University of Phoenix®

(ISC)²

(ISC)² FOUNDATION

Cybersecurity Workforce Competencies:

Preparing Tomorrow's Risk-Ready Professionals

About Us

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 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**.

Apollo Education Group's **Industry Strategy** team offers research and advisory solutions to help industries meet national and global talent development needs. Partnering with national and international industry associations, the Industry Strategy team helps industry leaders define the educational requirements for career success. With these insights, the Industry Strategy team helps University of Phoenix and other Apollo Education Group institutions continually adapt educational offerings and career-support services to develop career-ready industry talent. The Industry Market Insights Center, part of the Industry Strategy team, helps to inform the team's collaborative, research-based mission. For more information, visit **industry.phoenix.edu**.

About (ISC)²®

Formed in 1989 and celebrating its 25th anniversary, (ISC)² is the largest not-for-profit membership body of certified information and software security professionals worldwide, with 100,000 members in more than 135 countries. Globally recognized as the Gold Standard, (ISC)² issues the Certified Information Systems Security Professional (CISSP®) and related concentrations, as well as the Certified Secure Software Lifecycle Professional (CSSLP®), the Certified Cyber Forensics Professional (CCFPSM), Certified Authorization Professional (CAP®), HealthCare Information Security and Privacy Practitioner (HCISPPSM), and Systems Security Certified Practitioner (SSCP®) credentials to qualifying candidates. (ISC)²'s certifications are among the first information technology credentials to meet the stringent requirements of ISO/IEC Standard 17024, a global benchmark for assessing and certifying personnel. (ISC)² also offers education programs and services based on its CBK®, a compendium of information and software security topics. More information is available at **www.isc2.org**.

About the (ISC)²® Foundation

The (ISC)² Foundation is a non-profit charitable trust that aims to empower students, teachers, and the general public to secure their online life by supporting cybersecurity education and awareness in the community through its programs and the efforts of its members. Through the (ISC)² Foundation, (ISC)²'s global membership of 100,000 information and software security professionals seek to ensure that children everywhere have a positive, productive, and safe experience online, to spur the development of the next generation of cybersecurity professionals, and to illuminate major issues facing the industry now and in the future. For more information, please visit **www.isc2cares.org**.

About This Report

This report is based on the findings from an industry roundtable with cybersecurity professionals and talent development leaders, co-hosted by University of Phoenix and the (ISC)² Foundation. The objective of the session—part of an ongoing effort to investigate the competencies and career priorities of cybersecurity professionals—was to identify actionable recommendations for key stakeholders to better prepare students to enter careers in cybersecurity. The focus was on identifying what educational institutions, employers, industry associations, and students can do to bridge three education-to-workforce gaps: a competency gap, a professional experience gap, and an education speed-to-market gap.

Roundtable participants included representatives from institutions of higher education that educate cybersecurity professionals; organizations that employ cybersecurity professionals; industry associations that support and provide certifications to cybersecurity professionals; and the U.S. Department of Labor, which develops research and tools for workforce prosperity and advancement. The roundtable also incorporated the perspective of a cybersecurity student/career-starter on higher education practices and career entry.

Cybersecurity experts and other thought leaders with relevant experience in competency modeling, higher education, cybersecurity services, and cybersecurity credentialing engaged in facilitated discussion and participated in breakout sessions to identify actionable recommendations for better preparing the future cybersecurity workforce. This report summarizes those recommendations. The findings are designed to be useful to the larger community of industry leaders, employers, educators, and current or future cybersecurity professionals.

Contents

Executive Summary

The need for cybersecurity professionals is rising as individuals, organizations, and industries increasingly use data networks for business, commerce, and protection of sensitive information. With the frequency, sophistication, and cost of cyberattacks on the rise, investing in wide-scale cybersecurity has become a priority for corporate and public leaders.

Although the cybersecurity field is growing quickly and offers competitive pay, demand for these IT specialists exceeds the supply of credentialed, experienced professionals. To aid in building a pipeline of cybersecurity talent, industry leaders are calling for a common definition of the scope of cybersecurity work and the competencies that job candidates must demonstrate.

