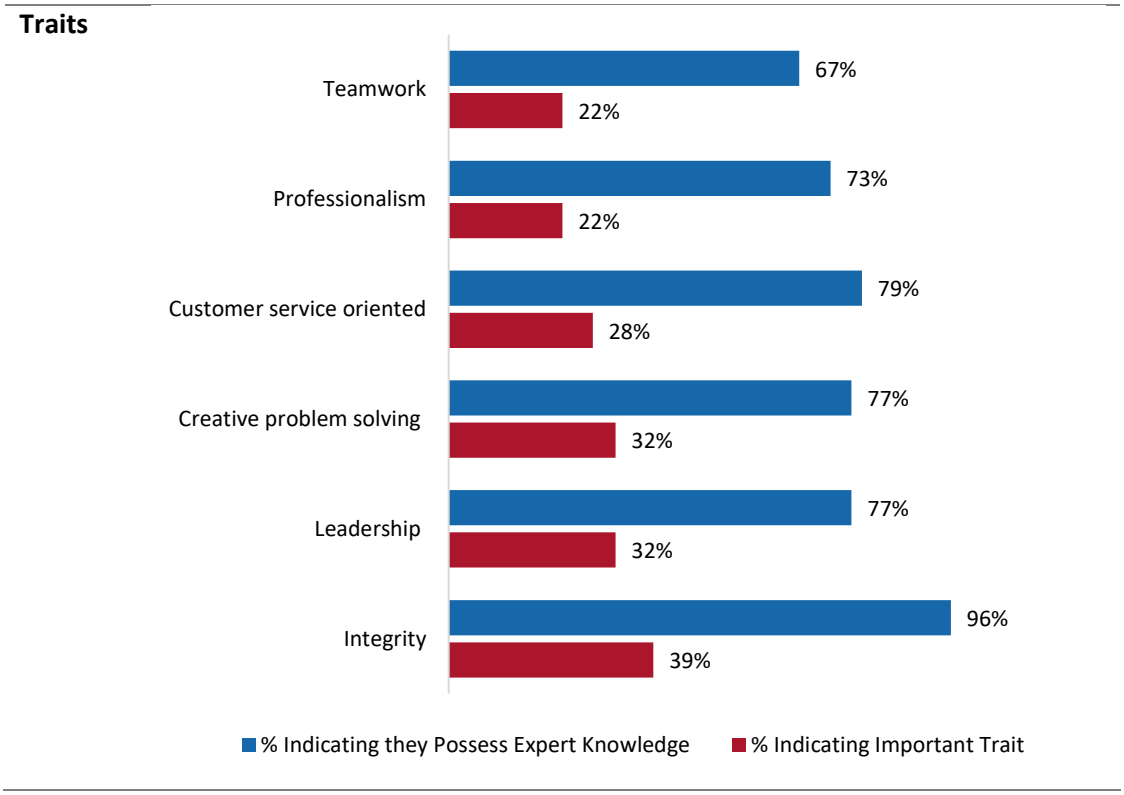
Management/Director Level: Key competencies include sales and business development, project management, customer service, subject matter expertise, security fundamentals, integrity, customer service orientation, and creative problem-solving skills.

Management/director level staff are less likely to indicate expertise in the area of executive management. Supplier personnel at the management/director level felt similar to professional level staff with respect to the importance of project management, customer service, subject matter expertise, security fundamentals, integrity, customer service orientation, and creative problem-solving skills. However, they were generally more likely than professional staff to identify themselves as experts in each area as well as responsible for management of teams of people.

The only skill where less than a majority of management/director level security industry supplier personnel felt as though they were experts was in executive management.[13] Just over one-third (38%) felt that they were fully proficient in this skill set. It is interesting to note that only 45% of suppliers at the executive level also felt as though they were experts in executive management – potentially suggesting the need for specific training for industry suppliers at the managerial or above levels of responsibility.



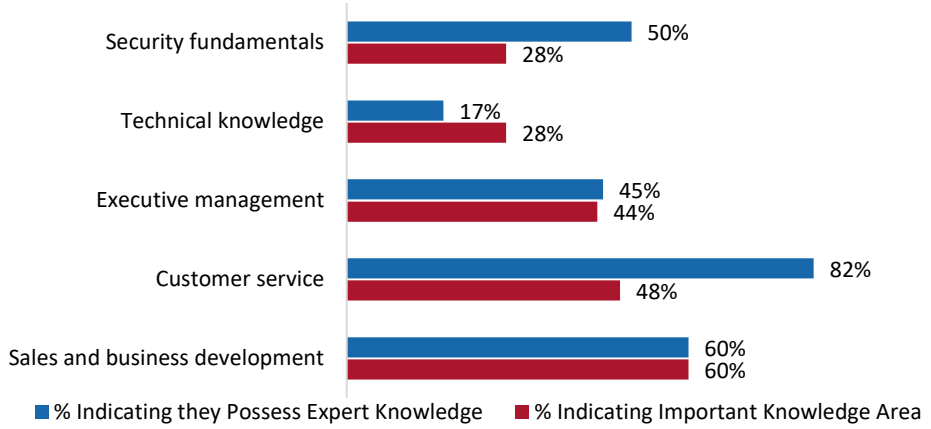
[13] Executive management was defined as "ability to build, motivate, and lead a professional team attuned to organizational culture."



Executive Level: Key competencies include sales and business development, customer service, executive management, leadership, and integrity. Executives note a need to enhance skills related to executive management as well as relationship management. Similar to management/director level suppliers, a minority of those at the executive level felt as though they possessed expert knowledge of executive management. Additionally, only 17% felt as though they were proficient with technical knowledge or relationship management.[14] It is important to note that the sample size of security industry suppliers (executive level) is fairly small at 25 participants, however; in an anecdotal sense, results from the survey suggest that supplier executives may benefit from training of relevant technical topics as well as executive management and relationship management.

[14] Technical knowledge was defined as "technical skills, hardware knowledge, network literacy, computer skills, electronics." Relationship management was defined as "developing, influencing and nurturing trust-based relationships with business unit leaders, government officials, and professional organizations)."

Skills



Traits

Domain Specific Knowledge

Regardless of level of responsibility, role or area of specialization/discipline, security management requires a broad understand of the principles of security and risk management, the ability to understand how your (or your client's) business operates and functions, and the skill to balance threats with practical solutions. However, organizations are complex and there are a variety of different forms of risk (e.g., cyber threats, workplace violence, loss prevention, intellectual property); it is not uncommon for security professionals to specialize in one or more specific disciplines. While this allows professionals to develop a high level of expertise in that area, it also may require a specialized background or skillset. For example, while professionals that specialize in executive protection may require law enforcement or military training, those in security technology systems may need a background in technology. Furthermore, professionals on the suppler side may require different knowledge sets based on the type of company they work for. This can vary by type of company, which can include: access control product manufacturer, door/lock/hardware manufacturer, intrusion product manufacturer, camera product manufacturer (hardware/software), cyber security manufacturer, logical access manufacturer, specialty product/ software manufacturer, service providers (system integrators, security alarm dealer, locksmith), distributors and wholesalers.

The tables on the following pages describes the background, skills and ability that may be associated with common disciplines in the security field. Note that these are generalizations provided by the text comments of practitioners and suppliers in each discipline. There are multiple positions within each discipline, some may require very specific and technical knowledge, while others may require a broader understanding. The level of expertise required of any professional may connect to both their professional levels of responsibility (professional, management/director, executive) as well as their job responsibilities (operations, installer/integrator, etc.).

Domain	*Practitioner*	*Supplier*
Access Control	• Practitioners may need to possess a general understanding of the needs of their organization and the available technologies to best support them. • Also important is the ability to identify, hire, and manage knowledgeable and capable vendors.	• Suppliers of access control technology may require an expert knowledge of the technology and product capabilities, as well as installation methods and integrations with other systems.
Asset Protection	• Practitioners may require an understanding of the assets protected, including their value, as well as an understanding of the methodologies used for protecting them (e.g., physical security). This may vary according to the type of asset under protection (e.g., hotel versus manufacturing unit).	• Like practitioners, suppliers must understand the asset under protection. They may also need to match the strengths and weaknesses of various systems against the protection circumstance (i.e., what type of system is most effective given the asset and its environment?).
Background Screening and Due Diligence	• Practitioners may require keen instincts and knowledge of interviewing or human behavior. • Intangibles such as the ability to form and maintain relationships with internal (e.g., human resources) and external (e.g., law enforcement) stakeholders may be crucial.	• In addition to knowledge of background screening and due diligence methods, it may also be necessary to hold an understanding of legal issues and requirements.
Brand Protection	• Practitioners may require a broad understanding of the brand and the areas that might impact it. This likely involves an enterprise risk perspective as well as knowledge of, and relationship to, other closely connected departments including public affairs, the legal department, etc.	• Suppliers may need to develop not only an understanding of the brand, but also how their security services connect with an overall risk strategy.
Business Continuity and Resilience	• Practitioners may require an in-depth understanding of business operations as well as how they relate to the strategic goals of the organization and need to prepare for security events and quick response.	• Suppliers may require an understanding of security systems and their strengths and weaknesses relative to the client business, as well as how threats and systems link to business outcomes.

Domain	*Practitioner*	*Supplier*
Communications / Awareness	• Practitioners must have knowledge of available modes of communication (what to use, required etiquette, etc.) for receiving and delivering information to internal and external audiences, as well as be able to develop strategic relationships and drive awareness to key stakeholders.	• Suppliers must have an understanding of communication technologies as well as have the ability to inform both technical and non-technical audiences.
Compliance	• Practitioners may require an understanding of regulatory and compliance standards, as well as how to implement check points and processes to ensure they are being met/satisfied within the organization.	• Suppliers may require an understanding of regulatory requirements for equipment.
Corporate Security	• Success in corporate security may require a detailed knowledge of the organization, and how security plugs into the business. This may require very broad-based understanding, including operations, finance, and other key areas of the organization.	• Like practitioners, suppliers may need a broad understanding of their clients' business.
Counter Terrorism and Counter Intelligence	• Practitioners may require understanding of counter terrorism approaches, as well as geo-political threats, current events and other regional situations. Collaboration and the ability to form relationships with external stakeholders (e.g., government entities) may be critical. • Counter terrorism and intelligence may require military, government, or relevant experience or training.	• Suppliers may have similar requirements to practitioners in exercising counter terrorism and counter intelligence – including knowledge of current and global events and expertise in performing the function.

Domain	*Practitioner*	*Supplier*
Crime Prevention	• Practitioners may benefit from a local presence and connection to the community, as well as the ability to form and maintain relationships with external stakeholder groups (e.g., local law enforcement). Specialized knowledge of crime prevention methods and approaches may also be required.	• Suppliers may require specialized knowledge of crime prevention methods and approaches.
Crisis Management	• Practitioners working in crisis management may require excellent communication skills, the ability to prepare and execute a plan during potential chaotic events, and the ability to maintain poise and control under those circumstances. • Planning and preparation abilities may also be critical in crisis management.	• Suppliers may need to develop an expert knowledge of emergency preparedness and planning, a complete understanding of their clients' business, and be able to pair optimal solutions to their needs.
Cyber Security	• A strong understanding of information technology, technology systems may be crucial, as is the ability to keep up-to-date on new threats and developments in the cyber security arena. • Practitioners may also require the ability to develop and maintain a strong and current understanding of technology vendors and their solutions, including the ability to evaluate those solutions relative to their organization's technology needs.	• Suppliers may require an expert level of knowledge in technology, programming, hacking, passwords and encryption, and other related areas. • Additionally, a knowledge of threat assessment and threat penetration may be critical.
Drug Detection	• Practitioners should be able to identify behaviors of individuals who are under the influence of drugs and other substances. Additionally, they should have knowledge of laws, legal issues, and dealing with crisis management. • The ability to form and maintain relationships with law enforcement is also valuable.	• Depending on their role, security industry suppliers may require similar knowledge, skills, and abilities to practitioners.

