Competency Models for Enterprise Security and Cybersecurity

Research-Based Frameworks for Talent Solutions
About This Report

This report integrates findings from multiple, coordinated research efforts by Apollo Education Group and University of Phoenix. Drawing on interviews, focus groups, and surveys of more than 500 enterprise security and cybersecurity leaders, as well as multiple executive roundtables and industry forums featuring the additional perspectives of leaders from government and higher education, these consolidated findings reflect a consensus of key stakeholder groups in defining security workforce challenges and solutions.

A key component of this collaborative effort occurred at the National STEM Forum on Security Risks and Emerging Workforce Solutions held in Washington, DC in April 2015. Co-sponsored by Apollo Education Group and University of Phoenix, and co-hosted by STEMconnector®, the daylong forum convened experts on security practice and policy from the fields of business, government, and education. Through facilitated, cross-sector dialogue, forum panelists shared their perspectives on security risks and challenges, and discussed strategies to address workforce talent gaps and shortages in both enterprise (physical) security and cybersecurity.

Many of the forum panelists’ insights are reflected in the comments quoted throughout this report. These practitioner perspectives provide confirmation of the importance of cross-sector collaboration and alignment with industry-accepted standards for security workforce preparation, development, and advancement.

Also of note is the inclusion in this report of a globally applicable Enterprise Security Competency Model—the first of its kind in the field of enterprise security—created by Apollo Education Group in collaboration with University of Phoenix and ASIS International, and rigorously validated with input from numerous government, educational, and industry authorities from diverse sectors and geographic regions, including international contributors.

With the focus on security workforce competencies as essential to organizational competitiveness and industry leadership, this report is intended to be useful to a wide range of enterprise security and cybersecurity talent leaders—those concerned with the education, recruitment, and development of current and future security professionals. Related research can be found at apollo.edu/securityindustry.
# Table of Contents

**Introduction** 2
- Industry Snapshot: Data and Definitions 2
- Security Talent Gaps and Competency Models 2
- How To Use This Report 3

**DOL Competency Model Framework** 4
- U.S. Department of Labor (DOL) Competency Model Framework 4
  - Foundational Competencies 4
  - Industry-Related Competencies 4
  - Occupation-Related Competencies 4

**Enterprise Security** 5
- Enterprise Security Risks and Professional Competencies 5
- Enterprise Security Competency Model 5
- Implementations of the Enterprise Security Competency Model 6

**Cybersecurity** 10
- Cybersecurity Risks 10
- Cybersecurity Professional Competencies 10
- Cybersecurity Competency Model 11
- Implementations of the Cybersecurity Competency Model 12

**Last Words** 16
- Conclusion 16
- Acknowledgments 16
  - Speakers at the National STEM Forum on Security Risks and Emerging Workforce Solutions 17
- About Apollo Education Group, Inc. 17
- About University of Phoenix 17
- Learn More 17
Introduction

Industry Snapshot: Data and Definitions

Despite its market size of nearly $450 billion in the United States alone, the security industry is an often poorly understood field; its diverse, overlapping functions and sometimes non-standard terminology make precise delineations and data calculations difficult.1 Yet the risk-readiness and resilience of individuals, organizations, and entire economies depend on security systems and infrastructures that work. Running them requires a capable and informed workforce.

To further the understanding of two aspects of this industry—enterprise security and cybersecurity—a few definitions are in order. Here, enterprise security refers to the act of protecting any type of organization or structured community, including businesses, government and not-for-profit agencies, educational institutions, and even cities, states, and nations. Enterprise security—focused on protecting physical, human, financial and intellectual assets—includes operational security and IT security. Operational security entails "traditional protection activities...typically carried out by a security department," including "physical security...threat management, investigations, fraud detection, and intelligence."2 IT security—more familiar to the general public as "cybersecurity"—refers to protecting computers, systems, networks, and digital data. Worldwide, cybersecurity comprises a $71 billion market that is estimated to be more than double by 2019.3

Security Talent Gaps and Competency Models

As interconnected fields, enterprise security and cybersecurity share a common challenge: a deficit of qualified professionals to meet the growing demand for skilled and job-ready talent. Of the roughly 1.8 million private-sector security professionals in the United States, about two-thirds work in operational security; yet nearly 60% of the most recent security-related job growth is projected to be in IT security.4 In a 2015 global survey of nearly 14,000 information security professionals, 62.2% of respondents reported a lack of qualified workers in the profession.5 Even though the cybersecurity field is projected to grow by 1.3 million workers worldwide by 2019, that level of growth will still leave a global workforce shortfall of nearly 700,000 cybersecurity professionals.6