Establishing Cybersecurity Professional Competencies

Two sets of competencies—the National Initiative for Cybersecurity Education (NICE) National Cybersecurity Workforce Framework, and the U.S. Department of Labor (DOL) Cybersecurity Industry Competency Model—have been developed to standardize professional requirements.

The NICE Framework defines seven categories of typical job duties, covering cybersecurity work in 31 specialty areas across industries and job types. The DOL's model expands this Framework to include the competencies required at various career tiers. It includes soft skills, technical and functional competencies for specific sectors and the overall profession, and management and occupation-specific requirements.

Closing Education-to-Workforce Gaps

Stakeholders have identified three education-to-workforce gaps that are hindering efforts to fill cybersecurity jobs with qualified workers. These include gaps in competency, professional experience, and education speed-to-market. The report includes recommendations for employers, industry associations, higher education institutions, and cybersecurity students to play a role in closing the gaps. The recommendations are designed to improve alignment of educational content with workplace problems; boost the employability and ethics of cybersecurity students and aspiring professionals; and foster continuous professional development through networking, organizational memberships, and certifications.

Stakeholders have also defined the action items that could have the most immediate impact on closing the gaps:

- Higher education programs should integrate problem-based learning via case studies and labs.
- Higher education institutions should partner with employers to promote internships for cybersecurity degree completion.
- Students should seek stakeholder guidance and take appropriate steps to position themselves for employment.

Introduction: Cybersecurity Industry Snapshot

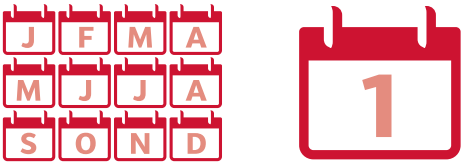
Cybersecurity, or the practice of protecting electronic data from unlawful or unplanned use, access, modification, or destruction,[1] is more critical today than ever. Due to the growing numbers of data networks, digital applications, and mobile users—and the increased number and sophistication of cyberattacks—ongoing vigilance is needed to protect private and proprietary information.

As the United States increasingly relies on networks to collect, process, store, and transmit confidential data, the work of cybersecurity professionals is essential to protecting the online activities of individuals, organizations, and communities.[2] The Internet of Things (IoT)—the ability of everyday objects to transmit data through a network—increases the vulnerability of virtually all aspects of life to cyber threats. In IoT, embedded chips in all manner of "smart" objects—an automotive sensor, insulin pump, jet engine, or oil drill—become the potential "victims" of breaches or outages. Without adequate security, data breaches can result in outcomes ranging from minor inconveniences to personal, corporate, or government disasters with devastating consequences for individuals, enterprises, regional populations, or the global economy.

Recognizing that no organization is immune to cybersecurity threats, company leaders are increasingly making cybersecurity an operational priority. After the widely reported cyberattacks on leading retailers (Target and Neiman Marcus), financial services companies (JPMorgan Chase), and technology-based companies (eBay, Adobe, and Snapchat),[3] business leaders agree that boosting cybersecurity measures is a critical investment. Wade Baker, principal author of Verizon's Data Breach Investigations Report series, cautions: "After analyzing 10 years of data, we realize most organizations cannot keep up with cybercrime—and the bad guys are winning."[4]

The types of cyberattacks—and their causes—may vary. One report identified seven top causes of major cybersecurity breaches, shown in Figure 1 on page 4.[5] A data breach analysis of more than 63,000 cybersecurity incidents across 50 companies in 2013 revealed that 94% of data breaches fell into one of nine categories, illustrated in Figure 2 on page 4.[6]

200,000 Malware Attacks



Per **year** in 2006 | Per **day** in 2013

Source: "The Top Seven Causes of Major Security Breaches," Kaseya, accessed June 24, 2014, http://www.kaseya.com/resources/white-papers/the-top-seven-causes-of-major-security-breaches.

$46 Billion

Annual global spending on cybersecurity

20% Increase

In cybersecurity breaches per year

30% Increase

In annual cost of cybersecurity breaches

Source: Stuart Corner, "Billions Spent on Cyber Security and Much of It 'Wasted,'" The Sydney Morning Herald, April 3, 2014, http://www.smh.com.au/it-pro/security-it/billions-spent-on-cyber-security-and-much-of-it-wasted-20140403-zqprb.html.