Domain	*Practitioner*	*Supplier*
Economic Crime and Fraud	• The ability to understand financial controls and fraud, how to identify fraudulent money and activities, and the ability to conduct interviews relative to the incident(s). • The ability to understand and review forensic report data.	• Suppliers should have an understanding of the methods and approaches used in economic crime and fraud detection. • Potentially require the ability to form relationships with banking institutions and law enforcement.
Emergency Management	• Practitioners should have knowledge of emergency management procedures, including an understanding of how to work and communicate within an incident command structure, and how to direct a team during an incident. • The ability to prepare for an incident, and work through an emergency (before, during and after) – including partnering with first responders when they arrive to the event may be critical. Also potentially crucial is a complete knowledge of the facility or environment. • Specific trainings (e.g., FEMA) may be required.	• Suppliers may require an understanding of the local or regional threats and issues, including applicable codes standards of practice and available resources for emergency response. They should also be able to evaluate the strengths and weaknesses of available systems and equipment.
Engineering and Design	• Practitioners may require technical expertise in multiple areas, including a broad ranging of architectural and engineering disciplines (e.g. construction, electrical engineering) as well as an understanding of availability technologies and standards of compliance. Business and leadership expertise, including budgeting, project management, and other related factors (e.g., the role of unions) may also be important.	• It is important for suppliers to develop a keen understanding of the clients' needs, including the particular risks and threats they face. Suppliers may also require a holistic understanding of systems, market trends and the technologies user in different industries. • Depending on their role, suppliers may need to have expert understanding of systems integration, as well as how to design a system to meet client needs. This may also require documentation and technical writing skills.

Domain	*Practitioner*	*Supplier*
Environmental Health	• Practitioners may require knowledge of environmental health codes and OSHA regulations, safety risks (e.g., chemicals, fires) and exposures, and safety equipment. They may also need to possess specific certifications and or specialized knowledge (e.g., chemical hazard protection).	• Like practitioners, suppliers working in the discipline of environmental health may require knowledge of the principals of health and safety, as well as relevant codes and regulations.
Executive Protection	• Practitioners may require tactical experience, experience in close personal protection and hold an understanding of relevant concepts (awareness of movement, cover, concealment, experience with firearms). • Real world experience may be crucial. May require relevant prior experience in law enforcement or military, as well as training in martial arts, firearms defense and other methods of protection.	• Depending on their role, suppliers may require the same expertise and skills as required of practitioners.
Financial Asset Protection	• Practitioners may require or benefit from prior experience in banking as well as business experience. Knowledge and understanding of financial crimes, fraud, accounting, access control, and cyber threats may also be required. • The ability to recognize and understand the value of the organization's assets and the related risk factors associated with them.	• Suppliers may require varying levels of knowledge and expertise in cyber security, data protection, physical security, and technology. • The ability to recognize and understand client's business needs and threats.
Government	• Practitioners should understand the unique aspects of government compared to the private or non-profit sector: laws, regulations, policies, as well as the underlying mission and decision-making process. This includes a broad understanding of how government operates.	• Similar to practitioners, suppliers should understand the unique nature of how government entities work and should be able to comply with relevant requirements (e.g., purchasing).

Domain	*Practitioner*	*Supplier*
Intellectual Property	• Practitioners may require knowledge of laws and data/information related to intellectual property.	• Suppliers may require an understanding of client's business and systems relative to intellectual property.
Intelligence	• Practitioners may need to hold knowledge or experience in investigations and data gathering methodologies. • The ability to understand what data points and intelligence are important versus which may not be meaningful.	• Suppliers may require a knowledge of data and intelligence gathering methodologies, as well as the information technology systems, management, guidelines, and policies used to support them. Prior background experience in intelligence may be helpful or necessary.
Investigations	• Practitioners may require background experience or knowledge of the investigation process, interrogation techniques, and undercover operations. • The ability to listen well, identify and ask meaningful questions and record/document responses.	• Suppliers may require similar knowledge as practitioners in the investigation process.
Information Technology	• Practitioners may require formal training or certification in information technology, information security, cyber security, and related areas. • The ability to work collaboratively with other departments and functions, and at different levels of seniority.	• Suppliers may require extensive background knowledge or training in information technology security, computer systems, computer programming and hacking, hardware technology and systems, network technology, and other technology.
Legal Compliance	• Practitioners should have knowledge of regulations as well as laws relative to business' locale(s). • Ability to understand legal implications of policies, events and actions.	• Similar to practitioners, suppliers should have understanding of liability, contracts, compliance, codes, and government regulations.
Loss Prevention	• Practitioners may require a total understanding of the business and its assets, as well as how loss may occur (internal versus external). • Ability to understand and implement controls and systems to prevent loss.	• Suppliers may require an understanding of clients' vulnerabilities as well as relevant systems (metal detecting, tag software systems, etc.). • Ability to stay current with crime trends.

Domain	*Practitioner*	*Supplier*
Personnel Security	• Practitioners may need a variety of interpersonal skills, including the ability to understand and work with people from different generations, cultures and backgrounds. Must be able to conduct background checks, screenings, interviews, and follow-ups. • Management and supervisory skills. Ability to understand and work within company culture.	• Suppliers should have understanding and expertise in systems and procedures for background checks and screenings.
Physical Security	• Experience in field operations, police training and/or certifications may be required. • Knowledge of a variety of areas may be required, such as risk management, information technology, budgeting, etc.	• In addition to current trends in crime, suppliers may need expertise in areas such as electronic systems and barriers (fences, etc.), intrusion detection, surveillance, access control, etc.
Public Safety	• Practitioners may require understanding and ability to keep up-to-date with current approaches and trends in public safety, including relevant standards (e.g., OSHA, FEMA). May require ability to develop and provide training to others. • The ability to form and maintain relationships with law enforcement and external stakeholders.	• Understanding and knowledge of public safety principles, threats and security management approaches. • Suppliers will benefit from understanding and knowledge of public safety systems related to their clients' needs and environments (e.g., campus communication systems, hospital security).
Risk Management	• Practitioners may require the ability to understand the many sources of risk impacting the environment as well as be able to prioritize the sources of risk. They may need to have or develop expertise in threat mitigation in areas related to priority areas.	• Suppliers may need a general understanding of risk management and the threats that impact the sectors they serve. They may also need an understanding of the process and systems in place to mitigate risks in their client businesses.

Domain	*Practitioner*	*Supplier*
Security Consulting	• Practitioners may require broad experience in security management to evaluate risk and threats. They may need to have a theoretical understanding of risk and security management approaches as well as a practical understanding of how security is applied in a variety of situations. • The ability to balance theoretical concerns with practical applications. • The ability to successfully match solutions to client or organization's business needs.	• Similar to practitioners, suppliers may need to have broad understanding (theoretical and practical) in security management. They may need to have great expertise in their area of specialty but must also be able to understand the client's broader needs and business context.
Security Education	• Up-to-date knowledge of security practices as well as the ability to present information clearly to adults. • An understanding of adult learning.	• The ability to present information to a variety of audiences that may have different technical backgrounds. • An in-depth understanding of the systems and technology subject matter.
Security Management	• General knowledge of security and security field, including the ways in which security fits into organization(s). • Experience in managing staff, or relevant training or certification.	• Understanding of security and security management principles, including relevant training or experience in management. • Knowledge of the types of solutions available in your area(s) of focus.
Security Operations	• In addition to a general understanding of security and risk management, should have broad knowledge and skillset that may include budgeting, human resources, databases/spreadsheets, contracting, compliance, etc. • The ability to work with upper management as well as other functions/roles within organization.	• Suppliers should possess both a broad understanding of client organization as well as how technology and systems will be understood, used and implemented within organization. This includes the technical component (programming, functionality) as well as human/operational side (who will be using the technology, what are their responsibilities).

Domain	*Practitioner*	*Supplier*
Security Systems	• Practitioners may require the ability to understand their organization (or client organization) business needs and match to appropriate technology or system. May require technical background and/or training. • The ability to stay current with security technology and knowledgeable about products available on the market.	• Expertise and knowledge of security systems on market, including new and developing technology. This may include product knowledge, an understanding of installation as well as knowledge of buildings. • A general or broad understanding of security and risk threats and principles, sufficient to understand client's needs and goals and determine appropriate solutions.
Security Technology	• Practitioners should have depth of understanding in the systems and technologies in place at organization. This may require a technical background in order to understand equipment, hardware, software, and programming. • The ability to stay current with new trends and technologies entering the marketplace.	• Suppliers may require understanding of security management and risk principles as well as available technologies and how best to match to client needs.
Supply Chain	• Specific and detailed understanding of the technical systems used in supply chain security management. The ability to understand, develop and design controls for supply chain. • Ability to understand contract and legal requirements, service level agreement, partnership with others involved in the supply chain.	• Similar to practitioners, suppliers must have detailed knowledge of the technical solutions and systems available for supply chain security. • The ability to understand client needs and match to available solutions.
Threat Assessment	• Practitioners may require an understanding of threat assessment and related approaches and methodologies. Should be able to understand and evaluate the nature of the business, assets, operating environments, competitors, and the impact that potential threats may have on the business.	• Suppliers may require similar skills, knowledge and experience as practitioners.

Domain	*Practitioner*	*Supplier*
Travel Risk Management	• Practitioners should understand the various threats that exist in different areas of the world, including political and social/cultural factors. Must have depth of understanding of world/regional issues and travel advisories.	• Suppliers may require similar skills, knowledge and experience as practitioners.
Video	• Practitioners may require technical background or training in systems and systems integration. May require depth of knowledge in CCTV management and dissemination protocols, technology changes, bandwidth management, network configurations, and privacy rules and policies.	• Suppliers should have understanding of systems and technologies, including ability to evaluate strengths and weaknesses of various systems. Understanding of optics, electronics, signal management, camera placement and data retrieval, etc. • The ability to match solutions to client's business needs.
Workplace	• Practitioners should have an understanding of the causes of workplace violence, prevention, response, training, and other principles of workplace security. • Understanding of relevant laws and the ability to stay current and up-to-date.	• Suppliers should have an understanding of workplace security as well as available technologies. • Understanding of legal issues related to workplace violence and security.

Career Development and Planning Your Next Steps

The following consideration points are offered to help professionals of all levels within the security field better understand how to prepare for, and advance, to higher levels of authority and responsibility in their careers.

1. **Establishing a career and pathway in the security field**: The security field is a diverse industry with many roles and domains of focus. Security professionals may enter into the field at different levels of responsibility (professional, management/director, executive) based on their education and experience.
    - **Education**: For both practitioners and suppliers, at every level of responsibility[15], it is most common to hold a bachelors or masters degree. And, while criminal justice-related and business degrees may be helpful in preparing all security professionals for their careers, those on the practitioner-side may benefit from social sciences

[15] Chart not included in report.

degrees while engineering and technical degrees may support those on the supplier side of the industry. However, regardless of level of responsibility, a strong majority of security professionals feel as though their background area of study was helpful in preparing them for their career.

