University of Phoenix® | ASIS FOUNDATION™

# Security Industry Survey of Risks and Professional Competencies

Executive Summary

## Background and Purpose

The U.S. security industry is a more than $350 billion market.[1] From small businesses to multinational corporations, today's organizations face increasingly complex enterprise-wide risks. Despite the critical and expanding role of today's security professionals, to date there exists no agreed-upon, complete set of competencies utilized across all roles and levels of the security workforce; nor are there uniform educational guidelines for individuals to develop these competencies.[2]

To help address this deficit, the ASIS Foundation partnered with University of Phoenix to undertake a series of research activities to identify the industry's talent needs and to generate actionable recommendations for strengthening the industry's workforce.

One such research activity was a national survey of security industry professionals conducted by University of Phoenix and the ASIS Foundation in fall 2013. The survey's purpose was to verify and prioritize previously identified security risks, challenges, and professional competencies.

## Survey Process

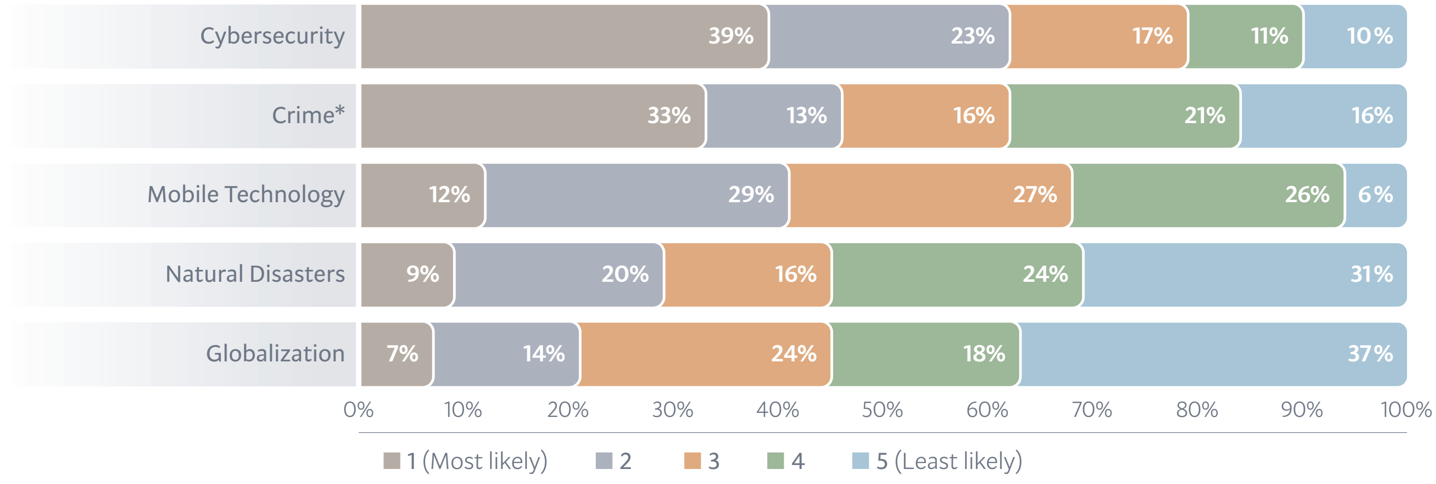
The ASIS Foundation invited members of ASIS International to participate in the online survey. To help ensure validity of the results, survey participants were required to meet certain professional criteria.

More than 1,880 ASIS International members indicated interest in participating in the survey. Of that pool, 483 respondents met the survey criteria.

Those who met the criteria were asked to complete the survey by (a) responding to demographic questions, (b) ranking previously identified security industry risks and challenges, and (c) rating the importance and frequency of 22 professional competencies used in the security industry.

All 483 respondents were currently working in the United States and had a professional focus on general security management. Just over 70% were currently directors or managers, with more than 75% of those being responsible for managing or supervising security functions only for their employer.

### Rankings for Each of the Five Security Risks Most Likely to Affect Enterprises



*Crime values total 99% due to rounding.

[1] ASIS International and the Institute of Finance and Management, *The United States Security Industry: Size and Scope, Insights, Trends, and Data*, Alexandria, VA: ASIS International, 2013, https://www.asisonline.org/ASIS-Store/Products/Pages/The-United-States-Security-Industry-Size-and-Scope-Insights-Trends-and-Data.aspx. While the security industry spans both operational and informational security, the term "security" in this executive summary and in the corresponding report refers only to operational security, comprising activities to mitigate and prevent harm across an enterprise.