[1] University of Maryland University College, "Cybersecurity," 2014, http://www.umuc.edu/cybersecurity/about/cybersecurity-basics.cfm.
[2] U.S. Department of Homeland Security, "Cybersecurity Overview," accessed June 24, 2014, http://www.dhs.gov/cybersecurity-overview.
[3] Yoav Leitersdorf and Ofer Schreiber, "Is a Cybersecurity Bubble Brewing?" Fortune, June 17, 2014, http://fortune.com/2014/06/17/is-a-cybersecurity-bubble-brewing/.
[4] "Verizon 2014 Data Breach Investigations Report Identifies More Focused, Effective Way to Fight Cyberthreats," Verizon Corporate (press release), April 23, 2014, http://newscenter.verizon.com/corporate/news-articles/2014/04-23-data-breach-investigations-report/.
[5] "The Top Seven Causes of Major Security Breaches," Kaseya, accessed June 24, 2014, http://www.kaseya.com/resources/white-papers/the-top-seven-causes-of-major-security-breaches.
[6] Verizon, 2014 Data Breach Investigations Report, 2014, http://www.verizonenterprise.com/DBIR/2014/?gclid=CO6dqdqPk78CFdBi7AodYz8Amw.

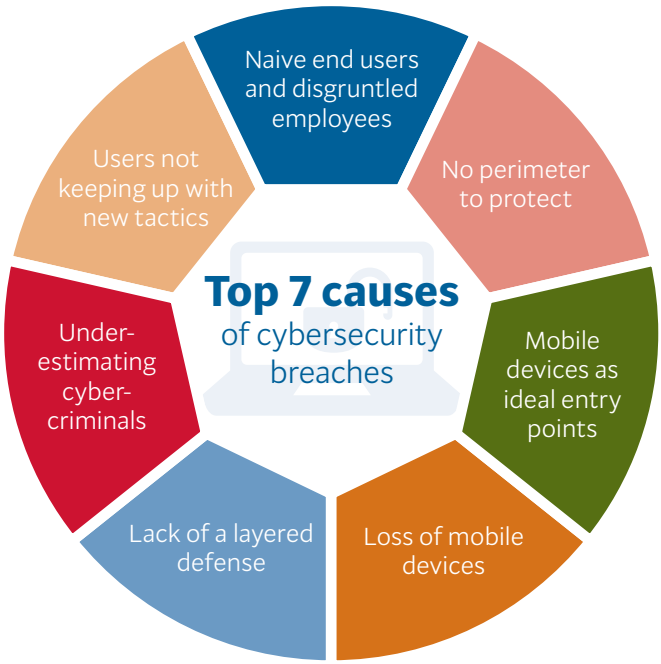
63% of U.S. Federal CIOs (Chief Information Officers) and CISOs (Chief Information Security Officers) say **improving cybersecurity is a top priority**

Proposed annual **U.S. Department of Defense** spending on cyber activities

Annual cost of computer- and network-based crimes worldwide

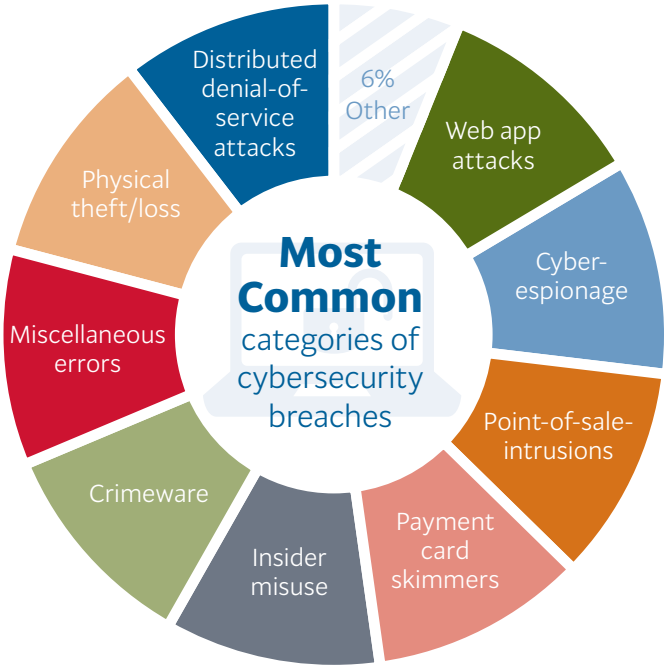
Sources: Homeland Security News Wire, "Improving Cybersecurity Top Priority: Federal CIOs, CISOs," June 12, 2014, http://www.homelandsecuritynewswire.com/dr20140612-improving-cybersecurity-top-priority-federal-cios-cisos. Andy Sullivan, "Obama Budget Makes Cybersecurity a Growing U.S. Priority," Reuters, April 10, 2013, http://www.reuters.com/article/2013/04/11/us-usa-fiscal-cybersecurity-idUSBRE93913S20130411. Tom Risen, "Study: Hackers Cost More Than $445 Billion Annually," U.S. News & World Report, June 9, 2014, http://www.usnews.com/news/articles/2014/06/09/study-hackers-cost-more-than-445-billion-annually.