- **Experience**: Many security industry personnel enter the field at the professional, management/director and even executive-levels. In fact, regardless of their level of responsibility, around 70%-80% of security industry professionals reported that their previous position was in the security field. Additionally, while those on the supplier side tend to come from a wider breadth of backgrounds, security practitioners (regardless of their level of responsibility) tend to enter the field with backgrounds in business, management, and administration, military service, and/or law enforcement.

Given that so many security practitioners and suppliers tend to have had previous jobs within the field – perhaps the most important pathway through the security field is through demonstrating dedication and high performance.

2. **Credentials and professional service can help:** In addition to performance, there are multiple options for a security professional to demonstrate their expertise, achieve leadership experience and show their commitment to being a better professional through engagement with the field. For example, nearly all security professionals that achieve relevant certifications (e.g., CPP, CSPM, PSP, PSI) find them to be important to those in their role, and since credentialing is typically seen as a way to both ensure expertise and demonstrate commitment – it may be a great stepping stone to additional responsibility. Additionally, many managers/directors and executives volunteer with industry associations (e.g., ASIS International, SIA) or serve as mentors to less experienced professionals. Participating in these types of activities is an excellent way to gain the type of leadership skills needed for higher levels of responsibility while also growing a network of connections.

3. **The skills that made you successful in your prior role won't be enough in the next**: Both practitioners and suppliers will need increasing levels of leadership and business skills as they transition from professional roles to management/director and executive-level responsibilities. This includes both a shift in their focus (thinking department and organization-wide, as opposed to task-focused) as well as a growing understanding in business functions (management, strategy, etc.). Compared to their previous role, new managers and directors are more likely to encounter responsibilities that include general management, planning and strategy, and budget and finance. Executives will in turn need to understand these elements, as well as the range of other business concerns, such as human resources, procurement, R&D, etc. Those with external clients and supplier side will also hold increasing responsibility over sales and business development.

4. **Professional development should be a priority for anyone aspiring to climb the "career ladder"**: Security field practitioners and suppliers need to build a range of

knowledge, skills, and abilities in each step along the career ladder. For example, practitioners aspiring to management/director roles may find that they are most in need of greater subject-matter expertise in their domain area; a broader understanding of risk management and general organization-wide security fundamentals; a growth in their grasp of business acumen and regulatory and compliance knowledge; and, general skills and abilities in executive management and leadership. The nuances between roles (practitioner, supplier) and levels of responsibilities (professional, manager/director, executive) are described in the "Competencies and Specialized Knowledge" section of this report. Professionals of every level should compare their own development against the core knowledge, skills and abilities required of peers at their level, and those at higher levels of authority. This provides a measurement against one's strengths and reveals opportunities and areas for future development.

5. **Flexibility and an openness to new challenges and domains may help to propel you through your career**: The security field represents many dozens of distinct domain areas (e.g., brand protection, compliance, executive protection). Professionals who are open to growing their knowledge-base and exploring other domain areas may not only find new opportunities and potentially, a better professional fit, but will also be expanding their breadth of knowledge in a field that is increasingly inter-connected between domain areas. This type of interdisciplinary/inter-domain knowledge may continue to grow in importance in the future, and thus make those who have a broad knowledge of domains more marketable and valuable within their organizations.

Appendix A: Select Questionnaire Results

1. In which country do you hold citizenship?

Respondents provided with a list of countries. Answers re-coded into United States versus Outside of United States below.

	PRACTITIONER		OTHER[16]		
	End-user (N = 912)	Provider (N = 364)	Law Enf. / Military / Intelligence (N = 135)	Instructor / Faculty (N = 31)	Consultant (N = 302)
United States	58%	54%	76%	45%	47%
Outside of USA	42%	46%	24%	55%	53%

	SUPPLIER			
	Distributor (N = 15)	Engineering / Design Consultant (N = 73)	Integrator (N = 91)	Manufacturer (N = 60)
United States	47%	56%	62%	70%
Outside of USA	53%	44%	38%	30%

[16] Note that the "other " category was composed of three distinct occupations that were determined to be unique in the focus of their work. This includes law enforcement/military/intelligence professionals, instructors in universities/colleges, and security or risk consultants. Instructors were composed of "instructors, faculty, or academicians in educational institutions." Security or risk consultants was composed of individuals that may hold roles in providing advice/counsel, technical experts, or some other role.

2. How would you classify your employer's business?

	PRACTITIONER		OTHER		
	End-user (N = 920)	Provider (N = 370)	Law Enf. / Military / Intelligence (N = 139)	Instructor / Faculty (N = 31)	Consultant (N = 313)
Public/Government	*22%*	*8%*	*89%*	*29%*	*7%*
Private Corporation	*68%*	*89%*	*10%*	*39%*	*88%*
Non-profit or NGO	*9%*	*2%*	*0%*	*23%*	*3%*
Other	*2%*	*1%*	*1%*	*10%*	*2%*

	SUPPLIER			
	Distributor (N = 16)	Engineering / Design Consultant (N = 73)	Integrator (N = 93)	Manufacturer (N = 62)
Public/Government	*19%*	*10%*	*13%*	*10%*
Private Corporation	*81%*	*84%*	*84%*	*90%*
Non-profit or NGO	*0%*	*1%*	*0%*	*0%*
Other	*0%*	*5%*	*3%*	*0%*

3. Please indicate the type of technology your company provides or deals in: please select all that apply. (Suppliers only)

	SUPPLIER			
	Distributor (N = 16)	Engineering / Design Consultant (N = 70)	Integrator (N = 93)	Manufacturer (N = 62)
Access control	*69%*	*84%*	*97%*	*63%*
Alarms/intrusion detection	*44%*	*77%*	*88%*	*34%*
Asset tracking	*44%*	*36%*	*33%*	*15%*
Identity management	*38%*	*64%*	*73%*	*24%*
Information technology	*56%*	*53%*	*40%*	*24%*
Life safety	*19%*	*39%*	*43%*	*21%*
Magnetometers	*0%*	*13%*	*13%*	*2%*
Perimeter protection	*38%*	*76%*	*65%*	*21%*
Scanners/x-ray machines	*6%*	*34%*	*26%*	*2%*
Video surveillance	*63%*	*80%*	*94%*	*53%*

4. In which sectors do you work? Please select all that apply.

	PRACTITIONER		OTHER		
	End-user (N = 857)	Provider (N = 344)	Law Enf. / Military / Intelligence (N = 124)	Instructor / Faculty (N = 25)	Consultant (N = 286)
Banking, finance and insurance	*18%*	*31%*	*2%*	*4%*	*52%*
Business services	*3%*	*24%*	*2%*	*4%*	*44%*
Construction	*5%*	*27%*	*3%*	*4%*	*41%*
Corporate	*21%*	*51%*	*6%*	*8%*	*68%*
Critical infrastructure	*12%*	*29%*	*17%*	*8%*	*50%*
Education or school system	*7%*	*28%*	*9%*	*84%*	*45%*
Food and agriculture	*3%*	*18%*	*2%*	*4%*	*26%*
Food service	*2%*	*17%*	*2%*	*0%*	*21%*
Gaming and wagering	*2%*	*12%*	*2%*	*0%*	*23%*
Government	*16%*	*30%*	*52%*	*12%*	*58%*
Healthcare	*10%*	*26%*	*3%*	*8%*	*40%*
Homeland/national security	*7%*	*23%*	*40%*	*8%*	*40%*
Information	*7%*	*18%*	*7%*	*20%*	*27%*
Law enforcement and intelligence	*5%*	*21%*	*75%*	*12%*	*38%*
Leisure, hospitality and entertainment	*6%*	*27%*	*6%*	*4%*	*40%*
Manufacturing and distribution	*12%*	*26%*	*4%*	*0%*	*44%*
Military	*2%*	*15%*	*23%*	*8%*	*27%*
Museums and cultural properties	*3%*	*20%*	*4%*	*0%*	*31%*
Natural resources and mining	*30%*	*14%*	*3%*	*0%*	*30%*
Non-governmental organizations (NGOs)	*3%*	*19%*	*2%*	*4%*	*35%*
Non-profit	*6%*	*17%*	*5%*	*8%*	*32%*
Petrochemical, chemical, and/or extractive ind.	*7%*	*21%*	*4%*	*0%*	*41%*
Pharmaceutical industry	*5%*	*19%*	*2%*	*0%*	*35%*

Real estate	*4%*	*23%*	*3%*	*4%*	*29%*
Religious organizations	*2%*	*17%*	*3%*	*0%*	*31%*
Transportation and/or warehousing	*8%*	*28%*	*5%*	*0%*	*43%*
Utilities	*7%*	*19%*	*2%*	*4%*	*37%*
Wholesale and/or retail trade	*6%*	*24%*	*3%*	*0%*	*32%*
Other	*7%*	*20%*	*5%*	*16%*	*19%*

5. In which sectors do you provider services or technology? Please select all that apply.

	SUPPLIER			
	Distributor (N = 16)	Engineering / Design Consultant (N = 65)	Integrator (N = 85)	Manufacturer (N = 57)
Banking, finance and insurance	*75%*	*43%*	*62%*	*82%*
Business services	*63%*	*31%*	*51%*	*60%*
Construction	*56%*	*65%*	*65%*	*74%*
Corporate	*75%*	*66%*	*72%*	*82%*
Critical infrastructure	*75%*	*65%*	*59%*	*84%*
Education or school system	*50%*	*55%*	*64%*	*81%*
Food and agriculture	*44%*	*28%*	*36%*	*61%*
Food service	*44%*	*17%*	*35%*	*54%*
Gaming and wagering	*44%*	*25%*	*29%*	*74%*
Government	*69%*	*77%*	*69%*	*93%*
Healthcare	*56%*	*51%*	*68%*	*81%*
Homeland/national security	*63%*	*42%*	*40%*	*84%*
Information	*75%*	*22%*	*31%*	*54%*
Law enforcement and intelligence	*69%*	*45%*	*35%*	*77%*
Leisure, hospitality and entertainment	*63%*	*49%*	*53%*	*75%*
Manufacturing and distribution	*69%*	*38%*	*60%*	*77%*
Military	*56%*	*37%*	*38%*	*77%*
Museums and cultural properties	*56%*	*45%*	*53%*	*75%*
Natural resources and mining	*56%*	*22%*	*31%*	*63%*
Non-governmental organizations (NGOs)	*63%*	*20%*	*32%*	*63%*
Non-profit	*38%*	*17%*	*35%*	*65%*
Petrochemical, chemical, and/or extractive ind.	*69%*	*35%*	*55%*	*77%*
Pharmaceutical industry	*69%*	*34%*	*47%*	*75%*

Real estate	*56%*	*38%*	*48%*	*70%*
Religious organizations	*44%*	*25%*	*44%*	*70%*
Transportation and/or warehousing	*69%*	*57%*	*60%*	*86%*
Utilities	*56%*	*46%*	*61%*	*81%*
Wholesale and/or retail trade	*69%*	*31%*	*42%*	*65%*
Other	*31%*	*12%*	*18%*	*44%*