The lack of human capital is one of the biggest challenges in the cybersecurity industry.
—Jeff Snyder, Vice President, Cyber Programs, Raytheon

Security talent gaps have driven employers and educators to re-examine the use of competency models as tools to define and assess worker qualifications and skills. A competency is defined as the knowledge, 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.7 A competency model is a structured collection of competencies that define successful performance in a particular role, occupation, or industry.8

The U.S. Department of Labor (DOL) has developed, collected, and published a comprehensive set of general and industry-specific competency models and related tools that employers and educators can use for multiple talent-related purposes, including developing curriculum and job descriptions, evaluating and hiring job candidates, and measuring employee performance.9 However, until recently, no standard, industry-recognized competency models existed for the enterprise security and cybersecurity industries. Yet the rising demand for skilled professionals in these fields—coupled with the challenge to educate and train workers at a pace that keeps up with the

---

Physical and cybersecurity cannot be separated. We live in a world of blended threats.
—Paul Kolbe, Director, International Security Affairs, BP

demand—has led to the unprecedented collaboration of leaders in higher education, industry, and government to create, validate, adopt, and disseminate a standard-setting model for enterprise security, and a similar model for cybersecurity. Both models are presented in this report.

How To Use This Report

This report differs from previous research in that it addresses two sides of the security industry: enterprise security and cybersecurity. In addition, by presenting industry-standard competency models for both fields, this report enables readers to identify overlaps and distinctions that can aid in the education, recruitment, and development of workers in both professions.

Spearheaded by Apollo Education Group in collaboration with University of Phoenix and the ASIS Foundation, the recent creation of the Enterprise Security Competency Model presented in this report represents the culmination of years of custom research, including surveys and interviews of more than 500 security professionals as well as multiple roundtables, focus groups, and executive forums comprising industry association leaders, employers, talent recruitment and development professionals, higher education leaders, and students. The result is a first-of-its-kind competency model for the enterprise security field, validated by leading national and international authorities on career-focused education, including the U.S. Department of Labor and numerous global employers and educators.10

Similarly, the Cybersecurity Competency Model presented in this report reflects the pyramidal structure of the Department of Labor’s general competency model and incorporates competencies from the National Cybersecurity Workforce Framework developed by the National Initiative for Cybersecurity Education (NICE). Apollo Education Group and University of Phoenix collaborated with (ISC)² and the Council on Cybersecurity to help validate the model and used it as a basis for designing action steps to close cybersecurity workforce gaps.11

The comments from subject matter experts throughout the report are intended to provide a sampling of the cross-sector dialogue that both reinforces the industry research and provides supplemental, often practical, perspectives on implementing solutions to current and emerging workforce challenges.

Through both variety and consistency, these comments underscore the urgency of collaborative efforts among employers, educators, and policymakers to build a qualified, sustainable security talent pool.

Several stakeholder groups may benefit by using the competency models and other insights from this report.

- **Hiring managers** are encouraged to use the competency models as tools to identify the skills, knowledge, and attributes for specific roles, and to track employees’ performance and skill development against the identified competencies.

- **Talent leaders** may use the models to develop recruitment, screening, and selection tools as well as career paths. The models can also serve as a resource to ensure the relevance and completeness of training offerings and career advancement programs.

- **Higher education curriculum designers** can benefit by integrating identified competencies into educational programs, and by offering assignments and work-simulation activities that enable students to demonstrate proficiency.

- **Professional development content developers** can create targeted training focused on building or enhancing one or more of the identified competencies.

- **Career counselors** can draw on the models to pinpoint strengths and gaps in a job seeker’s credentials.

- **Industry associations** are encouraged to socialize the competency models among their members and to solicit feedback on the models’ effectiveness and uses. This feedback can be shared with the models’ authors to facilitate ongoing updates and refinements.

- **Policymakers** may find the models helpful in designing public programs and policies that support career-focused training and employment opportunities.

---

The competency models presented in this report use the U.S. Department of Labor’s Competency Model Clearinghouse public toolkit as an organizing framework. To assist businesses, educators, and workforce development professionals in identifying the industry-specific skills and competencies that workers will require, the framework consists of a set of building blocks arranged into nine tiers containing specific sets of related competencies. The DOL explains the rationale for the model’s structure as follows:

The arrangement of the tiers in a pyramidal shape represents the increasing level of specificity and specialization of content. As a user moves up through the various tiers of the model, the competencies become specific to certain industries and/or occupations.