Figure 1. **Most major cybersecurity breaches have one of seven causes.**



Source: Kaseya.

Figure 2. **Ninety-four percent of cybersecurity breaches in 2013 fell into these nine categories.**



Source: Verizon, based on reports from 50 companies.

Career Opportunities in the Cybersecurity Industry

With the urgent need to build a national workforce of well-qualified cybersecurity professionals, the security industry offers substantial employment opportunities. Accounting for approximately 10% of all IT occupations in the United States, cybersecurity-related positions are growing faster than all IT jobs.[7] Postings grew 74% from 2007 to 2013, with 209,749 postings in 2013.[8]

While cybersecurity job openings take 24% longer to fill than all IT openings, and 36% longer to fill than all vacancies (regardless of industry), U.S. employers pay qualified candidates a premium for cybersecurity jobs—an average of $93,028 annually, or over $15,000 more than other IT jobs overall.[9] As an example of the scarcity of qualified candidates: In 2013, U.S. employers posted 50,000 new jobs requiring a Certified Information Systems Security Professional (CISSP) credential—but there are only 60,000 total existing CISSP holders.[10]

U.S. cybersecurity jobs account for **~10%** of all IT jobs and take **24% longer** to fill than all IT jobs.

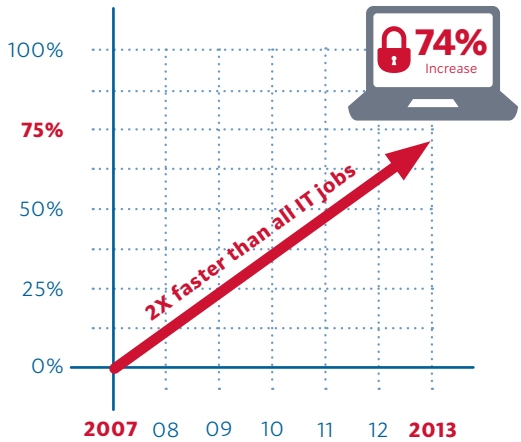
U.S. cybersecurity salaries are

$15,000

higher on average than IT jobs overall.

Source: Burning Glass.

U.S. Cybersecurity Job Postings



[7] Burning Glass Technologies, "The Growth of Cybersecurity Jobs," 2014, http://www.burning-glass.com/research/cybersecurity/.
[8] Ibid.
[9] Ibid.
[10] Ibid.

Defining a Common Set of Cybersecurity Professional Competencies

With the rising demand for qualified cybersecurity talent, industry leaders are increasingly calling for a common definition of the scope of work that cybersecurity covers—and agreed-upon competencies that cybersecurity professionals must demonstrate.[11] Defining a standard set of industry-aligned professional competencies can help in educating, recruiting, developing, and retaining the caliber of talent that the industry needs.

Striving toward common definitions and competencies, the **National Initiative for Cybersecurity Education** (NICE) developed the National Cybersecurity Workforce Framework, and the **U. S. Department of Labor** (DOL) developed the Cybersecurity Industry Competency Model.