6. Which of the following security disciplines are areas of focus in your work? Please select all that apply.

	PRACTITIONER		OTHER		
	End-user (N = 857)	Provider (N = 344)	Law Enf. / Military / Intelligence (N = 124)	Instructor / Faculty (N = 25)	Consultant (N = 286)
Access control	*86%*	*69%*	*60%*	*32%*	*62%*
Asset protection	*78%*	*69%*	*57%*	*32%*	*60%*
Background screening and due diligence	*43%*	*36%*	*46%*	*12%*	*44%*
Brand protection	*36%*	*21%*	*10%*	*12%*	*30%*
Business continuity and resilience	*56%*	*38%*	*29%*	*24%*	*61%*
Communications/awareness	*46%*	*32%*	*31%*	*28%*	*42%*
Compliance	*44%*	*36%*	*32%*	*16%*	*46%*
Corporate security	*74%*	*63%*	*31%*	*24%*	*70%*
Counterterrorism and counter intelligence	*29%*	*25%*	*50%*	*12%*	*48%*
Crime prevention	*56%*	*50%*	*49%*	*28%*	*59%*
Crisis management	*67%*	*48%*	*51%*	*40%*	*63%*
Cyber security and cyber crime	*25%*	*17%*	*34%*	*20%*	*35%*
Drug detection/interdiction	*16%*	*18%*	*20%*	*8%*	*18%*
Economic crime and fraud	*23%*	*19%*	*24%*	*8%*	*28%*
Emergency management	*61%*	*47%*	*50%*	*40%*	*57%*
Engineering and design	*24%*	*21%*	*11%*	*8%*	*37%*
Environmental health and safety	*29%*	*27%*	*9%*	*16%*	*26%*
Executive protection	*47%*	*44%*	*34%*	*12%*	*43%*
Financial asset protection	*21%*	*21%*	*10%*	*8%*	*24%*
Government	*21%*	*24%*	*63%*	*20%*	*35%*
Intellectual property	*23%*	*20%*	*10%*	*8%*	*27%*

Intelligence (information)	*35%*	*26%*	*48%*	*8%*	*44%*
Investigations	*63%*	*49%*	*63%*	*20%*	*46%*
IT security	*20%*	*20%*	*25%*	*12%*	*32%*
Legal compliance	*24%*	*19%*	*23%*	*16%*	*28%*
Loss prevention	*51%*	*47%*	*24%*	*12%*	*47%*
Personnel security	*64%*	*62%*	*53%*	*40%*	*55%*
Physical security	*86%*	*77%*	*69%*	*56%*	*70%*
Public safety	*32%*	*37%*	*53%*	*24%*	*37%*
Risk management	*62%*	*54%*	*53%*	*52%*	*77%*
Security consulting	*31%*	*62%*	*34%*	*32%*	*88%*
Security education or training	*62%*	*56%*	*53%*	*72%*	*70%*
Security management	*76%*	*70%*	*55%*	*36%*	*74%*
Security operations	*75%*	*74%*	*57%*	*36%*	*81%*
Security systems	*68%*	*49%*	*37%*	*24%*	*49%*
Security technology	*54%*	*43%*	*33%*	*24%*	*47%*
Supply chain	*23%*	*21%*	*13%*	*8%*	*32%*
Threat assessment	*66%*	*52%*	*65%*	*44%*	*72%*
Travel risk management	*44%*	*28%*	*32%*	*24%*	*45%*
Video surveillance	*64%*	*46%*	*33%*	*16%*	*46%*
Workplace violence	*62%*	*42%*	*36%*	*36%*	*46%*

7. Please indicate which security discipline(s) you provide services or technology to in your work: Please select all that apply.

	SUPPLIER			
	Distributor (N = 16)	Engineering / Design Consultant (N = 65)	Integrator (N = 85)	Manufacturer (N = 57)
Access control	*88%*	*92%*	*95%*	*75%*
Asset protection	*50%*	*55%*	*47%*	*44%*
Background screening and due diligence	*44%*	*17%*	*9%*	*14%*
Brand protection	*31%*	*12%*	*12%*	*21%*
Business continuity and resilience	*38%*	*32%*	*26%*	*25%*
Communications/awareness	*38%*	*32%*	*31%*	*37%*
Compliance	*63%*	*31%*	*22%*	*37%*
Corporate security	*63%*	*48%*	*39%*	*42%*
Counterterrorism and counter intelligence	*25%*	*23%*	*11%*	*28%*
Crime prevention	*44%*	*37%*	*27%*	*37%*
Crisis management	*38%*	*17%*	*19%*	*25%*
Cyber security and cyber crime	*50%*	*37%*	*26%*	*28%*
Drug detection/interdiction	*25%*	*14%*	*8%*	*16%*
Economic crime and fraud	*31%*	*12%*	*11%*	*16%*
Emergency management	*25%*	*25%*	*21%*	*28%*
Engineering and design	*63%*	*88%*	*65%*	*51%*
Environmental health and safety	*25%*	*18%*	*18%*	*30%*
Executive protection	*38%*	*15%*	*12%*	*19%*
Financial asset protection	*38%*	*12%*	*13%*	*25%*
Government	*50%*	*42%*	*24%*	*30%*
Intellectual property	*31%*	*14%*	*9%*	*18%*
Intelligence (information)	*38%*	*15%*	*14%*	*23%*
Investigations	*31%*	*14%*	*11%*	*18%*
IT security	*50%*	*32%*	*33%*	*40%*

Legal compliance	*31%*	*17%*	*11%*	*21%*
Loss prevention	*44%*	*29%*	*34%*	*46%*
Personnel security	*56%*	*26%*	*21%*	*26%*
Physical security	*63%*	*82%*	*72%*	*63%*
Public safety	*50%*	*26%*	*25%*	*32%*
Risk management	*44%*	*48%*	*29%*	*39%*
Security consulting	*56%*	*85%*	*60%*	*40%*
Security education or training	*56%*	*32%*	*39%*	*33%*
Security management	*50%*	*35%*	*42%*	*30%*
Security operations	*56%*	*28%*	*39%*	*35%*
Security systems	*75%*	*74%*	*80%*	*65%*
Security technology	*69%*	*72%*	*72%*	*60%*
Supply chain	*38%*	*12%*	*12%*	*19%*
Threat assessment	*38%*	*54%*	*27%*	*19%*
Travel risk management	*31%*	*15%*	*12%*	*14%*
Video surveillance	*63%*	*85%*	*79%*	*51%*
Workplace violence	*38%*	*20%*	*18%*	*25%*

8. Which of the following best describes your current job level?

	PRACTITIONER		OTHER		
	End-user (N = 843)	Provider (N = 340)	Law Enf. / Military / Intelligence (N = 123)	Instructor / Faculty (N = 25)	Consultant (N = 284)
Executive	*7%*	*26%*	*11%*	*16%*	*36%*
Management	*74%*	*59%*	*56%*	*44%*	*38%*
Professional	*17%*	*11%*	*26%*	*32%*	*21%*
Other/unsure	*2%*	*5%*	*7%*	*8%*	*4%*

	SUPPLIER			
	Distributor (N = 16)	Engineering / Design Consultant (N = 64)	Integrator (N = 84)	Manufacturer (N = 57)
Executive	*31%*	*14%*	*17%*	*26%*
Management	*38%*	*42%*	*49%*	*51%*
Professional	*25%*	*44%*	*33%*	*16%*
Other/unsure	*6%*	*0%*	*1%*	*7%*

9. Which of the following responsibilities do you have as part of your job? Please select all that apply

	PRACTITIONER		OTHER		
	End-user (N = 720)	Provider (N = 306)	Law Enf. / Military / Intelligence (N = 106)	Instructor / Faculty (N = 25)	Consultant (N = 260)
Budget and finance	61%	54%	39%	28%	58%
Compliance	61%	52%	46%	28%	49%
Consultant/advisor	51%	58%	38%	48%	85%
Engineering and/or design	23%	10%	9%	16%	27%
Executive protection	39%	23%	22%	12%	25%
General mgmt (incl personnel, planning, etc.)	57%	60%	36%	40%	51%
Human resources	14%	38%	19%	16%	22%
Information technology (IT) and security	16%	10%	18%	12%	22%
Instruction/education	50%	41%	44%	68%	50%
Investigations/intelligence	69%	47%	67%	28%	44%
Law enforcement/policing	14%	11%	64%	12%	10%
Legal advice and counsel	8%	8%	5%	8%	12%
Marketing and/or marketing research/analytics	3%	19%	1%	8%	26%
Parking and transportation	22%	12%	12%	20%	8%
Procurement and contracting	29%	21%	19%	12%	25%
Program or project manager	38%	30%	33%	36%	42%
Research and development (R&D)	9%	10%	8%	20%	18%
Risk management	61%	54%	57%	40%	74%
Sales and business development	2%	39%	3%	8%	41%
Security mgmt. (sec ops, planning, etc.)	83%	73%	58%	32%	64%
Security ops. (monitoring, resp to threats, etc.)	78%	61%	58%	28%	48%
Strategy and planning	56%	49%	51%	36%	62%
Supply chain and distribution	13%	10%	3%	8%	12%
Technician/tech resp. (e g , inst, maintenance)	17%	9%	9%	4%	13%
Travel	34%	15%	22%	16%	32%
Other	2%	1%	2%	4%	1%

10. Which of the following responsibilities do you have as part of your job? Please select all that apply.

	SUPPLIER			
	Distributor (N = 14)	Engineering / Design Consultant (N = 57)	Integrator (N = 78)	Manufacturer (N = 48)
Budget and finance	57%	56%	49%	35%
Compliance	43%	32%	38%	23%
Consultant/advisor	43%	86%	59%	38%
Engineering and/or design	43%	86%	68%	38%
Executive protection	7%	5%	4%	2%
General management (including personnel, planning, etc.)	43%	37%	44%	35%
Human resources	21%	12%	13%	10%
Information technology (IT) and security	21%	35%	24%	15%
Instruction/education	29%	19%	35%	17%
Investigations/intelligence	14%	11%	8%	4%
Law enforcement/policing	14%	0%	5%	0%
Legal advice and counsel	14%	5%	5%	2%
Marketing and/or marketing research/analytics	29%	18%	23%	44%
Parking and transportation	0%	7%	8%	0%
Procurement and contracting	7%	25%	23%	4%
Program or project manager	29%	39%	45%	19%
Research and development (R&D)	21%	12%	13%	10%
Risk management	29%	42%	24%	8%
Sales and business development	79%	46%	67%	90%
Security management (managing sec. ops, planning, etc.)	14%	21%	35%	8%
Security operations (monitoring, responding to threats, etc.)	29%	16%	19%	2%

Strategy and planning	50%	40%	37%	58%
Supply chain and distribution	29%	7%	10%	4%
Technician/technical resp. (e.g., installation, maintenance)	29%	19%	36%	10%
Travel	36%	16%	18%	13%
Other	0%	0%	0%	0%

11. Below is a list of general knowledge areas typically required of many or most professionals in the security field at your level of responsibility/seniority. Regardless of your personal knowledge level in each area, please indicate the top three most important areas required of someone in your role. Please select up to three options.