In the framework, the nine tiers are grouped into three clusters: foundational competencies, industry-related competencies, and occupation-related competencies. Based on DOL definitions, these clusters can be described as follows:

**Foundational Competencies**

Tiers 1 through 3 at the bottom of the pyramid represent baseline competencies that are required of virtually any individual in the workforce. Together, they constitute “employability skills” that are common across industries and occupations.

On Tier 1 are **Personal Effectiveness Competencies**—characteristics such as integrity, reliability, and adaptability—which individuals generally begin to develop early in life as part of their personal values. These attributes can be learned at home, in school, or through affiliations with religious or other values-based communities (e.g. Boy Scouts).

Tier 2 consists of **Academic Competencies** such as reading, writing, and critical thinking, which are generally learned and refined through formal education (primary, secondary, and postsecondary).

Tier 3 includes **Workplace Competencies** such as teamwork, planning, and organizing, which are essential to performing almost any job-related function.

**Industry-Related Competencies**

The second cluster, spanning Tiers 4 and 5, contains **Industry-Related Competencies** that are specific to an industry or industry subsector, but not specific to any occupation or role. Individuals who demonstrate these competencies have skills that are transferrable across roles and occupations within the industry.

Tier 4 houses **Industry-Wide Technical Competencies**. Examples of these in the enterprise security industry are risk management and crisis management. Because these types of competencies cut across roles and occupations, they facilitate workforce mobility within the industry. Since they are broad-ranging and not associated with specific roles, these competencies generally involve “awareness or understanding, rather than performing specific job tasks.”

On Tier 5 are **Industry-Sector Functional Areas**. Examples for enterprise security are the various industry sectors in which enterprise security functions are critical, such as manufacturing, banking and finance. The competencies of workers in these sectors would reflect a combination of general security-industry skills (Tier 4) and specialized industry-sector skills (Tier 5) that enable functioning at the “crossroads” of two industries.

**Occupation-Related Competencies**

Occupation Competencies are located on Tiers 6 through 8 of the pyramid. They are highly specific to roles in the relevant industry. They may be used to define job performance criteria, identify the requirements for a specific credential (e.g. professional license or certification), or to create curriculum for career-focused educational offerings. Because of their specificity and uniqueness to the jobs at hand, competencies on these tiers are generally not

---

**Competency** – A cluster of related knowledge, skills, and abilities that affects one’s job, correlates with job performance, can be measured against well-accepted standards, and can be improved through training, development, and experience.
Enterprise Security

pre-defined by the DOL, but formulated by the respective talent manager or industry professional responsible for delineating the requirements for a position or role. The DOL’s Competency Clearinghouse website provides other resources, including instructional videos and interactive tools, to support profession-specific competency mapping.16

Enterprise Security Risks and Professional Competencies

In preparation for the development of the Enterprise Security Competency Model and the creation or refinement of career-relevant security educational offerings, Apollo Education Group and its subsidiary, University of Phoenix, undertook a series of research activities in partnership with the security professional association ASIS International and its research arm, the ASIS Foundation. Through expert interviews, an industry executive roundtable, and a survey of security industry leaders working across the United States in various economic sectors, researchers gathered input from more than 500 respondents on emerging security risks and professional competencies.17 The results are summarized on p. 6.

Enterprise security leaders largely agree on the key risks that organizations will face in the immediate future, as well as on the competencies that security professionals must demonstrate to mitigate and manage those risks. In addition to the most critical competencies noted on p. 6, researchers identified more than a dozen other competencies—spanning technical, industry-specific, and “soft” skills—that security professionals will need to demonstrate to perform their jobs. A full list of the competencies and their definitions is included on page 7.

Enterprise Security Competency Model

Using the identified security professional competencies as a baseline, Apollo Education Group adapted the DOL’s generic competency model pyramid to reflect industry-specific technical, workplace, academic, and personal effectiveness competencies. The model was modified and validated with input from the DOL, the ASIS Foundation, University of Phoenix, Bridge School of Management (an Apollo Education Group subsidiary in India), and more than 125 employers and subject matter experts, including international stakeholders. The resulting schematic, illustrated on p. 9, is now featured on the Department of Labor’s CareerOneStop Competency Clearinghouse website.18

DOL Competency Model Framework

OCCUPATION RELATED

INDUSTRY RELATED

FOUNDATIONAL

Occupation-Related Competencies
Tier 9 – Management Competencies
Tier 8 – Occupation-Specific Requirements
Tier 7 – Occupation-Specific Technical Competencies
Tier 6 – Occupation-Specific Knowledge Competencies

Industry-Related Competencies
Tier 5 – Industry-Sector Technical Competencies
Tier 4 – Industry-Wide Technical Competencies

Foundational Competencies
Tier 3 – Workplace Competencies
Tier 2 – Academic Competencies
Tier 1 – Personal Effectiveness Competencies

Source: CareerOneStop.