[2] A "competency" is defined as a group of related skills and abilities that influence a major job function, indicate successful job performance, are measurable against standards, and are subject to improvement through training and experience; CareerOneStop, "Develop a Competency Model," 2014, http://www.careeronestop.org/COMPETENCYMODEL/userguide_competency.aspx.

## Key Findings

Cybersecurity, crime, mobile technology, natural disasters, and globalization—in that order—were ranked as the top five risks most likely to affect an enterprise over the next five years. Management issues and limited resources, industry segmentation, the aging workforce, and a lack of standardized education and certifications were ranked as the leading challenges facing the security industry.

Decision making, oral communication, critical thinking, maximizing others' performance, and persuasive influencing were ranked as the most critical among 22 core competencies that security practitioners will require to successfully perform their responsibilities over the next five years.

## Recommendations for Stakeholders

**Organizations** should ensure their current personnel and new hires have the competencies and skills to address the security risks identified in the survey as those most likely to affect enterprises in the next five years, and should identify any additional training and education programs needed to increase risk readiness in these categories.

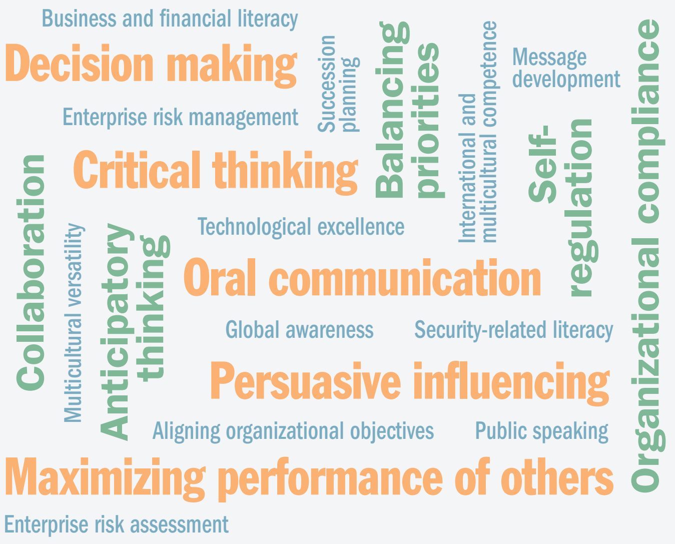
**Security industry leaders** should collaborate with corporate or enterprise executives to ensure that management issues and limited resources—identified as the top challenge facing security personnel—do not impede security readiness. Security leaders should also continue to expedite the convergence of operational and IT security resources via dialogue between professionals in both areas, and by establishing training programs, job descriptions, and operational processes that emphasize this goal.

**Career counselors** should consider the core competencies rated most highly in this survey when advising individuals with security-industry career aspirations. Understanding core competency requirements can aid prospective students in the important process of identifying the right training and education for their success in the industry. Beyond the core competencies, all 22 identified competencies will likely be relevant to security professionals' successful job performance.

**Talent development leaders** should convene to endorse the competencies identified as essential for workforce success, and should maintain a competency model for use by industry stakeholders.

**Higher education institutions** may find industry segmentation a challenge when crafting cohesive educational tracks owing to the wide variety of jobs, settings, and specialties across the industry. By developing non-degree and for-credit educational offerings with industry leaders' and employers' input, colleges and universities can improve the career relevance of their programs.

### Security professional competencies


Business and financial literacy
Decision making
Enterprise risk management
Succession planning
Balancing priorities
International and multicultural competence
Message development
Organizational compliance
Collaboration
Critical thinking
Self-regulation
Multicultural versatility
Anticipatory thinking
Technological excellence
Oral communication
Global awareness
Security-related literacy
Persuasive influencing
Aligning organizational objectives
Public speaking
Maximizing performance of others
Enterprise risk assessment

*Note.* The varying sizes of items in the word cloud reflect how the 22 competencies in the survey can be clustered into three groups: the top five most critical (largest font), the next five most critical (medium font), and all others (smallest font).

**Current security professionals** should supplement their technical skills and security specializations by developing cross-functional knowledge and interdisciplinary competencies to improve collaboration with professionals in other specialties and functional areas, with the goal of enhancing enterprise-wide security functions and preparedness.

**Aspiring security professionals** should identify educational programs that best equip them to succeed in the profession.

**Career changers** should identify existing gaps in their education and career experience and opportunities to obtain targeted education and training to close the gaps.

## Learn More

Read the full report and related research at **industry.phoenix.edu.**