The NICE Framework describes cybersecurity work across industries, organizations, and job types, and consists of seven categories, with 31 specialty areas.[12] For each specialty area, the Framework identifies the job tasks, knowledge, skills, and abilities that individuals must demonstrate to perform effectively. The seven categories of the NICE Framework are shown in Figure 3. The categories represent typical job duties performed by cybersecurity professionals.

Figure 3. **Categories of the National Initiative for Cybersecurity Education (NICE) National Cybersecurity Workforce Framework.**

Adapted from NICE, The National Cybersecurity Workforce Framework.

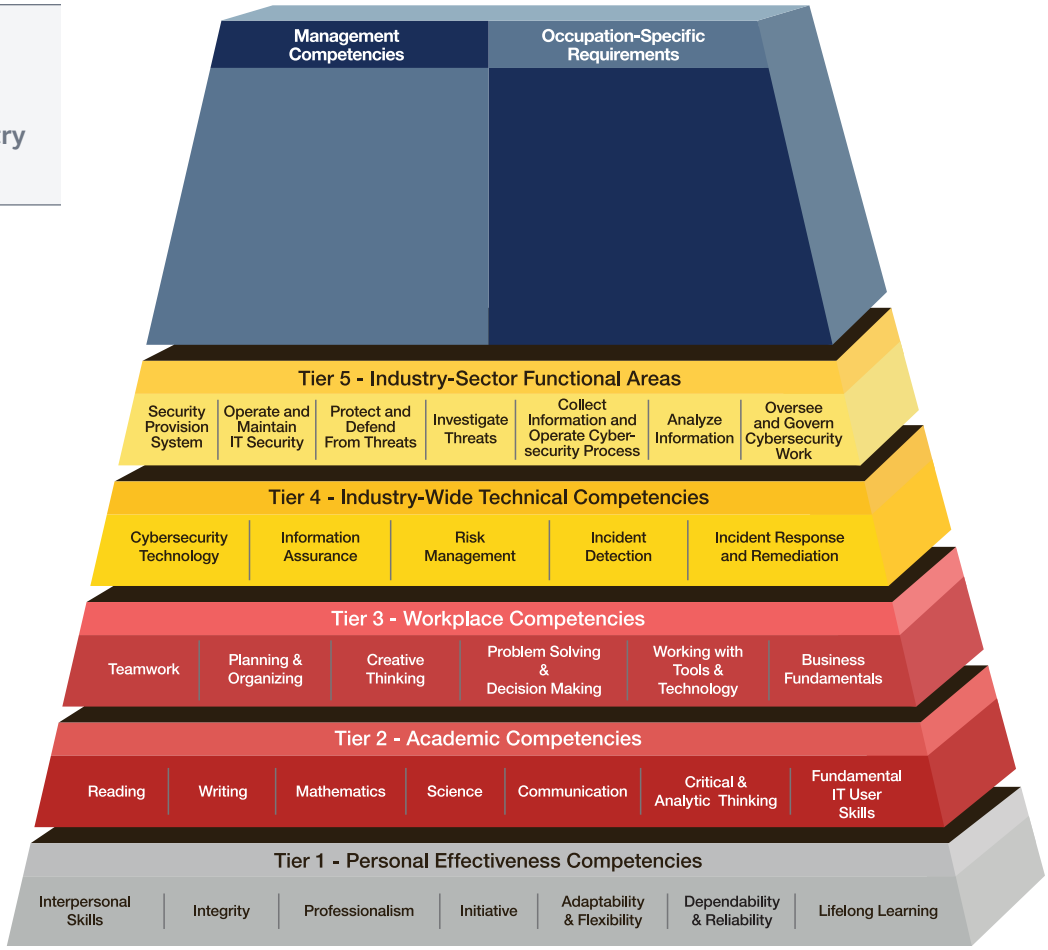
[11] A competency is defined as a group of related skills and abilities that influence a major job function, indicate successful job performance, are measurable against standards, and are subject to improvement through training and experience. See CareerOneStop, "Develop a Competency Model," 2014, http://www.careeronestop.org/COMPETENCYMODEL/userguide_competency.aspx.
[12] National Initiative for Cybersecurity Education, The National Cybersecurity Workforce Framework, last modified February 6, 2013, http://csrc.nist.gov/nice/framework/national_cybersecurity_workforce_framework_03_2013_version1_0_interactive.pdf.