Implementations of the Enterprise Security Competency Model

The Enterprise Security Competency Model is being applied in academic, professional development, and business settings. ASIS International offers security professional certificate programs that were designed using content from the model. These programs—developed in collaboration with GSX (Global Skills X-Change) and Pherson Associates—align with the talent development needs of the enterprise security, defense, and intelligence communities.

Top 5 security risks that enterprises will face in the next 3 years

1. Cybersecurity
2. Crime
3. Mobile technology
4. Natural Disasters
5. Globalization

Most critical security professional competencies

- STEM literacy
- Oral communication
- Maximizing others’ performance
- Decision making
- Critical thinking
- Persuasive influencing

Source: Apollo Education Group, University of Phoenix, and ASIS Foundation.

**Enterprise Security Competency Definitions**

**Aligning Organizational Objectives**—Identifies and implements security-related goals that align with overall corporate goals and comply with regulatory standards.

**Anticipatory Thinking**—Proactively seeks to identify potential security industry risks, and develops and implements strategic plans to address long- and short-term goals to ensure organizational preparedness to mitigate and respond to risks.

**Balancing Priorities**—Takes actions that demonstrate appropriate balance between security needs and the rights of individuals.

**Business and Financial Literacy**—Exhibits sufficient business, financial, and legal understanding to speak the language of company executives, make the case for the ROI of the security function, develop meaningful security-related business recommendations, and successfully deploy security strategies that align with corporate goals.

**Collaboration**—Accomplishes security-related work activities and goals by effectively working with a diverse group of people in a team environment and engaging others in best practices.

**Critical Thinking**—Gathers and analyzes data, using logic and reasoning, to make sound short- and long-term security-related business decisions.

**Decision Making**—Makes sound, fact-based, and timely security-related decisions, even when under pressure, that reflect the long- and short-term security interests of the organization.

**Enterprise Risk Assessment**—Proactively uses knowledge of risk assessment theories and crisis indicators to effectively recognize crisis situations or potential disasters.

**Enterprise Risk Management**—Takes a holistic approach to risk management, working to break down silos between physical and technological security and provide comprehensive risk management solutions.

**Global Awareness**—Understands global security issues and how the organization will compete to successfully achieve security-related business objectives worldwide.

**International and Multicultural Competence**—Seeks understanding of perspectives, traditions, values, and practices of culturally diverse individuals and applies understanding to perform security-related tasks effectively.

**Maximizing Performance of Others**—Supports, encourages, and helps other security professionals achieve their full potential, coaching and providing effective learning resources and experiences to help other security professionals maintain security systems and follow protocols.

**Message Development**—Develops and delivers appropriate messages that need to be communicated to stakeholders (e.g., to media, law enforcement, public safety officials), especially in emergency situations.

**Multicultural Versatility**—Adapts own behavior to demonstrate proper and culturally appropriate behavior when dealing with others from different cultures and countries on security-related issues.

**Oral Communication**—Expresses thoughts verbally in a clear, succinct, logical, and organized manner.

**Organizational Compliance**—Develops, follows, and enforces standard security operating procedures and crisis/emergency protocols (e.g., using Direction, Control, and Warning).

**Persuasive Influencing**—Uses compelling communication to persuade others (e.g., organizational executives) to listen and commit to, and act on, security-related issues.

**Public Speaking**—Delivers polished and persuasive presentations, confidently and credibly, when addressing diverse groups of people within and outside the organization.

**Security-Related Literacy**—Stays abreast of security industry trends and best practices, and maintains access to current industry data to inform organizational decision-making and operations.

**Self-Regulation**—Remains in control and calm when under pressure to identify resources and lead others when responding to and recovering from emergency situations.

**Succession Planning**—Anticipates long-range security staffing needs and develops the internal talent necessary to support the organization’s strategy.

**Technological Excellence**—Proactively seeks to maintain and expand hard science, technology, engineering, and math (STEM) knowledge needed to perform tasks involving security-related technologies (e.g., biometrics, radio frequency identification systems, satellite-based surveillance and tracking systems, hybrid technology cards) and understand emerging IT security solutions and system integration processes.