EXECUTIVE LEVEL

(INSTRUCTOR NOT INCLUDED, CONSULTANT REPORTED IN SUPPLIER TABLES)	PRACTITIONER		OTHER
	End-user (N = 36)	Provider (N = 57)	Law Enf. / Military / Intelligence (N = 9)
Case management (understanding the systems to manage, analyze, report and present findings from investigations)	*3%*	*12%*	*11%*
Compliance, legal and regulatory aspects (developing and maintaining security policies, procedures, and practices, that comply with relevant elements of criminal, civil, administrative and regulatory law to minimize adverse legal consequences)	*39%*	*28%*	*44%*
Crisis management (understanding the process through which an enterprise deals with a critical incident or major event that threatens to harm the organization, its property, assets, systems, continuity or people)	*42%*	*21%*	*56%*
Executive management (ability to build, motivate, and lead a professional team attuned to organizational culture)	*72%*	*67%*	*78%*
Investigations (understanding the methodology the organization undertakes to collect and preserve information in reports to enable the enterprise to make reliable decisions in response to situations)	*17%*	*14%*	*22%*
Project management (initiating, planning, executing, controlling, and closing the work of a team to achieve specific goals and meet specific success criteria at the specified time)	*42%*	*37%*	*11%*
Security fundamentals (understanding the basic concepts involved in security and security management)	*25%*	*53%*	*22%*

Subject matter expertise (providing or seeing to the provision of technical expertise appropriate to knowledge of risk, security, and the cost-effective delivery of mitigation solutions)	*33%*	*33%*	*56%*
Tools and technology (selecting, using and maintaining tools and technology to facilitate work activity)	*3%*	*12%*	*0%*
Vendor management (identifying, vetting and managing vendors and suppliers)	*3%*	*2%*	*0%*
Other	*6%*	*2%*	*0%*

12. Below is a list of general knowledge areas typically required of many or most professionals in the security field at your level of responsibility/seniority. Regardless of your personal knowledge level in each area, please indicate the top three most important areas required of someone in your role. Please select up to three options.

MANAGEMENT LEVEL

(INSTRUCTOR NOT INCLUDED, CONSULTANT REPORTED IN SUPPLIER TABLES)	PRACTITIONER		OTHER
	End-user (N = 336)	Provider (N = 117)	Law Enf. /Military / Intelligence (N = 39)
Business acumen (understanding basic business principles, trends, and economics)	*23%*	*30%*	*15%*
Case management (understanding the systems to manage, analyze, report and present findings from investigations)	*5%*	*8%*	*23%*
Compliance, legal and regulatory aspects (developing and maintaining security policies, procedures, and practices, that comply with relevant elements of criminal, civil, administrative and regulatory law to minimize adverse legal consequences)	*27%*	*29%*	*36%*
Crisis management (understanding the process through which an enterprise deals w/ critical incident or major event that threatens to harm the org., its property, assets, systems, continuity or people)	*28%*	*16%*	*23%*
Executive management (ability to build, motivate, and lead a prof. team attuned to org. culture)	*28%*	*44%*	*23%*
Investigations (understanding the methodology the organization undertakes to collect and preserve info. in reports to enable the enterprise to make reliable deci. in response to situations effectively)	*14%*	*9%*	*33%*
Project management (initiating, planning, executing, controlling, and closing the work of a team to achieve specific goals and meet specific success criteria at the specified time)	*21%*	*35%*	*21%*

Risk management (ability to identify threats/risks and vulnerabilities taking into account the frequency, probability, speed of development, severity and reputational impact to achieve a holistic view across the entity)	*43%*	*38%*	*33%*
Security fundamentals (understanding the basic concepts involved in security and security management)	*40%*	*38%*	*26%*
STEM competency (e g , ability to use scientific approaches to solve problems, understanding technology used in your work, ability to develop/design/enhance security systems, ability to use mathematics to understand performance metrics, budgets, etc.)	*7%*	*3%*	*8%*
Subject matter expertise (providing or seeing to the provision of technical expertise appropriate to knowledge of risk, security, and the cost-effective delivery of mitigation solutions)	*39%*	*30%*	*38%*
Tools and technology (selecting, using and maintaining tools and tech. to facilitate work activity)	*9%*	*8%*	*3%*
Vendor management (identifying, vetting and managing vendors and suppliers)	*7%*	*3%*	*0%*
Other	*1%*	*4%*	*0%*

13. Below is a list of general knowledge areas typically required of many or most professionals in the security field at your level of responsibility/seniority. Regardless of your personal knowledge level in each area, please indicate the top three most important areas required of someone in your role. Please select up to three options.

PROFESSIONAL LEVEL

(INSTRUCTOR NOT INCLUDED, CONSULTANT REPORTED IN SUPPLIER TABLES)	PRACTITIONER		OTHER
	End-user (N = 74)	Provider (N = 20)	Law Enf. /Military / Intelligence (N = 20)
Business acumen (understanding basic business principles, trends, and economics)	*16%*	*20%*	*15%*
Case management (understanding the systems to manage, analyze, report and present findings from investigations)	*15%*	*20%*	*25%*
Crisis management (understanding the process through which an enterprise deals with a critical incident or major event that threatens to harm the organization, its property, assets, systems, continuity or people)	*31%*	*50%*	*25%*
Investigations (understanding the methodology the organization undertakes to collect and preserve information in reports to enable the enterprise to make reliable decisions in response to situations)	*30%*	*20%*	*35%*
Project management (initiating, planning, executing, controlling, and closing the work of a team to achieve specific goals and meet specific success criteria at the specified time)	*36%*	*20%*	*30%*
Risk management (ability to identify threats/risks and vulnerabilities taking into account the frequency, probability, speed of development, severity and reputational impact to achieve a holistic view across the entity)	*58%*	*65%*	*45%*
Security fundamentals (understanding and applying the basic security principles to the security of the enterprise or a specific structure, system or process)	*62%*	*50%*	*70%*

STEM competency (e g , ability to use scientific approaches to solve problems, understanding technology used in your work, ability to develop/design/enhance security systems, ability to use mathematics to understand performance metrics, budgets, etc.)	*9%*	*0%*	*15%*
Tools and technology (selecting, using and maintaining tools and technology to facilitate work activity)	*22%*	*10%*	*15%*
Vendor management (identifying, vetting and managing vendors and suppliers)	*7%*	*15%*	*10%*
Other	*1%*	*5%*	*0%*

14. Below is a list of general knowledge areas typically required of many or most professionals in the security field at your level of responsibility/seniority. Regardless of your personal knowledge level in each area, please indicate the top three most important areas required of someone in your role. Please select up to three options.

ALL LEVELS	**OTHER**	**SUPPLIER**			
(SUPPLIER LEVELS OF RESPONSIBILITY MERGED FOR REPORTING	Consultant (N = 193)	Distributor (N = 10)	Engineering / Design Consultant (N = 43)	Integrator (N = 59)	Manufacturer (N = 37)
Business acumen (understanding basic business principles, trends, and economics)	*27%*	*0%*	*26%*	*15%*	*24%*
Customer service (the knowledge and ability to communicate and interact with customers and clients in a way that is sensitive to their situation, including their personality and needs)	*40%*	*50%*	*40%*	*46%*	*35%*
Executive management (ability to build, motivate, and lead a professional team attuned to organizational culture)	*33%*	*40%*	*14%*	*31%*	*30%*
Information technology expertise (technical expertise in systems design, systems architecture, etc.)	*4%*	*0%*	*7%*	*14%*	*5%*
Project management (initiating, planning, executing, controlling, and closing the work of a team to achieve specific goals and meet specific success criteria at the specified time)	*42%*	*10%*	*42%*	*32%*	*22%*
Sales and business development (ability to identify and prioritize sales targets and strategies, understand customer needs and respond with effective solutions/proposals)	*18%*	*60%*	*19%*	*39%*	*86%*
Security fundamentals (understanding the basic concepts involved in security and security management)	*47%*	*30%*	*49%*	*34%*	*27%*

Subject matter expertise (technical expertise appropriate to knowledge of risk, security, and the cost-effective delivery of mitigation solutions)	*58%*	*20%*	*58%*	*39%*	*35%*
Technical knowledge (technical skills, hardware knowledge, network literacy, computer skills, electronics)	*12%*	*30%*	*37%*	*37%*	*30%*
Vendor management (identifying, vetting and managing vendors and suppliers)	*5%*	*30%*	*5%*	*8%*	*3%*
Other	*2%*	*0%*	*0%*	*2%*	*0%*

15. Below is a list of common professional traits required of many or most professionals in the security field at your level of responsibility/seniority. Regardless of your personal skill level in each area, please indicate the most important top three traits required of someone in your role. Please select up to three options.

EXECUTIVE LEVEL (EMPLOYER TYPES MERGED FOR REPORTING)	TOTAL (N = 183)
Adaptability (demonstrating unique ways of thinking, being open to new ideas, dealing with ambiguity)	*17%*
Business acumen (understanding of the business context of situations)	*25%*
Collaboration skills (ability to work effectively with individuals and teams)	*17%*
Dedication / "cultural fit" (loyalty to your job/organization, acting harmoniously within organization)	*9%*
Digital/technology skills (understanding of computer technology and information systems)	*2%*
Integrity (ethical behavior, acting fairly, taking responsibility)	*42%*
Leadership (building, motivating, and leading a professional team attuned to the organizational culture, responsive to business needs, and committed to integrity and excellence)	*45%*
Negotiation skills (ability to work towards a mutually acceptable outcome between two or more parties)	*13%*
Planning and organizing (managing your time effectively, prioritizing responsibilities, project management)	*22%*
Relationship management (developing, influencing and nurturing trust-based relationships with business unit leaders, government officials, and professional organizations)	*32%*
Results-oriented (focusing on the outcome and "making things happen")	*23%*
Strategist (generating innovative and creative solutions, providing vision and developing goals)	*25%*
Teamwork (demonstrating concern for others, insight into other's behavior, having open communication, showing respect for diversity, resolving conflicts)	*21%*
Other	*1%*

16. Below is a list of common professional traits required of many or most professionals in the security field at your level of responsibility/seniority. Regardless of your personal skill level in each area, please indicate the most important top three traits required of someone in your role. Please select up to three options.

MANAGEMENT LEVEL (EMPLOYER TYPES MERGED FOR REPORTING)	TOTAL (N = 615)
Adaptability (demonstrating unique ways of thinking, being open to new ideas, dealing with ambiguity)	*17%*
Business acumen (understanding of the business context of situations)	*12%*
Collaboration skills (ability to work effectively with individuals and teams)	*16%*
Creative problem solving (identifying problems, relevant info., generating alt. and choosing and implementing solutions)	*27%*
Customer service oriented (displaying positive attitudes and behaviors to customers in order to respond to and meet their needs, requirements and expectations)	*17%*
Dedication / "cultural fit" (loyalty to your job/organization, acting harmoniously within organization)	*6%*
Dependability (fulfilling obligations, paying attention to details, compliance with policies and procedures)	*9%*
Digital/technology skills (understanding of computer technology and information systems)	*4%*
Integrity (ethical behavior, acting fairly, taking responsibility)	*31%*
Leadership (building, motivating, and leading a professional team attuned to the organizational culture, responsive to business needs, and committed to integrity and excellence)	*44%*
Lifelong learning (interest in learning, participation in training, anticipating changes at work, identifying career interests and taking charge of your professional development)	*8%*
Motivation and initiative (persistence, taking initiative, setting challenging goals, working independently)	*10%*
Negotiation skills (ability to work towards a mutually acceptable outcome between two or more parties)	*7%*
Planning and organizing (managing your time effectively, prioritizing responsibilities, project management)	*20%*
Professionalism (demonstrating self-control, holding a professional appearance, having a positive attitude)	*24%*

Teamwork (demonstrating concern for others, insight into other's behavior, having open communication, showing respect for diversity, resolving conflicts)	*20%*
Verbal communication (giving full attention to what others are saying, clearly communicating thoughts and ideas)	*14%*
Written communication (understanding work related documents, clearly compiling and preparing written reports)	*12%*
Other	*0%*

17. Below is a list of common professional traits required of many or most professionals in the security field at your level of responsibility/seniority. Regardless of your personal skill level in each area, please indicate the most important top three traits required of someone in your role. Please select up to three options.

