Enterprise Security Risks and Workforce Competencies:
Findings from an Industry Roundtable on Security Talent Development
About The ASIS Foundation

The ASIS Foundation is a nonprofit organization dedicated to providing high-quality and contemporary research and education opportunities that enhance the security profession and support the mission of ASIS International. The topics researched by the Foundation produce valuable and actionable knowledge for the security professional. Additionally, through the awarding of scholarships, the Foundation ensures that those pursuing a career in the field of security management are able to realize the highest academic achievements.

Foundation programs are supported solely by contributions from individuals, ASIS chapters, and other organizations who share its vision of advancing both the security profession and the professional. For more information, visit www.Foundation.ASISOnline.org.

About University of Phoenix

University of Phoenix is constantly innovating to help working adults move efficiently from education to careers in a rapidly changing world. Flexible schedules, relevant and engaging courses, and interactive learning can help students more effectively pursue career and personal aspirations while balancing their busy lives. University of Phoenix serves a diverse student population, offering associate, bachelor’s, master’s, and doctoral degree programs from campuses and learning centers across the U.S. as well as online throughout the world. For more information, visit www.phoenix.edu.

University of Phoenix has been serving professionals in the criminal justice and security field for more than 30 years. The College of Criminal Justice and Security offers degree programs with management-focused curriculum to provide the skills required to be a leader within the fields of criminal justice and security. Visit www.phoenix.edu/cjs.

The Industry Strategy Group at University of Phoenix offers research and educational advisory services to help industries meet national and global workforce development needs. Collaborating with national and international industry associations, University of Phoenix conducts roundtables and other thought leadership initiatives to help industry leaders and employers identify what skills and competencies today’s workers need, and how best to help working learners build these skills while pursuing an industry-endorsed certification or an accredited college degree. University of Phoenix regularly adapts its certification and degree programs to align with industry needs, and helps employers increase workforce competitiveness in multiple economic sectors. Visit www.industry.phoenix.edu or contact IndustryStrategy@phoenix.edu.
About This Report

The ASIS Foundation and University of Phoenix hosted a National Roundtable on Security Talent Development in summer 2013. The purpose of the roundtable was to identify the top risks the security industry will face in the next five years, and to initiate a discussion about standard competencies that security professionals will need to demonstrate to protect tomorrow’s enterprises. Security executives and thought leaders from industry, higher education, and government provided their insights and recommendations, which are summarized in this report.

The roundtable event comprised two sessions: During a four-hour, large-group discussion, participants examined current and imminent risks the security industry faces. During three one-hour breakout sessions, participants identified and mapped key workforce competencies to one or more assigned security risks. Breakout discussions were organized around the general topics of technology, unintended risks, and resilience.

In addition, University of Phoenix researchers conducted a scan of existing literature to identify current trends and issues in today’s security industry. The literature review provided context and supporting data for this report.

To complement the research conducted to date, the ASIS Foundation and University of Phoenix launched a research survey of ASIS International members in fall 2013. The survey results will help to further define enterprise risks and security professional competencies. To learn more, contact IndustryStrategy@phoenix.edu.
Introduction: Today’s Security Industry

The U.S. security industry is a $350 billion market that includes private-sector spending of $282 billion, and an additional $69 billion in federal government expenditures on homeland security. Security is an essential business function that impacts every public and private sector. Security professionals must protect people, property, and information from ever-changing risks in a variety of organizational and geographic settings worldwide. This multifaceted industry also protects the infrastructures critical to the daily lives of every individual, organization, and government agency—including communication networks, transportation and utility delivery systems, and public protection services. The industry is also growing: For 2013 alone, private security (non-IT) spending was estimated at $202 billion, with projected growth of 5.5%; IT-related private security spending was projected at $80 billion with 9% expected growth.