Defining a Common Set of Cybersecurity Professional Competencies (cont.)

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."[13] The competency model is a tiered, "building block"-style pyramid displaying the competencies required by various levels of cybersecurity professionals—from entry-level to manager or senior leader (see Figure 4).

The model includes the soft skills (personal effectiveness, academic, and workplace skills) needed by all individuals whose work affects cybersecurity; the industry-level technical and functional competencies needed by individuals industry-wide or in particular sectors; and management competencies and occupation-specific requirements.

Figure 4.
U.S. Department of Labor's Cybersecurity Industry Competency Model.



Source: CareerOneStop.

[13] CareerOneStop, "Cybersecurity Competency Model," 2014, http://www.careeronestop.org/competencymodel/competency-models/cybersecurity.aspx.

Three Education-to-Workforce Gaps

Talent management professionals and industry stakeholders have identified three gaps in the education-to-workforce pipeline that are hindering organizations' efforts to meet current and future cybersecurity needs:

- **Competency gap:** Many cybersecurity job applicants lack the level of proficiency that organizations need their cybersecurity professionals to demonstrate.
- **Professional experience gap:** Many of these applicants also lack the level of professional experience that organizations expect from their cybersecurity professionals.
- **Education speed-to-market gap:** Higher education curriculum is not being adjusted fast enough to ensure an adequate pipeline of qualified individuals for cybersecurity roles.

Stakeholders have identified actionable recommendations for what educational institutions, industry associations, organizations, and students can do to help bridge education-to-workforce gaps.

Closing the Gaps

Recommendations to Close the Competency Gap

Stakeholders recommend that the higher education community take the following actions to improve the competency of cybersecurity job applicants.

For higher education institutions

Integrate Problem-Based Learning
Build "labs" or "case studies" into curricula so students must apply knowledge and skills, and faculty must assess not only students' technical proficiency, but also their critical thinking, problem solving, oral and written communication, and teamwork skills.

Employ Practitioner Faculty
Engage front-line cybersecurity practitioners to teach cybersecurity, serve as adjunct faculty, or partner with academic faculty for team teaching.

Ensure Alignment with Certifications
Bring certifying bodies into the classroom, as teaching hospitals do with physician instructors, to help ensure instructional quality and alignment with certification requirements.

Focus on Competency Development
Don't leave development of personal effectiveness competencies to chance. Build opportunities to develop competencies such as teamwork and integrity into curricula using case-based competitions, and use interdisciplinary teams to focus on real-world business or public-policy problems, not merely technical challenges such as malware or forensics issues.

Promote Professional Ethics
Integrate professional ethics as a vital aspect of every course in the cybersecurity curriculum. Professional ethics are of paramount importance, since cybersecurity experts often have access to an organization's (and customers') most valuable and irreplaceable data.

Emphasize Industry Experience
Promote awareness by cybersecurity students that earning a degree or certification is not sufficient to guarantee career readiness. Cybersecurity graduates must acquire informal and formal industry experience by networking, taking the initiative to learn about employers' needs, and participating in industry conferences.

Closing the Gaps (cont.)

Recommendations to Close the Professional Experience Gap

Stakeholders recommend a variety of strategies to increase the levels of professional experience across the cybersecurity talent pipeline.

For higher education institutions

Support Internships: Encourage credible, rigorous, accredited cybersecurity internships that grant college credit and offer meaningful work assignments—enabling students to demonstrate current knowledge and skills, build new skills, and showcase relevant experience on their résumé. Ensure internship guidelines clearly state requirements and expected outcomes.

Promote Workplace Presence: Encourage or expedite volunteering and job-shadowing in the cybersecurity field.

Provide Networking Opportunities: Offer an "industry day" for professional networking events: Invite employers to speak about their industry, giving students the opportunity to make company contacts, gain insights about industry trends, and learn specific tips about starting a cybersecurity career.

For students

Get Involved: Develop meaningful professional relationships, demonstrate interest in the field, and stay current on industry trends by getting involved in professional associations and networks.