PROFESSIONAL LEVEL (EMPLOYER TYPES MERGED FOR REPORTING)	TOTAL (N = 189)
Adaptability (demonstrating unique ways of thinking, being open to new ideas, dealing with ambiguity)	*17%*
Business acumen (understanding of the business context of situations)	*6%*
Collaboration skills (ability to work effectively with individuals and teams)	*25%*
Creative problem solving (identify problems, identifying relevant information, generating alternatives and choosing and implementing solutions)	*32%*
Customer service oriented (displaying positive attitudes and behaviors to customers in order to respond to and meet their needs, requirements and expectations)	*17%*
Dedication / "cultural fit" (loyalty to your job/organization, acting harmoniously within organization)	*6%*
Dependability (fulfilling obligations, paying attention to details, compliance with policies and procedures)	*17%*
Digital/technology skills (understanding of computer technology and information systems)	*7%*
Integrity (ethical behavior, acting fairly, taking responsibility)	*33%*
Lifelong learning (interest in learning, participation in training, anticipating changes at work, identifying career interests and taking charge of your professional development)	*20%*
Motivation and initiative (persistence, taking initiative, setting challenging goals, working independently)	*12%*
Negotiation skills (ability to work towards a mutually acceptable outcome between two or more parties)	*10%*
Planning and organizing (managing your time effectively, prioritizing responsibilities, project management)	*25%*
Professionalism (demonstrating self-control, holding a professional appearance, having a positive attitude)	*28%*
Verbal communication (giving full attention to what others are saying, clearly communicating thoughts and ideas)	*21%*
Written communication (understanding work related documents, clearly compiling and preparing written reports)	*20%*
Other	*1%*

Appendix B: Domain Specific Knowledge (Reflective Quotes)

The ASIS International-SIA Career Survey collected input regarding 41 distinct security field domains, including the type of specific knowledge, skills and abilities required for successful performance in each area. This section includes quotes related to each domain, segmented by practitioner and suppliers.

Question:
You previously indicated having a focus in the area(s) below. Please describe in general terms any specialized knowledge that is required for someone in your role in each area. Please be as detailed as possible and describe:
1. What type of knowledge of the subject-area is helpful and necessary in your role.
2. How much expertise is required in the specific area compared to the overarching principles, methods and approaches used in the security field more generally.

Access Control

	Selected Quotes
Security Management Practitioner	'You must have a knowledge of access control software technologies since the type of protection you're aiming to provide will necessitate the type of software and functions that are needed. '
	'You should know the basic functioning of the equipment involved with your security, thoroughly know the policies and procedures your client expects, and how the two are integrated with each other.'
	'You need to understand how systems work and are implemented. This is important to maximize the potential of the system you have and integrate surveillance, access control and computer programs. Expertise is not needed- only a desire to learn and implement change.'
	'I need to keep up with the innovations in access control so that I hire the right contractors to provide the access control system and keep it current and ahead of the bad guys.'
	'It is important to understand the appropriate use of access control and for what purpose. For example, can a card reader replace a guard at a particular location? If so, based on the potential risk, it may be a good value to implement. It is critical to understand the appropriate application for various access control devices, such as bio-metric readers. These devices tend to be used in high value areas where access is only granted to a few individuals. You have to consider your ability to administer the program as well and relevant expertise to do so.'

Security Industry Supplier	'It is necessary to know the architecture of systems and to hold a general knowledge of high security products that are available in the region. This includes a full understanding of product capability even if it is not used on some projects as well as a complete knowledge of codes, locks, reader technology, hacks, certification of manufacturers, specifications and solution implementation.' 'For me I cannot stress enough the importance of having the highest level of expertise in all that I do, and since access control is the main offering of the product I represent…it is hugely important.' 'It is important to know the technology: the level of access authentications, type of locks and card readers, control panels, communication security and integration with other systems.' 'You need to know the manufacturers' products and their capabilities and limitations. This includes the organization where the technology will be implemented (i.e., an understanding of the traffic flow and categories of workers...who is permitted in what areas at what times).' '(In my job) it requires technical knowledge of systems and how to design access control. You need to know how to assess if access control is required.'
Security Management Practitioner	'Should be a candidate who can be responsible in positions of trust.' 'Understanding the contract requirements and implementing those requirements is an important facet of my job.' 'An important aspect of this job is partnering with HR to avoid bad hires.' 'We should have strong level of emotional intelligence with access to security profiling techniques.' 'ASIS PBS standard is an excellent place to start. Relationships with law enforcement, government and private sector partners is essential [to this job]. Experience and proper training propagate expertise.'
Security Industry Supplier	'A moderate to extensive level of knowledge in legal should be required for suppliers as well as certification in CPP.'

Brand Protection

Security Management Practitioner	‘An overarching understanding of enterprise risk management is necessary for this job.’ ‘You should have a deep understanding of the base principles used in the protection of your brand. Most importantly though is the comprehensive tie to the crisis communications and overarching business resiliency plan.’ ‘We should liaison internally with HR and corporate communications to identify areas where the brand may potentially be compromised and ensure that policies are in place to deter this from within.’ ‘We should have a strong understanding of the Brand and impacts that can effect it, which is wide ranging with a myriad of considerations.’ ‘Understanding the risk associated with your organization from brand perspective and working collaboratively with other functions such as public affairs, risk management and legal when the need arises.’
Security Industry Supplier	‘You should have a business understanding of where security plugs into a customer's goals. Strong understanding of how any security or shared services spending directly impacts business outcomes for a prospect.’ ‘This job requires a medium level of expertise in brand knowledge and legal competence.’ ‘Should have a strong understanding the value of "Brand" both the tangible and intangible along with a valuation so that an appropriate risk strategy can be applied.’

Business Continuity and Resilience

Security Management Practitioner	'My job requires an understanding of best practices and implementation of planned responses to catastrophe.' 'We need to always be quick to respond with anything that develops in this area.' 'You should have an in-depth knowledge of business operations overall to the company goals and strategic directions.' 'The job requires a detailed knowledge of the planning process, risk acceptance process, remediation and recovery plans.'
Security Industry Supplier	'Basic knowledge required to understand different systems' strengths and weaknesses and apply to a situation in the field. You need knowledge of latest technology and a strong understanding of the particular business and the mission critical assets. 'Understanding prevailing theory and application of standards and industry practice within the region.' 'Must be familiar with redundant network infrastructure, fail safe access control, integration of communications and corporate network infrastructure.'

Communications / Awareness

Security Management Practitioner	'You must have the ability to drive awareness to a mass or select audience using various communications media and through various communications channels.' 'Be able to build strategic relationships to be able to receive information internally and externally and ensure that it is passed on to the relevant people as soon as possible.' 'Must have a detailed knowledge of your organization and what audiences to target in disseminating information.' 'Have a strong knowledge of the communication equipment used and proper etiquette for its use.' 'You need to be quick on your feet and to be able to communicate in a crisis.'
Security Industry Supplier	'Must be able to write good reports and executive summaries to bring translational skills to both the technical and non-technical reviewers of your communication products.' 'Have a strong understanding critical points to communicate to different departments internally.' 'Must be able to present information to wide audience in a formal setting.'

Compliance

Security Management Practitioner	'Have a strong understanding of the regulatory standard, as well as keeping up to date on changes to standards, and participation in standards review process.' 'Must have a strong understanding of the internal and external standards that apply to security.' 'A provider of compliance security is a subject matter expert.' 'We have to know how to implement check points to ensure all employees and locations are in full corporate and federal compliance.' 'In my job we need to have an awareness of unique compliance requirements, such as PKI, SOX, PCI-DSS, HIPAA.'
Security Industry Supplier	'Understanding Provincial and Federal Guidelines that apply to our sector within our region' 'Must have knowledge of UL/ULC, FM, CE, FCC/IC and other regulatory requirements for security equipment.'

Corporate Security

Security Management Practitioner	'A detailed knowledge is essential due to responsibility of the position held and being core business.' 'In my job we must know structure of company and all responsibilities assigned to the Corporate Security.' 'It is extremely important to have knowledge of all threats as well as best practices when dealing with these threats.' 'Understanding how to handle internal and external guests is an important aspect for the end-user in corporate security.'
Security Industry Supplier	'A supplier must have a strong understanding of the client's operational needs.' 'You need to know broad range of issues/areas, expertise dependent on area.' 'Must have financial, organizational, operational knowledge of the organization. Understand the flow of control and operations.

Counterterrorism and Counter Intelligence

Security Management Practitioner	'In addition to military and police experience, this role requires ongoing threat training, and expert knowledge of counter terrorism protocols.' 'Must have a strong understanding of national and international situations. Should have significant experience dealing with international situations. 'Networking with partners in government agencies is crucial in this role.' 'Need to keep up with specialized federal training.' 'Should have strong awareness of terrorist trends, current events, and indicators. Need to be in regular communication with external and internal sources.'
Security Industry Supplier	"Counterterrorism suppliers should have a strong understanding of current trends, as well as technical and operational knowledge." "They should have a high level of expertise including within law enforcement or via a military background."

Crime Prevention

Security Management Practitioner	'In order to work in the system, understanding of how and where crime works and resides is crucial. High degree of presence and community engagement must be taken seriously and the understanding of each role every agency plays is crucial.' 'General knowledge of principles with more in-depth knowledge of legal aspects and liability.' 'CPTED courses are very helpful [for this role]. So is working with your local police department.' 'Must have training, awareness, education, location selection, and strong alliances to be successful in this role.' 'Must have specialized Knowledge of crime prevention principles.'
Security Industry Supplier	"[Suppliers must have a] basic knowledge of crime prevention is required in order to understand different systems' strengths and weaknesses in order to find and available solution (and apply to a situation in the field)."

Crisis Management

Security Management Practitioner	'[You must] always have a plan before the crisis! Know who is responsible for what, and make sure they have a copy of the plan before the crisis.' 'Business continuity is standing up after the crisis, this is surviving the crisis and that takes considerable forethought and preparation; you need to understand your core assets and take care of your people to get everyone through the crisis…but know the risks associated and account for loss.' 'Communication skills are extremely important. On one hand a security manager must be able to report to their incident commander with unembellished details and then may have to communicate with the victims with compassion.' 'Preparedness is the key, companies that offer services in the crisis/disaster area must maintain a high degree of readiness. Relationships over time are a key in working together with outside agencies.' 'Training in crisis management is very helpful as every individual handles crisis differently, but any crisis can be handled through scenario based training.'
Security Industry Supplier	"As a crisis management supplier, emergency preparedness is important" "Suppliers should understand business processes, from and operational point of view." "Supplier should have a general knowledge of available solutions"

Cyber Security

Security Management Practitioner	'Working collaboratively with the Information Technology function in any organization is critical. 'The field of cyber-security requires In-depth knowledge of IT systems and understanding the risk vectors for the business so as to build sufficient risk mitigation measures.' 'The IT department works with Security to maintain a secure network. Third party testing and feedback provide updates.' 'Have an up-to-date understanding of threat/risk and mitigations. Having the right touch points in agencies to get the right advice.' 'Need to be experienced. Must have a working knowledge of systems, technology, components and their limitations.'
Security Industry Supplier	'The most important knowledge is the vendor contacts when needing deeper level knowledge of the products.' 'Understand IT asset protection and threat penetration.' 'Have a working knowledge of encryption, passwords, and standards.' 'Must have an extensive background in high tech investigations, computer, programming and hacking skills.'