Protecting physical property from natural disasters or crimes such as theft, break-ins, and fraud has been a historical concern, but in the information age, security personnel’s responsibilities have broadened to include cybersecurity—the protection of digital communications, information, data systems, financial transactions, intellectual property, and much more. Within businesses, security professionals oversee the protection and integrity of products and global supply chains; they also help to screen employees and manage training in security protocols and procedures throughout the organization. In today’s marketplace, security breaches are likely to have widespread and possibly instantaneous repercussions affecting the livelihood of individuals, organizations, and nations. As a result, security professionals bear massive responsibilities unlike those faced during previous periods in history.

Careers in security include opportunities to work for public- or private-sector organizations, or as consultants in firms specializing in security functions. In jobs that range from entry-level to executive-level, the number of full-time security workers is estimated at between 1.9 million and 2.1 million. Increasingly, companies are employing a Chief Security Officer at the executive level to handle crisis management, risk mitigation, and contingency planning.

Salaries for security executives are rising, with the median compensation at $102,000.

2 Ibid.
3 Ibid.
5 Ibid.
management responsibilities for their organizations. Salaries also tended to be higher in larger, private companies than for government positions. In addition, formal education, certifications, and professional experience correlated to higher compensation. Personnel in entry-level positions or with fewer responsibilities can expect to earn more modest salaries.6

The need for security professionals is expected to grow, providing steady opportunities for career growth at all levels of responsibility.7 In the IT area, for example, the U.S. Department of Labor projects higher-than-average job growth of 22% through 2020;6 private detective/investigator jobs are also projected to grow by 21% during that time.8 A recent survey by (ISC)2, a leading nonprofit organization that educates and certifies information security professionals, found nearly full employment among IT security professionals; only 7% were unemployed at any time during 2011.9 More than one-third of those surveyed said they had changed jobs in the last year, and a majority had made the change because they had an opportunity for advancement.10

Enterprise Security Risks

Roundtable participants identified the following internal and external risks to enterprise-wide security:

Cybersecurity. Cyberterrorism and cybersecurity breaches were among roundtable participants’ most serious concerns, a finding that mirrors a 2012 Securitas USA survey of Fortune 1000 companies.7 In 2008, federal agencies reported three times as many cyber-related incidents to the Department of Homeland Security as in 2006; in the case of organizational data breaches, these attacks cost an average of $6.6 million, or more...

---

7 U.S. Census Bureau, Service Segmentation by Revenue.
11 Ibid.
than $200 per compromised record. Cybersecurity risks may come from organized external perpetrators, terrorists, and individuals who capitalize on victims’ carelessness, or from internal personnel with criminal intentions. The source of these risks may be international corporate espionage or an at-home hacker.

Difficulty of detection can compound some cybersecurity risks. Malware may be built into software and designed to blend in with the system it infects, allowing security breaches to begin as soon as the software is installed. “Some companies may not perform due diligence in reviewing the code they receive—or may not even have the staff to do so,” says Rae Hayward, Senior Manager of Product Development for (ISC)², “so there may be malicious code put into these products that allows hackers to do damage.” With the assumption that software may already be compromised, security efforts must shift to an investigative and monitoring approach rather than a reactive one. In addition, many security professionals need substantial knowledge of technology and/or software engineering to make informed choices in software purchases and to implement sophisticated computerized security infrastructures.

Mobile technology. Distributing enterprise data across mobile technologies increases the vulnerability of confidential and proprietary information. As these technologies blur the boundaries between professional and personal spheres, users contend with the constant threats of surveillance and compromised data. The amount of malicious software aimed specifically at mobile devices increased 185% in less than a year, according to a 2012 Government Accountability Office (GAO) report. Although organizations may implement strong internal security protections, vulnerabilities in the design of mobile devices—and the carelessness in their use outside the workplace—increase the threats. “If you keep sensitive data on a laptop or smartphone, or you use any network, somebody is watching or listening. You have to be very, very careful,” warns Kevin Doss, President and CEO of Level 4 Security, a company that specializes in physical security.