*The security industry is moving toward using the term enterprise security risk management to designate this competency.

In the academic community, Missouri Baptist University (MBU) has been at the forefront among educational leaders in using the Enterprise Security Competency Model for curriculum development and delivery of security offerings. The model is being used in the design of MBU’s Master of Science degree program in Corporate Security Leadership to ensure that course content reflects the model’s terminology and tiered approach to competency building.

At MBU, students learn Tier 1 (Personal Effectiveness) competencies through observation of instructors’ role-modeling behavior and through explicit coverage of these competencies in courses such as “Ethical Security Leadership” and “Security Law and Compliance.” Because Tier 2 (Academic) competencies form the substance of MBU students’ scholastic preparation, a list of those skill sets can help facilitate the assessment of both the students’ proficiency and the instructors’ effectiveness. Students demonstrate Tier 3 (Workplace) competencies in the capstone phase of their MBU coursework, as they are challenged to integrate all three tiers of foundational competencies in preparation for entering or advancing in a security career.

In the business community, the Human Resources (HR) department of a Fortune 100 technology firm is using the Enterprise Security Competency Model to conduct a market analysis of job titles and descriptions with current and required workforce skills to identify gaps. Where appropriate, job descriptions are being rewritten to reflect the competencies included in the model. As a standardizing factor in the creation of job descriptions, the model facilitates consistency, comparability, and equitability among role definitions. This rational approach to job definitions helps to reduce “job creep” that can occur when extraneous responsibilities are integrated into a role without consideration of the impact on the scope or level of the position or its place on a career path.

Similar business uses of the model could be applied in learning and development functional areas to assess training needs, update talent development programs, and aid in succession planning. At the organizational level, the model can assist talent leaders with overall workforce planning and advancement. At the individual level, the model can help with career preparation and progression.

Preparing security professionals requires a holistic approach focused on developing STEM literacy, soft skills, industry-specific knowledge and business acumen.

—Mark A. Arnold, Director of Information Security, PTC

There’s no such thing as completing one’s education in the security industry. Security professionals need to continually update their skills, and employers must support ongoing education.

—Linda F. Florence, President, ASIS Foundation Board of Trustees

The Enterprise Security Competency Model is an excellent demonstration of the results that can be achieved through the collaboration of industry and educational organizations.

—Bernard D. Greenawalt, Vice President, Securitas USA

Preparing security professionals requires a holistic approach focused on developing STEM literacy, soft skills, industry-specific knowledge and business acumen.

—Mark A. Arnold, Director of Information Security, PTC

There’s no such thing as completing one’s education in the security industry. Security professionals need to continually update their skills, and employers must support ongoing education.

—Linda F. Florence, President, ASIS Foundation Board of Trustees

The Enterprise Security Competency Model is an excellent demonstration of the results that can be achieved through the collaboration of industry and educational organizations.

—Bernard D. Greenawalt, Vice President, Securitas USA
Enterprise Security Competency Model

Source: CareerOneStop.
Cybersecurity Risks

While security professionals in our national survey named cybersecurity as the #1 risk that enterprises are likely to face in the next 3 years, cybersecurity leaders have somewhat differing opinions on which threats will be most critical. In a Raytheon-sponsored study of 1,125 globally dispersed IT and IT security leaders, 49% of respondents predicted the #1 threat would be “zero-day” attacks—attacks on software vulnerabilities that the hacker discovers before they are repaired by the developer. “Zero-day” refers to the same-day responsiveness that is necessary to thwart this type of attack—usually by issuing a “patch” or software update that fixes the problem.

After zero-day attacks, the Raytheon study, conducted by the Ponemon Institute, identified a number of additional cybersecurity risks believed to be most threatening; rounding out the top five are cloud data leakage, mobile malware/targeted attacks, SQL injection (the insertion of malware into the developer’s code) and phishing attacks (attempts to uncover sensitive personal or financial information).20 (See graphic of cyber threats on p. 11.)

Public safety and homeland security jobs are STEM jobs. Whether we are dealing with natural or technical disasters, man-made attacks or disease outbreaks—the responses always involve the application of one or more STEM disciplines.