Drug Detection

Security Management Practitioner	'Must be knowledgeable on substances and have experience in dealing with persons under influence. Should have experience dealing with legal issues and crisis management.' 'General knowledge of illegal drugs or designer drugs. Hands on experience in physically recognizing drugs and behaviors/symptoms of being under the influence of drugs or alcohol.' 'Need to network and liaison with law enforcement at all levels and basic familiarity with CT-PAT.' 'Monitoring of activities for indications of illegality, behavior changes is vital to the role. Creation and dissemination of SOP's regarding unacceptable practices in the workplace. Must have knowledge of specific symptoms of various drug types.'
Security Industry Supplier	'Suppliers should have a moderate to high expertise – including symptoms of illegal drug use and in threat analysis and solutions.'

Economic Crime and Fraud

Security Management Practitioner	'Must have the ability to help staff identify fraudulent monies and government identifications. Understand what to do when something is discovered and how to report it to the proper authorities.' 'Evaluate forensic report data to identify possible commission, equipment, or subscriber fraud and to identify suspects for interview. 'Must know brand reputation of your company and areas of vulnerabilities.' 'This role requires an understanding of financial controls and opportunities in the company.'
Security Industry Supplier	'You need to know general concepts/issues and have a medium to advanced level of expertise.' 'Should have a working relationship with banking and financial institutions as well as with and federal law enforcement."

Emergency Management

Security Management Practitioner	"Should have advanced knowledge of threat assessment and management" "Be able to deal with the emergency immediately and hold knowledge of facility along with others that will assist until the authorities arrive on-site" "It is important to have completed trainings, including FEMA and state level training, ICS and NIMS training" "Knowing how to operate within an incident command structure. Knowing how to communicate directions up and down the structure and how to keep the team focused as they respond."
Security Industry Supplier	"Should have understanding of the prevailing theory and application of standards as well as industry practice within the region." "A basic knowledge is required in order to understand different systems' strengths/weaknesses and apply to a situation in the field. Need knowledge of locally adopted codes and standards, as well as local jurisdiction emergency plans and contact information." "Should have an understanding of local conditions and availability of local resources – as well as equipment to react to situations"

Engineering and Design

Security Management Practitioner	'Have a moderate knowledge of engineering and design in the architectural, electrical, and security disciplines and a basic knowledge of civil, mechanical, and construction trades.' 'Have a good understanding of available technologies for the effective management of physical security, employee management and appropriate tools used, especially the role of unions.' 'Technical knowledge of systems design, compliance factors, business factors. Should have demonstrated experience in project management and budget management.' 'Must have operational experience, education and certification.'
Security Industry Supplier	'A complete systems understanding and knowledge of integration capabilities is very important [for this role]. Technical writing skills is also very important.' 'Getting to understand the needs of the client and the risks, threats and liability they face.... and be able to address it appropriately.' 'Know how to design and specify a system. This requires a significant knowledge base of design documentation, construction, and technical knowledge of current products and market trends.' 'Structural knowledge of the different industries and the what the market offers to cover these requirements. This may require four years of relevant hardware and software experience.' 'Understanding of a layered approach to security design from the perimeter fence to the most attractive target and identifying appropriate mitigation strategies.'

Environmental Health

Security Management Practitioner	'Ability to provide a healthy, pleasant and safe place for people to work and patients to obtain services. Ensure compliance with fire and safety codes and chemical exposures.' 'Work with staff to address and mitigate risk in this area.' Must have a knowledge of personal safety equipment and risks first, then assessing and responding to priority needs' 'CPP & PSP Certification' 'Have a basic knowledge of chemical hazard protection.'
Security Industry Supplier	"Should understand general principles and methods" "Possess knowledge of OSHA and regulations regarding hazardous materials." "Should have a science background"

Executive Protection

Security Management Practitioner	"Close protection experience needed" "Formal education and experience in executive protection, with a high level of expertise." "Must have knowledge of general principles. Prior experience in military, law enforcement or corporate security with significant training in weaponless defense, firearms, driving, etc." "Should have an excellent understanding the specific needs of the individual and the corporation." "You need to be very tactically sound in order to handle executive protection….you must be aware of proper movement, cover and concealment, along with a high comfort level with firearms."
Security Industry Supplier	"Real world experience here is necessary. There is a gap between theory and application that many folks do not realize." "Good understanding of the client's needs" "High expertise in personal protection, martial arts, and/or military background"

Financial Asset Protection

Security Management Practitioner	"Need a deep understanding of how financial scams and threats occur and relate to my situation. Industry specific knowledge is needed in banking." 'Must have skills in business analysis, accounting, commercial crime and fraud awareness and training.' 'Knowledge of electronic access control and understand the potential for cyber threats and relevant security mitigation measures.' 'Recognize what are the largest and highest value assets and what needs to be done to protect those assets. Spend time on protecting the most valuable.' 'We protect monetary instruments and negotiable items.'
Security Industry Supplier	"Must have an understanding of the company and their goals to provide proper service." "Understanding of cyber, data protection, physical security principles and technology."

Government

Security Management Practitioner	'Have a critical understanding of laws, regulations, policies, mission/objectives and politics.' 'Need to understand how government operates to better see how a quasi-government entity would operate.' 'Government processes and regulatory requirements is a must-know.' 'Conduct their security clearance background investigations.'
Security Industry Supplier	'Need to have an understanding client objectives, requirements and classification of projects.' 'Should have knowledge of government guidelines, (local, state and federal) requirements, mandates, and purchasing rules' 'Understanding the systems at a high level and knowledge of government standards is critical.' 'Basic knowledge required to understand different systems' strengths and weaknesses and apply to a situation in the field. Need knowledge of specific agency requirements or local requirements.'

Intellectual Property

Security Management Practitioner	'Should be skilled in data classification, stakeholder awareness, assignment of asset ownership, business value, and technology.' 'Have a fundamental understanding of the threat-scape and how to appropriately respond when a victim reports such crime.' "Extensive experience with intellectual property and legal experience is needed.' 'You need to know the guidelines and laws around data protection and a written process in place to protect the intellectual property.' 'Should have at least basic knowledge of EAR/ITAR, CI background, OPSEC, and legal training.'
Security Industry Supplier	"Should have knowledge of the systems and their various devices so a system can be designed to operate correctly" "Should have an understanding of the client needs and potential impacts"

Intelligence

Security Management Practitioner	'Need to have knowledge in investigations and be able to process and handle large amounts of information. Furthermore, IT knowledge can be helpful.' 'Business intelligence experience and data gathering expertise.' 'A comprehensive intelligence gathering and maintenance program including effective relationships with appropriate public/private entities is paramount to success within this role as you are the one person Leadership comes to when everything is going wrong.' 'Role includes intelligence gathering and understanding what is important to gather and why. If you collect data and no one is interested in it or does not find value in it - you should question why you are collecting it. Intelligence data should be gathered that speaks to the company's interest and is either informative or actionable.'
Security Industry Supplier	'Role should require experience in the field of technology supporting intelligence operations' 'Collection of relevant data and analytical functions to derive actionable intelligence is an important function of a supplier.' 'Must have knowledge of IT management, practices, and guidelines'

Investigations

Security Management Practitioner	'Going undercover undetected, taking information, keeping records of information in certain organizations are important aspects of this role.' 'Need to have experience with interview and interrogation techniques, and how and when to employ them.' 'Proper training and education on how to conduct a legal and proper investigation.' 'Must cultivate the ability to listen, ask meaningful questions and record your findings in writing.' 'End-users must work with people and information and find methods of discovering the gaps within the information.'
Security Industry Supplier	'Have legal and procedures knowledge.' 'Should be able to understand both verbal and non-verbal communications.'

Information Technology

Security Management Practitioner	'Must have some level of certification and training; formal training.' 'Understanding of technology, IT, stakeholder engagement, clear role definition, upper management support, appropriate policy development and approval, and flexible budget to allow for a dynamic response to the changing threat environment.' 'Need experience in information security, computing security, cyber security, and/or information assurance experience.'
Security Industry Supplier	'Supplier role should have an extensive background in IT security as well as extensive computer, programing, and/or hacking skills.' 'Need to have a high level of expertise in current technology.' 'Be familiar with types of hardware (firewalls, router access list, communication servers), software (iOS, antivirus, analytics, patches) and Intrusion detection 'Job is based with very new technology standards – general knowledge is not enough any more.' 'Understand network design and security, encryption, secured IP and managed network devices.'

Legal Compliance

Security Management Practitioner	'Have knowledge of appropriate governmental regulations, and knowledge of local laws and records of dealings.'
	'Have a willingness to ask questions prior to event and basic level of understanding of legal implications.'
Security Industry Supplier	'Have a strong understanding and awareness of liability as well as contract review.'
	'Understand compliance to meeting codes in design and compliance in governmental regulations.'
	'Be well versed with specific legal obligations (i.e., OSHA reporting AML)'

Loss Prevention

Security Management Practitioner	'Depending on your industry this is a crucial area to have knowledge in. You want to protect all of your organizations assets, but loss prevention focuses on internal and external larceny.' 'From a physical asset protection perspective - overarching understanding and some practical application preferred.' 'Skill, knowledge and area expertise and working with client agencies to match law with their policies and procedures to enact a program. As in any area working in conjunction with LEO trust becomes a huge factor and knowledge base is crucial in forming relationships and being taken seriously on cases we work.' 'You need to understand where your vulnerabilities are and where the high value is, then determine what controls to implement to protect and reduce loss.'
Security Industry Supplier	'Suppliers need to have an understanding the current trends in crime and be able to apply CPTED in meaningful way.' '[My job] uses operational, business processes, information, social engineering skills.' 'The greatest asset to bring to the table is knowing the customer's pain points and how to create a solution to solve them.' 'Asset tracking, metal detection, tag software systems and inventory control integration are all tasks related to the role.'

Personnel Security

Security Management Practitioner	‘Should have awareness training, intelligence, cultural transformation, and knowledge of generational differences.’ ‘This role requires excellent interpersonal skills for interviewing, screening, background checks, training supervision and follow up.’ ‘Management skills are a must. Overarching principles, methods and approaches are sufficient for this subject area.’ ‘People are one of the greatest business assets and critical to know how to preserve them in a business-friendly manner.’ ‘Understanding people and how to interact with them in a way that's both personal but also professional and in line with the company's corporate culture and structure.’
Security Industry Supplier	‘Need to be proficient at commercial and public vetting and background checking standards and procedures.’ ‘Need to have strong background in systems knowledge as well as personnel behavior and crime trends.’ ‘Background investigation and continuous vetting are vital parts of my role.’

Physical Security

Security Management Practitioner	'Need formal training and certifications, including CPP & PSP certification, education, police training and field operations.' 'Knowledge of industry trends, technology, physical security principles, industry best practices, capital and expense budgeting.' 'This role also includes the areas of risk management, IT, electronics, business administration, and finances.'
Security Industry Supplier	'Have a strong awareness of current and persisting threats coupled with construction design and how they can be exploited based on the sophistication of the advisory.' 'Need a knowledge of electronic systems, barriers, fencing, etc.' 'Must have a knowledge of Intrusion detection equipment (sensors and CCTV analytics), surveillance (CCTV and Audio), access control (credential readers, biometrics, anti-pass back) 'Have experience with perimeter protection, access/egress tracking, sally door design, and integration of video and door control systems.' 'Role requires technical knowledge of systems and how to design access control. You need to know how to assess what type or element of physical security is required.'