---

Globalization. Increased globalization of enterprise functions has expanded the footprint of security professionals’ responsibilities from local to worldwide. The outsourcing of data management and offshoring of supply chains present multiple, complicated security challenges. Outsourced data management functions may introduce added risks to intellectual property and other information. For example, when a company outsources functions, it has little or no control over the selection of personnel performing the work, and must rely on the vendor to demonstrate professionalism, integrity, and sound decision-making in the staffing process. Offshoring the supply chain may also expose the company to political conflicts and socioeconomic problems in overseas locations that can restrict access to resources, utilities, and transportation, gravely disrupting industrial operations. Quality assurance measures and trusted relationships in overseas operations are critical to mitigating the risk of counterfeit products and parts, which can damage a company’s reputation, competitiveness, and viability.

Natural disasters. Natural disasters—potentially intensified because of climate change—pose an increased threat to companies worldwide, and globalization increases exposure to these types of risks. Natural disasters are by definition unpreventable, which means security professionals must manage the inevitable crises that result from them, and must institute post-event resiliency efforts. Small companies are particularly challenged to develop resiliency to natural disasters and other crises. According to the U.S. Small Business Administration, small businesses comprise 99.7% of U.S. employer firms.17 “One major problem can put these smaller organizations out of business,” notes Lawrence Berenson, Corporate Security Advisor for Avitecture, Inc., which provides integrated audiovisual IT solutions, systems, and support.

Crime. Theft and fraud from within or outside an organization are ever-present security risks. Of particular concern today is also workplace violence, which companies in the 2012 Securitas USA survey listed as second on their list of top security threats.18 The U.S. Bureau of Labor Statistics reported in 2005 that 5% of the 7.1 million private business establishments in the country experienced a violent incident within the last year, and half of the larger companies (employing more than 1,000 staff members) reported an incident.19

18 Securitas USA, 2013.
Security Industry Challenges

In addition to internal and external security risks, roundtable participants noted a variety of challenges that can impede the industry’s development and cohesiveness:

**Industry segmentation.** The immense segmentation of the security industry is one of the biggest challenges to workforce development. Because the security field includes such a wide variety of jobs, settings, and specialties, little comprehensive, industry-wide data exists. Characterized largely by specialization and silos, the industry has shown resistance to uniformity and convergence. Although many security professionals recognize the value in merging physical and informational security into one comprehensive responsibility, most find this unrealistic because very few security professionals have sufficient skills in both realms. In some cases, forced cooperation under the leadership of an executive-level security officer has been identified as necessary to ensuring a cohesive approach to organizational security.

**Aging workforce.** The security industry and security-focused educational programs are not attracting sufficient numbers of qualified people to keep up with the growing demand. One reason may be that the industry has not adequately promoted security as a career path with diverse, well-compensated opportunities beyond the entry level, and educational programs do not reflect these more complex requirements. As baby boomers retire, security industry leaders worry about a talent shortage in the next several decades. “New workers entering the industry must have access to the education, mentorships, and continuous learning opportunities that will prepare them for successful careers,” says Kathy Lavinder, Executive Director of SI Placement, a niche executive search firm serving the security industry.

**Management issues and limited resources.** Security departments across numerous industries face a host of management challenges. Most security functions exist within the corporate world, which can present challenges for those security professionals whose training and education focused on technology and physical protection systems with little

---

22 Securitas USA, 2013.
attention to business, finance, or management principles. This lack of business literacy can block security professionals from an equal place at the table in corporate strategic planning. It can also further hinder risk assessment and containment, which require comprehensive communication systems and thorough integration of security systems within overall business operations.

Roundtable participants emphasized that every employee in an organization must understand the importance of security protocols and practices, and be able to implement them. Thus security personnel must work closely with other functional areas such as human resources, training and development, and compliance. Security professionals must also work with IT departments to help ensure all staff members in the organization are able to use the latest technology to mitigate potential threats.