Build a Portfolio: Demonstrate a specific interest or area of expertise by co-presenting at industry conferences and completing projects that build your professional "portfolio."

Seek Opportunities: Be proactive in seeking out ways to obtain relevant professional experience through internships, job shadowing, volunteering, or work-study jobs.

For industry associations

Support Student Memberships: Subsidize students' association membership fees to the extent that the students' share of costs still gives them a stake in participating.

Conduct Chapter Outreach: Connect students with local chapters for networking and educational resources.

Increase Industry Access: Provide higher education institutions and students with access to industry partners.

Share Standards: Partner with higher education institutions and provide information about industry-accepted training and certification standards such as the (ISC)² CBK® (Common Body of Knowledge), so that institutions may better align their curricula to industry needs.

For employers

Promote Partnerships: Build partnerships with higher education institutions to support industry-relevant curriculum development, internships, job-shadowing, and career networking opportunities.

Encourage Professional Experience: Develop and fund programs that provide industry experience to students. Ensure programs meet the National Security Agency's Centers of Academic Excellence accreditation requirements, and seek accreditation approval for such programs.*

Hire Interns: Treat interships as a viable step to employment, to demonstrate the value of entry-level experience as a pathway to a career.

*National Security Agency—Central Security Service. National Centers of Academic Excellence. http://www.nsa.gov/ia/academic_outreach/nat_cae/index.shtml.

Closing the Gaps (cont.)

Recommendations to Close the Education Speed-to-Market Gap

To help higher education institutions keep pace with the demand for qualified cybersecurity graduates, stakeholders recommend the following actions.

For higher education institutions

Tap Industry Resources: Map curricula to industry-endorsed competencies such as those outlined in the NICE Framework and the DOL's Cybersecurity Industry Competency Model. If needed, engage with local employers on how to integrate work skills into academic projects. (Industry associations can help facilitate connections to business.)

Advocate Certifications: Help students to identify and prepare for the relevant certification exams for their chosen career pathway.

Showcase Standards: Integrate state and international standards into curricula, and make students aware that hiring companies have their own standards.

For students

Get Certified: Identify and obtain career-relevant certifications that can supplement your associate's or bachelor's degree and help enhance your employability.

Be Clear on Clearance Requirements: Consider that many jobs in this field will require a federal security clearance, and be mindful of personal behaviors and actions that could affect your eligibility.

For employers

Engage with Educators: Participate in higher education curriculum advisory boards, offer internships, and sponsor student competitions.

Champion Cybersecurity Careers: Adopt or partner with middle schools and high schools, and participate in activities to increase awareness of cybersecurity career opportunities.

Steer Clear of Clearances: Decouple entry-level jobs from tasks that require a security clearance, as many applicants, such as non-U.S. citizens, may not be able to obtain a security clearance readily.

High-Priority Action Items

Based on the preceding recommendations, stakeholders have defined the action items that could have the most immediate impact on closing the education-to-workforce gaps:

Higher education programs should integrate problem-based learning via case studies and labs.

Just as many organizations evaluate employees on meeting goals and demonstrating the competencies used to achieve them, higher education institutions should evaluate students not only on mastering concepts and theories, but on applying their knowledge and demonstrating the practical skills needed to solve workplace problems. Simulating workplace scenarios in the classroom through case studies or labs can help students practice their skills in a controlled environment, while gaining insight into realistic workplace challenges. Practical skill-building opportunities should be designed to help students develop the competencies aligned with very specific industry-wide performance standards and evaluation criteria.

Higher education institutions should partner with employers to promote internships for cybersecurity degree completion.

Internships provide students the opportunity to gain experience, gain a real-world perspective, accumulate new skills, and establish mentor relationships. Internships also provide employers with a pool of candidates with experience in their own organization and with an opportunity to observe how these future employees can demonstrate critical competencies and apply their knowledge. Internships should be based on clearly outlined standards, agreed upon between organizations and higher education institutions, and aligned with accreditation requirements. Optionally, a central clearinghouse for cybersecurity internships should be established so that students could readily identify which employers offer relevant internships in a given geographic area.

Students should seek stakeholder guidance and take appropriate steps to position themselves for employment.