—Brian J. Moran, Secretary of Public Safety and Homeland Security, Office of the Governor of Virginia

Cybersecurity Professional Competencies

In the face of evolving cybersecurity risks, IT security professionals in an Apollo Education Group research study identified key competencies needed to prevent, mitigate, and manage imminent threats.22 (See Cybersecurity Competencies on p. 13.)
Cybersecurity Competency Model

In an effort to define a common set of cybersecurity competencies, the National Initiative for Cybersecurity Education (NICE) developed the National Cybersecurity Workforce Framework (see p. 14), and the U. S. Department of Labor developed the Cybersecurity Competency Model (see p. 15). The NICE Framework describes cybersecurity work across industries, organizations, and job types, and consists of seven categories, with 31 specialty areas.23 For each specialty area, the Framework identifies the job tasks, knowledge, skills, and abilities that individuals must demonstrate to perform effectively. The seven categories represent typical job duties performed by cybersecurity professionals.

Incorporating the competencies of the NICE Framework, the DOL's Cybersecurity Industry Competency Model expands the Framework by including the competencies needed "to safely interact with cyberspace."24 The DOL's familiar "building block"-style pyramid displays the competencies required by various levels of cybersecurity professionals—from entry-level to...

"By the year 2020 cybersecurity will be...

...a well-defined set of career paths.”
—Greg Simmons, Vice President for Institutional Advancement, UMBC

...a passé term. Threat prevention capabilities will be embedded in machines.”
—Doug Benefield, Chief Executive Officer and President, CIPHIR Tech

...a problem we are still trying to solve.”
—Randi Parker, Director, Public Advocacy, CompTIA

Top 5 Cyber Threats in the Next 3 Years (Ponemon Institute)
(% of survey respondents identifying each threat)

- Zero-Day Attacks: 49%
- Cloud data leakage: 41%
- Mobile malware/targeted attacks: 38%
- SQL Injection: 37%
- Phishing Attacks: 36%

Source: Ponemon Institute, 2015.

manager or senior leader. The bottom tiers reflect the soft skills needed by all individuals whose work affects cybersecurity: personal effectiveness, academic, and workplace skills. The middle tiers contain the industry-level technical and functional competencies needed by individuals industry-wide or in particular sectors. The top tiers include management competencies and occupation-specific requirements.

**Implementations of the Cybersecurity Competency Model**

The Cybersecurity Competency Model serves as a multifaceted tool for cybersecurity workforce planning, performance management, and articulation of career pathways and educational requirements. It promotes broad understanding of the cybersecurity field and provides a holistic view of organizational components, functions, and roles. It also helps to codify the industry’s cohesion through the shared elements of foundational and industry-wide skills across subsectors and occupations.

The global leader in educating and certifying information security professionals, (ISC)²—the International Information System Security Certification Consortium—has effectively implemented the Cybersecurity Competency Model by mapping job tasks to the knowledge units in the NICE Framework (which are also present in the competency model) to help academics develop the curriculum for two critical industry certification programs, the CISSP (Certified Information Systems Security Professional) and SSCP (Systems Security Certified Practitioner).¹² Both certifications are vendor-neutral and globally recognized as gold-standard credentials.

---

¹² See (ISC)², Credentials. https://www.isc2.org/credentials/default.aspx

---

### Top 5 Cyber Threats in 2015

(ThreatTrack® Security)

<table>
<thead>
<tr>
<th>Threat</th>
<th>% of Survey Respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Persistent Threats</td>
<td>65%</td>
</tr>
<tr>
<td>Targeted Malware Attacks</td>
<td>61%</td>
</tr>
<tr>
<td>Spear Phishing</td>
<td>42%</td>
</tr>
<tr>
<td>Zero-Day Attacks</td>
<td>33%</td>
</tr>
<tr>
<td>Insider Threats</td>
<td>33%</td>
</tr>
</tbody>
</table>

### Cybersecurity Competencies

<table>
<thead>
<tr>
<th>Key Knowledge Focus Areas</th>
<th>Key Skills</th>
<th>Key Abilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Common cybersecurity concepts</td>
<td>• Advanced Internet search skills</td>
<td>• Adaptability</td>
</tr>
<tr>
<td></td>
<td>• Assessing risks</td>
<td>• Assertiveness</td>
</tr>
<tr>
<td>• Contractual and regulatory language</td>
<td>• Data analytics Prioritizing</td>
<td>• Confidence</td>
</tr>
<tr>
<td>Documentation policies</td>
<td>• Business acumen (ability to make profitable business decisions)</td>
<td>• Cultural Awareness</td>
</tr>
<tr>
<td>• Forensics</td>
<td>• Business analytical skills (ability to identify business needs and确定 solutions to business problems)</td>
<td>• Willingness to learn</td>
</tr>
<tr>
<td>• Industry best practices</td>
<td>• Change management</td>
<td></td>
</tr>
<tr>
<td>• IPV6 (International Protocol Version 6)</td>
<td>• Customer service skills</td>
<td></td>
</tr>
<tr>
<td>• Legal terms</td>
<td>• Interpersonal skills</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Marketing skills</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Negotiation skills</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Platform-specific technical skills</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Sales skills</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Teamwork skills</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Vendor management</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Written and verbal communication skills</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Vendor management</td>
<td></td>
</tr>
</tbody>
</table>