Security departments frequently compete for critical resources within many organizations’ limited budgets. These departments must be able to demonstrate value and return on investment (ROI) to company executives and boards of directors to secure sufficient funding for prevention tactics. Benjamin Butchko, President and CEO of Butchko Security Solutions, a firm that designs security systems, points out the hazard of failing to demonstrate ROI: "One of the biggest challenges we face is from organizations that do not perceive the security team as adding value, so they do not pay for the right protections. We as security professionals can actually create our own risk by not demonstrating that value."

The close interrelationship of business management and security poses a “provocative question,” says Steve Chupa, Director of Global Security for Medical Devices for the Johnson & Johnson Family of Companies. “Should we train business people to understand security, or should we train security people to understand business?” he asks. “As a business, we place a lot more emphasis on having a security person who understands the nuances of business and how any application of a security program affects the business in which it is applied.”

**Lack of standardized education and certifications.** Roundtable participants emphasized that additional educational standards and certifications, particularly at the entry level, would help the security industry meet organizational standards and attract a well-qualified workforce. However these measures must ensure competency in a variety of settings, according to Arminda Valles-Hall, Director of Education and Training for the Security Industry

---

23 Ernst & Young, 2012.
Arminda Valles-Hall, Director, Education and Training, Security Industry Association

“One-size-fits-all certifications may not work—as soon as we define the competencies and skills that are needed, the industry changes. Instead, we should define levels of proficiency, and let organizations determine the level they will require of a specific job.”

The risks and challenges within the security industry today call for comprehensive education and training to prepare individuals who personify what Valles-Hall calls “a whole-brain security professional”—that is, someone with business acumen as well as the technical abilities to utilize new business applications and other tools to meet specific security needs.

Mary Lynn Garcia, retired from Sandia National Laboratories, a science and engineering laboratory for national security and technology innovation, calls for an increased emphasis on STEM programs in preparing security professionals: “We should concentrate on competencies that are unique to security, and bring a science-based approach to security education programs.”

Portrait of a Security Professional: Mapping Necessary Competencies

To help address talent development needs, roundtable participants identified the fundamental competencies security professionals must attain and consistently demonstrate, regardless of their work environment.

- **Enterprise risk management.** Roundtable participants discussed the trend toward a holistic approach to enterprise risk management, which breaks down silos between physical and technological security and provides comprehensive risk management solutions. Examples include using technology such as video cameras and computerized entry systems in conjunction with security guards who protect physical buildings and property perimeters. Although nearly 60% of companies in a recent survey embraced centralized management of security systems, barriers resulting from traditional methods and professional differences remain.24 Security professionals must overcome these barriers with a continuum of experience and competency in both technological and physical security that blends the purpose and value of each.

• **Business and financial management.** Roundtable participants widely agree that security personnel need business acumen, including an understanding of financial management, to successfully deploy security strategies within organizations. Kathy Lavinder of SI Placement underscores the importance of business literacy: “Hiring managers generally prefer to hire a security person who knows business, rather than a business person who knows security.”

Business and financial skills also help security professionals make the case for the ROI of the security function. “Professionals must have a good understanding of business finance, especially in publicly traded companies, where there is an expectation to produce reasonable profits and grow the business each year,” notes Bernard Greenawalt, Vice President of Securitas Security Services USA, Inc., a locally focused security services company.

Security professionals who speak the same language as company executives can also contribute to succession planning and an overall risk management strategy that aligns with corporate goals. “Business executives want to work with security professionals who can follow them into the C-suite and talk business,” says Robert Hulshouser, a Partner at Urban Environmental Research, a consulting firm that offers public and private sector security solutions.

• **Diverse leadership and communication skills.** Security professionals must have strong interpersonal skills, including leadership and team-building strengths, to successfully collaborate with diverse groups of employees and engage them in best practices. Security team members are often charged with teaching others how to maintain security systems and follow protocols, which requires strong communication and presentation skills.

Security personnel must demonstrate leadership abilities that will inspire confidence in emergency situations as well as everyday operations. Well-honed external communication skills are also essential, because security professionals may be called upon to interact with media, law enforcement, or other public safety officials in crisis situations.