Employers seek job candidates with multifaceted, value-adding attributes, including academic credentials as well as demonstrated practical competencies, and experience to make an immediate impact when hired. Earning a degree is not enough; students need the support of employers, credentialing associations, and educational institutions to identify the academic credentials, certifications, technical knowledge, soft skills, and experiences required in the career pathways they aspire to pursue. Students must appreciate their own responsibility for lifelong learning and for taking the necessary steps toward a desired career pathway, including seizing opportunities throughout their career to gain and maintain experience in the field.

Looking Ahead

The perspectives in this report represent an important step in addressing cybersecurity education-to-workforce gaps, but there is more work to be done. (ISC)^2 continues to advance its training seminars, certifications, and continuing education in support of professionals and students in cybersecurity and related fields through formally established programs like the Global Academic Program and the (ISC)^2 Foundation. A recommendation for future research is to identify best practices for integrating cybersecurity talent development insights into non-IT security functions to improve the policy, funding, and staffing decisions of security leaders.

Acknowledgments

University of Phoenix wishes to thank the (ISC)² Foundation for co-designing the roundtable event on which this report is based, and for securing the participation of distinguished roundtable participants. Special thanks belong to the Council on CyberSecurity for generously hosting the roundtable event at its Arlington, Virginia office, and to the U.S. Department of Labor for providing an overview of the Cybersecurity Industry Competency Model as a basis for stakeholder discussion. University of Phoenix extends its appreciation to all the industry and education leaders whose contributions to the roundtable discussion formed the basis for this report.

The Industry Strategy team at Apollo Education Group provided research expertise; event design, facilitation, and project management; and publication services to furnish this report.

Executive Sponsors

Dennis F. Bonilla, Executive Dean, College of Information Systems & Technology, University of Phoenix

Jeff Greipp, J.D., Senior Director, Industry Strategy, Apollo Education Group

Dr. Rae Hayward, Senior Manager, Education Programs, (ISC)²

Julie Peeler, Director, (ISC)² Foundation

Dr. Jo Portillo, Manager, Global Academic Programs, (ISC)²

Rico J. Singleton, Director, Technology, Industry Strategy, Apollo Education Group *(Roundtable Moderator)*

Dr. Tim Welsh, Senior Vice President, Industry Strategy, Apollo Education Group

Industry and Higher Education Leaders

Michael E. Burt, MBA, MS, CISSP, Security+, Professor, Information and Engineering Technology Department, Prince George's Community College

Timothy Cupp, Network Security Engineer

Eric J. Eifert, Senior Vice President, ManTech Cyber Security Solutions

Donald J. Fergus, CISSP, CRISC, Chairman, ASIS International IT Security Council; Senior Vice President, Professional Services, Patriot Technologies Inc.

Pamela L. Frugoli, O*NET/Competency Assessment Team Lead, Employment and Training Administration, U.S. Department of Labor

Ron Hale, Ph.D., CISM, Acting CEO and Chief Knowledge Officer, ISACA

Geoff Hancock, CISSP, CISA, PMP, Chief Executive, Advanced Cybersecurity Group LLC

Ryan Merclean, Researcher, Industry Competency Model Initiative, U.S. Department of Labor

Diane Murphy, Ph.D., Professor and Chair, Information Technology and Management Science, Marymount University

Bradley Purdy, D.M., Associate Dean, College of Information Systems & Technology, University of Phoenix

Dr. Vernon Ross, Jr., Director, STEM and Generations Engagement, Lockheed Martin Corporation

Michael Sajor, Chief Information Officer, Apollo Education Group

Ronald Sanders, Ph.D., Vice President and Fellow, Booz Allen Hamilton

Maurice Uenuma, Chief Operating Officer, Council on CyberSecurity

Industry Strategy, Apollo Education Group

Brian Cox, Graphic Designer

James Fraleigh, Copyeditor

Corinne Lyon Kunzle, Information Manager, Industry Market Insights Center

Leslie A. Miller, Ph.D., PHR, Research Associate

Caroline Molina-Ray, Ph.D., Executive Director, Industry Market Insights Center

Learn More

To download this report and related talent development research, visit **industry.phoenix.edu.**


University of Phoenix®
(ISC)²
(ISC)² FOUNDATION