Public Safety

Security Management Practitioner	'Important aspects of the role include law enforcement engagement and knowledge sharing, partnership will enforcement agencies- bylaw, fire, emergency management, emergency health services.' 'We need to have strong understanding and continuous training in Public Safety, FEMA, OSHA, etc.' 'Must attend and also implement training, drilling, and converging initiatives (i.e., matching chemical spill drills with active threat drills).'
Security Industry Supplier	'Should have formal training in a program of various general security theories and practices.' 'Having a law enforcement background opens doors that would normally be closed to security professionals.' 'Be knowledgeable about personal safety applications, campus notification systems, integration of security and public safety officer communications systems.' 'Must be familiar with school and hospital security requirements.' 'Persons in this role must have an understanding of various public safety entities, principles and threats'.

Risk Management

Security Management Practitioner	'Should have a sound grounding in risk management processes, an understanding of the organization's risk context and culture and effective communications ranging across the workforce, to management and senior executives.' 'Need to have an awareness of the overall threat/risk profile for the company and industry. Awareness of potential threat mitigation techniques, business resiliency measures.' 'Should be able to mitigate risk, identify significant risks and develop a weighted scale concerning actual risk versus possibilities of an incident.' 'Need to have experience and training, need to understand broad areas of risk. People in this role should consider appropriate secondary training (ARM/CRM).' 'End-users in risk management should have knowledge of the nature of the business, the operating environment, the assets, adversaries, and possible adversary actions, potential impact on business etc.' 'Should have knowledge of types of risk and organizational needs and the types of risks that impact the organization.'
Security Industry Supplier	'A good knowledge of how to identify, analyze and treat risk is essential. The expertise required is the ability to apply security risk management to other risk management practices.' 'Need to have a general overview of risk only (risk management 101 would suffice).' 'Should have an expert or advanced level.' 'Risk assessment skills are important to be able to determine risks and systems understanding and a critical piece to understand what measures can be taken to mitigate the risk.' 'Need to be proficient at identifying risk and be able to develop countermeasures.' 'Understanding of basic risk management principles for specific vertical markets.'

Security Consulting

Security Management Practitioner	'You need to have 'Big Picture thinking.' Must have real world experience over a considerable period of time. Ability to approach issues from multiple viewpoints/angles. Understanding and applying both tangible (legal, administrative, regulatory issues) and lesser defined threats such as criminal or other behaviors (protests, public perceptions) as required to build comprehensive and useful assessments to guide decision making.' 'Knowledge as to when to look to the outside to get various opinions and recommendations on how the industry handles like issues and trends.' 'We have strong knowledge of both the theoretical and practical – and how to apply them across a broad spectrum of industries and facilities.'
Security Industry Supplier	'Have the ability to look at the overall picture and how to address threats and vulnerabilities with systems, people, and procedures.' 'Must be able to speak business, know product lines, know system design and know implementation and testing processes. Be able to relay this to both technical and non-technical personnel.' 'Have a thorough knowledge of the security industry, especially in the area of one's supposed expertise. Need the ability to provide the customer with what he/she want and not necessarily what he/she asked for.'

Security Education

Security Management Practitioner	'Have an understanding of the ways in which adults learn can be very helpful here. Must have good public speaking skills.' 'This is an ongoing, every second process, with our guard force. It is only with further education, and constant utilization of what we have learned by training, that we can't continue to provide the security and safety our valued client expects. For me personally, I want to obtain my CPP certification within the next two years.' 'Should have continual updating of knowledge through articles, products or sharing knowledge with other Security Professionals and giving training to others on various topics throughout the organization.' 'Be trained sufficiently to demonstrate security methods and trends to educate corporate personnel.'
Security Industry Supplier	'Have continual education to remain current in industry.' 'Have extensive knowledge of features and functionality, as well as of the entire training process, to include ISD.' 'Knowing how to present information to wide audience in a formal setting (e.g. Toast Masters) is crucial to this role.' 'This role requires a certain type of person who can teach.'

Security Management

Security Management Practitioner	'You need to have a background in a security field, government or in law enforcement, CPP or equivalent certification. Also, degree in management or Six Signature training.' "You should be an expert or advanced knowledge of the field." 'You must understand or determine how security fits into organization and its interactions with various departments.' 'Should have a thorough background in management, specifically managing security personnel.'
Security Industry Supplier	'Should have general knowledge of available solutions.' 'Understand best practices for security operations management.' 'Should have a high level of expertise and experience/certification in CPP, PSP, Soft Skills.' 'You have to have the ability to see the big picture from manager's point of view.'

Security Operations

Security Management Practitioner	'Have a thorough understanding of concepts, practices and principles and their application in real world environments. This is also your daily nuts and bolts work.' 'You should have experience in risk management, business management, finances, database, spreadsheet, human resources, management, procedures and technical.' 'You need to understand how the badging system works, how to troubleshoot issues, understanding how the system works and who to go to for help, understanding dual employer issues, union dos and don'ts, understanding visitor policy and how that must be implemented in several different work environments.' 'You should have a general knowledge of specific business needs and operations as well as specific knowledge of compliance/regulatory needs. Have a demonstrated ability to look forward, work with upper management and all levels of business operations management.' 'You need experience running an operation and the challenges of running a security operation (HR, progressive discipline, training, contracting, budget management).'
Security Industry Supplier	'Security operations suppliers need to have a broad range (medium level of expertise) knowledge of issues/areas.' 'Need an understanding of how systems will be used, viewed and what responsibilities the person monitoring the system must do/achieve to be successful.' 'Suppliers should have an understanding of human interactions with security information systems.' 'You need a knowledge of programming, system functions, and day to day operational requirements.' 'You need to have an understanding of applications and use of technology to improve operational efficiency.'

Security Systems

Security Management Practitioner	'This role requires knowledge of industry needs, requirements for security systems and equipment. Also knowledge of various equipment or system availability and appropriateness of use for the corporation.' 'Have a strong technical knowledge of various security systems. Should have the ability to learn quickly when confronted with an unfamiliar system.' 'You should have a technological background, as everything updates and changes quickly you really need to stay up to date on current equipment, programming and software.' 'You must understand what is on the market and the capabilities of each type of system then determine what your needs are and match that up with the system that can meet your needs.'
Security Industry Supplier	'This role requires a continual updating of information to keep up with new security systems and new technologies used in this industry: attending security events, reading magazine, etc.' 'Must have a knowledge of sensors, data transmission equipment, information display technology.' 'Product knowledge, installation methods, understanding buildings are all very important requirements for this role.' 'You should have technical knowledge and background in IP technologies and application of physical security practices.' 'You need to have an understanding risk management and security policies, goals, procedures that a prospect would employ. Level of expertise is a basic understanding of how systems work, the major vendors, how prospect use the specific technology, value it, cost/benefit analysis.'

Security Technology

Security Management Practitioner	'I need to have specific knowledge of the systems in use at the current company. All too often a superficial knowledge will not be enough to use the available systems and technology effectively.' 'You should have a technological background, as everything updates and changes quickly you really need to stay up to date on current equipment, programming and software.' 'We need to stay informed on recent developments and trends in security technologies and know how to best apply them to campus security systems.' 'Being knowledgeable across new technologies and how they can improve the security function for our business. As this includes emerging tech, there isn't a specific knowledge, more of a requirement to be interested in finding out about new tech and its use'
Security Industry Supplier	'You need to have a strong understanding risk management and security policies, goals, procedures that a prospect would employ. Level of expertise is a basic understanding of how systems work, the major vendors, how prospect use the specific technology, value it, cost/benefit analysis.' 'Understanding what is out there competitively and where the markets are moving is required.' 'Being at the forefront of technology development for a product set is important. But not worth anything if people don't know that you product can do those new things. It is my job to make sure they have the right awareness of the technology we offer.'

Supply Chain

Security Management Practitioner	'Need to be able to design & implement cyber security controls in the supply chain process to minimize risk to the organization and meet regulatory requirements.' 'Legal and contract requirements, service level agreement development and approval, partnership and expertise embedded in supply chain management.' 'We should have specific knowledge of the systems in use at the current company. All too often a superficial knowledge will not be enough to use the available systems and technology effectively.'
Security Industry Supplier	'We should have a general knowledge of available solutions as a supplier of supply chain security.' 'Need to have a detailed understanding of the industry supply lines and processes.'

Threat Assessment

Security Management Practitioner	'The nature of the business, the operating environment, the assets, adversaries, and possible adversary actions, potential impact on business etc.' 'We should have specialized training, higher level of education and continuous learning.' 'Need to have knowledge of sources of information and understanding of how to do a security assessment. Mostly overarching principles are needed, though this field becomes more knowledge specific by the day.' 'You need to have a high level of awareness of the overall threat/risk profile for the company and industry. Awareness of potential threat mitigation techniques.'
Security Industry Supplier	'Must be able to identify the current and future threats that may affect an organization.' 'Need to have training in physical security practices or related law enforcement training.'

Travel Risk Management

Security Management Practitioner	'We need to have knowledge not just of trends and developments around the world, but also the ability to understand the different perspectives and experiences of traveling staff. Each employee carries his or her own "baggage" and this must be incorporated into the risk analysis and in the training of the employee.' "Need to be familiar with political, social and policy updates, travel restriction circulars, knowledge about interest gaps.' This role requires knowledge in security travel advisory services, risk assessment of areas of jurisdiction, and security briefing on places or countries.' 'Understanding the international risks and duty of care responsibilities. Significant experience is required.'
Security Industry Supplier	"This role requires a high level of experience and training and certifications. Need to maintain diverse sources.'

Video

Security Management Practitioner	"Need to be familiar with CCTV management and dissemination protocols.' 'You should have a bachelor's degree in computer science or information technology and be PSP Certified.' "Overlapping areas of expertise include physical security, physics, electronics, and IT. 'Role requires knowledge with technology changes, bandwidth management, network configuration, privacy restrictions, limited access to recordings, minimize use of video to necessary areas for detection and active monitoring or investigative tool.' 'You should have an understanding of security systems and system integration.'
Security Industry Supplier	'A basic knowledge required in order to understand different systems' strengths/weaknesses and apply to a situation in the field. Need knowledge of latest technology.' 'Knowing the different cameras, manufacturers, the way the camera systems work, and how to place cameras for the best surveillance.' 'Have a strong understanding of optics, electronics, operating environment, signal transmission, equipment mounting, data storage and retrieval.' 'Persons in this role should have an understanding risk management and security policies, goals, procedures that a prospect would employ. Level of expertise is a basic understanding of how systems work, the major vendors, how prospect use the specific technology, value it, cost/benefit analysis.'

Workplace

Security Management Practitioner	'We need a moderate level of expertise in understanding the causes of workplace violence, prevention, response, training and engagement with law enforcement, human resources and management.' 'We should be familiar with best practices and current laws, have experience, and up-to-date training.' 'You need an understanding of general and specific workplace violence risk, as well as assessment and management strategies.'
Security Industry Supplier	'You should have training and certification in mitigation and response techniques. Application of technology to prevent, detect.' 'Real world experience here is necessary. There is a gap between theory and application that many folks do not realize.' "should have a medium level of expertise. Be trained and familiar with CPP and legal competence.'