Furthermore, with the increase in globalization, security professionals must be able to exercise these competencies in complex multicultural settings. They may need an understanding of international relations, and may be called upon to implement security systems and protocols with sensitivity to local cultural norms. Global settings also require strong negotiation skills, as well as the ability to collaborate with very diverse groups of people.
• **Anticipatory and strategic thinking.** Identifying new and emerging risks and effectively responding to them are essential responsibilities. A type of question security professionals must consider, says Norman Spain, Professor of Safety, Security, and Emergency Management at Eastern Kentucky University, is, "What unintended risks are developing right now in a lab, in the social condition, or in an economic environment that will impact our organizational, national, and global security?"

Security professionals must have the vision to create a comprehensive risk management strategy to combat these imminent threats. Excellence in risk assessment means understanding the components of any crisis situation, including the systems and property affected. Once a risk is properly assessed, countermeasures must be determined, and mitigation must be planned. When an event does occur, security professionals must assemble resources and implement action plans under pressure and in volatile environments, while thinking clearly and being decisive. Managing risk also requires awareness, anticipation, and good judgment, and balancing the need for security with individual privacy rights.

• **STEM competencies.** With the convergence of physical and informational security, and with increasingly sophisticated technology, security professionals need a strong background in STEM areas: hard sciences, technology, engineering, and math. Security systems in a variety of settings often rely on biometrics, radio frequency identification systems (RFID), satellite-based surveillance and tracking, and hybrid technology cards. Security professionals must be able to work with these technologies, and understand emerging IT security solutions and systems integration processes. In addition, they must create standard operating procedures related to particular technologies, and communicate them to all areas of the organization that are called upon to implement them.

• **Specialization.** Security career opportunities span many different industries. Therefore security professionals must develop specialized expertise related to their particular sector. For example, security professionals working in healthcare must be skilled in dealing with people in emotionally stressful situations, and in community emergency management as well as patient protection and privacy. The universal nature of the security industry calls for knowledge and competencies that are both applicable to all sectors and specific to each.

Recommendations for Preparing the Security Workforce

To develop a security workforce well equipped to meet a multitude of risks and challenges, roundtable participants emphasized that the industry must better define itself by promoting its variety of dynamic career paths and required competencies. Today’s security careers span every industry, offer opportunities for specialization, and can open up paths to executive leadership roles. Security leaders need education and training that is distinct from that of law enforcement, and comprehensive enough to meet the growing need to safeguard a complex global economy.

Roundtable participants prioritized the following recommendations to help cultivate well-qualified security industry talent:

**Expedite the convergence of physical and informational security.** Enterprise risk management, and the convergence of informational and physical security, must continue to be primary industry goals. Education and training programs as well as job descriptions should emphasize these goals. “There is a critical need for more than just dialogue between the physical and informational sides of the security profession,” says Donald Fergus, Chairman, ASIS International IT Security Council, and Senior Vice President of Professional Services for Patriot Technologies, Inc., which provides IT security solutions and global logistics services. “There must be a blending of the two sides so that in 10 years the new security professional is fully experienced in both.”

A more unified approach may also facilitate industry-wide communication and collaboration to create a safer world, says Eugene Ferraro, Chief Ethics Officer of Convercent, Inc., which provides integrated compliance and analytics solutions for business. “We owe it not only to this country, but also to the free world, to think further ahead about future threats and what the solutions look like. And if we can reach consensus around these solutions, we will be in a better position to build them,” he says.

**Expand education and training programs to match industry challenges.** Roundtable participants noted that educational programs must help security professionals develop necessary competencies in risk assessment and management. The industry must focus on developing standardized curriculum and certification requirements that target entry-level
workers and span all the way to executive management. “Within the security industry, there is no common course curriculum, which is a huge problem,” says Mary Lynn Garcia, formerly of Sandia National Laboratories. “Standard principles and concepts should be taught, as in other professions.”