Source: Apollo Education Group and University of Phoenix, *Competencies and Certifications for Information Security Careers.*
Categories of the National Initiative for Cybersecurity Education (NICE) National Cybersecurity Workforce Framework

**SECURELY PROVISION** Specialty areas responsible for conceptualizing, designing, and building secure IT systems (i.e., responsible for some aspect of systems development).

**OPERATE AND MAINTAIN** Specialty areas responsible for providing support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security.

**PROTECT AND DEFEND** Specialty areas responsible for identification, analysis, and mitigation of threats internal to IT systems or networks.

**INVESTIGATE** Specialty areas responsible for investigation of cyber events and/or crimes of IT systems, networks, and digital evidence.

**COLLECT AND OPERATE** Specialty areas responsible for specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.

**ANALYZE** Specialty areas responsible for highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.

**OVERSIGHT AND DEVELOPMENT** Specialty areas providing leadership, management, direction, and/or development and advocacy so that individuals and organizations may effectively conduct cybersecurity work.

ISC² is also working on integrating content from the NICE Framework into an online career map showing entry-level through executive cybersecurity roles and the education, skills, and job responsibilities required for each role. Ideally, the map will also identify lateral and ascending promotional pathways from one role to the next, so that it can be used as a tool for career planning.

“Employers need to provide clear job descriptions and security career paths.”

—José Raúl Perales, Assistant Secretary, U.S. Department of Homeland Security

In the academic arena, the Cybersecurity Competency Model serves as a tool for instructional design at higher education institutions, including University of Phoenix, where the College of Information Systems and Technology draws on the model as a curriculum development framework and guide as it continues to expand its cybersecurity offerings in alignment with industry-required competencies.

Adapted from NICE, The National Cybersecurity Workforce Framework.
DOL Cybersecurity Competency Model

Tier 1 - Personal Effectiveness Competencies
- Interpersonal Skills & Teamwork
- Integrity
- Professionalism
- Initiative
- Adaptability-Flexibility
- Dependability-Reliability
- Lifelong Learning

Tier 2 - Academic Competencies
- Reading
- Writing
- Mathematics
- Science
- Communication
- Critical & Analytic Thinking
- Fundamental IT User Skills

Tier 3 - Workplace Competencies
- Teamwork
- Planning & Organizing
- Creative Thinking
- Problem Solving & Decision Making
- Working with Tools & Technology
- Business Fundamentals

Tier 4 - Industry-Wide Technical Competencies
- Cybersecurity Technology
- Information Assurance
- Risk Management
- Incident Detection
- Incident Response and Remediation

Tier 5 - Industry-Sector Functional Areas
- Security
- Provision
- Operate and Maintain IT Security
- Protect and Defend From Threats
- Investigate Threats
- Collect Information and Operate Cybersecurity Process
- Analyze Information
- Oversee and Govern Cybersecurity Work

Source: CareerOneStop.
Conclusion

Enterprise security and cybersecurity are distinct yet intertwined fields that comprise huge global markets and affect virtually every industry. As evolving risks influence these fields and drive up the demand for qualified talent, current and aspiring security professionals must demonstrate an expanded array of competencies to be able to prevent, mitigate, and manage these risks. The industry-standard competency models presented in this report can help employers, educators, and talent specialists to prepare, develop, and advance the enterprise security and cybersecurity workforce of the future.

Acknowledgments

Apollo Education Group and University of Phoenix wish to thank the following organizations for helping to facilitate the research that formed the basis for this report: ASIS International, the ASIS Foundation, the Council on Cybersecurity, (ISC)², STEMconnector®, and the U.S. Department of Labor. Special thanks belong to the speakers at the National STEM Forum on Security Risks and Emerging Workforce Solutions, whose contributions provided practical insights to enrich the research findings presented here. Additional subject matter experts include Mark H. Beaudry, PhD, CPP; Bernard D. Greenawalt, CPP; Rae Hayward, PhD; Daniel McGarvey; and Loftin C. Woodiel, PhD, CPP.