**Ensure that curriculum and competency standards apply to a variety of job descriptions.** Increasingly, business and STEM courses are emerging as essential requirements for security professionals; thus, interdisciplinary and integrated education programs can prepare the security workforce with a more expansive skill set. A strong business foundation can enable future leaders to link security goals with overall corporate strategies and to position security as a facilitator across business functions.27

Education for security professionals must also include experiential learning and critical thinking components that allow learners to practice skills under a variety of conditions, and apply their learning to solve complex problems. Mentoring and internships can help provide practical and cultural experience, and certification programs can train for role-specific competencies.

**Continue adapting education and training to keep security professionals current.** As security systems and technology evolve to meet emerging risks, so too must education and training programs advance. David Gilmore, Chairman of the ASIS Academic/Practitioner Symposium, recommends the industry decide “which competencies belong in an academic program and which are better suited to professional development outside the classroom.”

As the security function becomes increasingly critical, the industry must be poised to enhance its professionalism and define critical standards that will set security apart as a distinct field of study. Instituting professional standards can help to crystallize the understanding of emerging risks, and of security professionals’ responsibility for mitigating and managing them.

**Acknowledgments**

The following organizations and individuals deserve recognition for their work in making the National Roundtable on Security Talent Development a success, and for supporting the publication of this report.

**Roundtable Advisory Board**

**ASIS Foundation and ASIS International**
- **Barbara Buzzell**, Director, ASIS Foundation
- **Jim Evans**, Vice President and Chief Financial Officer, ASIS Foundation
- **John Lechner**, Director, Education Programs, ASIS International

**University of Phoenix**
- **James Ness, PhD**, Dean, College of Criminal Justice and Security, University of Phoenix
- **Caroline Molina-Ray, PhD**, Executive Director, Research and Publications, Industry Strategy Group, University of Phoenix
- **Jeff Greipp, JD**, Senior Director, Industry Strategy Group, University of Phoenix
- **Dr. Tim Welsh**, Senior Vice President, Industry Strategy Group, University of Phoenix

---

Roundtable Participants

- Lawrence K. Berenson, CPP, Corporate Security Advisor, Avitecture, Inc.
- Benjamin M. Butchko, CPP, President and CEO, Butchko Security Solutions
- Steve D. Chupa, Director, Global Security, Johnson & Johnson
- Kevin T. Doss, MS, CPP, PSP, President and CEO, Level 4 Security (L4S)
- Donald J. Fergus, CISSP, CRISC, Chairman, ASIS International IT Security Council; Senior Vice President, Professional Services, Patriot Technologies, Inc.
- Eugene F. Ferraro, CPP, CFE, PCI, SPHR, Chief Ethics Officer, Convercent, Inc.
- Mary Lynn Garcia, CPP, Former Principal Staff Member, Sandia National Laboratories
- David H. Gilmore, CPP, Chairman, ASIS Academic/Practitioner Symposium
- Bernard D. Greenawalt, CPP, Vice President, Securitas Security Services USA, Inc.
- Dr. Rae Hayward, Senior Manager, Product Development, (ISC)²
- Robert D. Hulshouser, CPP, Partner, Urban Environmental Research, LLC
- Kathy Lavinder, Executive Director, SI Placement
- Norman M. Spain, JD, Professor, Safety, Security, and Emergency Management, Eastern Kentucky University
- Arminda Valles-Hall, Director, Education and Training, Security Industry Association

Additional Contributions by University of Phoenix

Roundtable Event Support

- Corinne Lyon Kunzle, Project Manager
- Rico Singleton, Director, Technology, Industry Strategy Group, University of Phoenix

Roundtable Publication Support

- Sheila Bodell, Research Librarian
- Christine Eveker, Director, Publishing Operations, Industry Strategy Group, University of Phoenix
- James M. Fraleigh, Copy Editor and Proofreader
- Laura A. Long, Copywriter
- Graham B. Smith, Graphic Designer

Learn More

For more information about the roundtable, this report, and other workforce development initiatives, visit industry.phoenix.edu or contact IndustryStrategy@phoenix.edu.

© 2013 University of Phoenix. All rights reserved.