Speakers at the National STEM Forum on Security Risks and Emerging Workforce Solutions

Cynthia V. Anderson, Senior Advisor, Office of Policy, Nuclear Security Administration, U.S. Department of Energy
Mark A. Arnold, PhD, Director of Information Security, PTC
Edward Beck, Chief Information Officer and Senior Vice President, National Restaurant Association
Doug Benefield, Chief Executive Officer and President, CIPHIR Tech
Dennis Bonilla, Executive Dean, College of Information Systems and Technology, University of Phoenix
Donald G. Brady, Assistant Dean of STEM, Middlesex Community College
Mark Brenner, Senior Vice President, Business Development, Corporate Communications and External Affairs, Apollo Education Group
Guy Delp, Director, Cyber and Data Analytics Engineering, Lockheed Martin
Bob Fahy, Director, Global Security, Monsanto
Linda F. Florence, PhD, CPP, President, ASIS Foundation Board of Trustees
Edie Fraser, Chief Executive Officer, STEMconnector®
Dr. Stephen D. Gantz, Chief Security and Privacy Officer, Cognosante
Jeff Greipp, JD, Group Vice President, Apollo Education Group
Sharon C. James, Associate Chief Information Officer, Cybersecurity, Internal Revenue Service
The Honorable Mark T. Kimmitt, Brigadier General, US Army (ret.), Former Assistant Secretary of State for Political-Military Affairs, U.S. Department of State
Paul Kolbe, Director, International Security Affairs, BP
Jamie Lopez, PhD, Senior Associate, Booz Allen Hamilton

Too often when we talk about partnerships, we’re describing adjacencies. Employers and educators need to collaborate across domains.

— Greg Simmons, Vice President for Institutional Advancement, UMBC
Spider Marks, Executive Dean, College of Security and Criminal Justice, University of Phoenix

Brian J. Moran, Secretary of Public Safety and Homeland Security, Office of the Virginia Governor

Derrick Nixon, Senior Director, Security Solutions, Honeywell Technology Solutions, Inc.

Jane Oates, Vice President, External Affairs, Apollo Education Group

Randi Parker, Director, Public Advocacy, CompTIA

José Raúl Perales, Assistant Secretary for the Private Sector, Office of Policy, U.S. Department of Homeland Security

Greg Simmons, Vice President for Institutional Advancement, University of Maryland, Baltimore County (UBMC)

Jeff Snyder, Vice President, Cyber Programs, Raytheon

David Stender, Senior Vice President and Enterprise Security Officer, M&T Bank

Kari R. Strobel, PhD, Director, HR Competencies, Society for Human Resource Management

A. Spencer Wilcox, CISSP, CPP, Special Assistant to the Chief Security Officer - Managing Security Strategist, Exelon

About Apollo Education Group, Inc.

Apollo Education Group, Inc. is one of the world’s largest private education providers and has been in the education business since 1973. Through its subsidiaries: Apollo Global, College for Financial Planning, University of Phoenix, and Western International University, Apollo Education Group offers innovative and distinctive educational programs and services, online and on-campus, at the undergraduate, master’s and doctoral levels. Its educational programs and services are offered throughout the United States and in Europe, Australia, Latin America, Africa and Asia, as well as online throughout the world. For more information about Apollo Education Group, Inc. and its subsidiaries, call (800) 990.APOL or visit the Company’s website at www.apollo.edu.

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. As a subsidiary of Apollo Education Group, Inc. (Nasdaq: APOL), 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.

The College of Security and Criminal Justice at University of Phoenix offers undergraduate and graduate degree programs with management-focused curriculum to help students develop the skills required to be leaders within the security industry and other related fields. For more information, visit phoenix.edu/scj.

The College of Information Systems and Technology at University of Phoenix offers industry-aligned certificates as well as associate, bachelor’s, and master’s degree programs designed to equip students for successful IT careers. Through the College’s StackTrack™ program, students can obtain “en route” certificates while working toward a degree, without increasing cost or time to graduation. The College’s interactive curriculum gives students virtual access to tools commonly used by IT professionals and to training courseware that further prepares students for industry certification. For more information, visit phoenix.edu/technology.

Learn More

Apollo Education Group and its subsidiaries work with industry leaders to conduct talent management research and to design innovative human capital solutions. Download our security industry reports or contact us at apollo.edu/securityindustry.

© 2015 Apollo Education Group, Inc. All rights reserved.