CSX

CYBERSECURITY NEXUS

State of Cyber Security 2017

Part 1: Current Trends in Workforce Development

Abstract

State of Cyber Security 2017 reports the results of the annual ISACA global cyber security survey, conducted in October 2016. The survey results bolster the belief that the field of cyber security remains dynamic and turbulent during its formative years. Weekly news headlines confirm that cyberattacks are not a seasonal threat or dependent on specific industry environmental attributes, but are constant and should remain forefront in every enterprise executive's thought process. To equip you with a comprehensive understanding of the cyber security industry through the lens of those who define it—the managers and practitioners—ISACA is presenting the survey results in a series of reports that focus on individual topics. This report is the first in the *ISACA State of Cyber Security 2017* white paper series and presents timely information about cyber security workforce development and its current trends.

ISACA®

Trust in, and value from, information systems

Table of Contents

State of Cyber Security Study

State of Cyber Security 2017 reports the results of the annual ISACA global cyber security survey, conducted in October 2016. The survey results bolster the belief that the field of cyber security remains dynamic and turbulent during its formative years. Weekly news headlines confirm that cyberattacks are not a seasonal threat or dependent on specific industry environmental attributes, but are constant and should remain forefront in every enterprise executive thought process. To equip you with a comprehensive understanding of the cyber security industry through the lens of those who define it—the managers and practitioners—ISACA is presenting the survey results in a series of reports that focus on individual topics. This report is the first in the *ISACA State of Cyber Security 2017* white paper series and presents timely information about cyber security workforce development and its current trends.

Survey Methodology

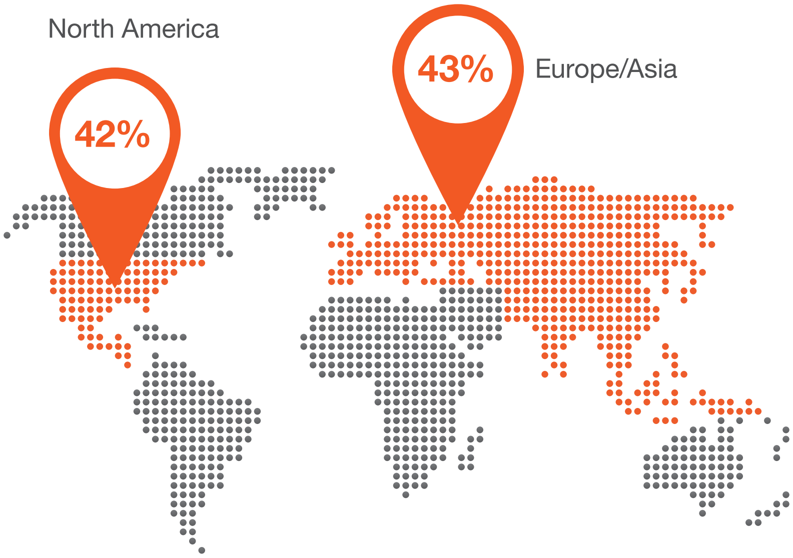
An invitation to participate in the survey was emailed to a global population of cyber security professionals who hold ISACA's Certified Information Security Manager® (CISM®) and/or Cybersecurity Nexus Practitioner™ (CSX Practitioner™) designations, and individuals in information security positions. The survey data was collected anonymously through SurveyMonkey®. The results reveal positive and negative findings about the current state of cyber security. The survey, which uses multiple-choice and Likert-scale formats, is organized into four major sections:

- Budgets, Hiring and Skills
- Threats
- Internet Crime and Fraud
- Organizational Security and Governance

The ISACA survey targets managers and practitioners who have cyber security job responsibilities. Although 950 individuals participated in the survey, only those respondents whose primary job function is cyber security or information security (633 participants) are included in the survey results.

A typical respondent can be described as:

100%
A member
of ISACA



28%

Working in technology
services/consulting

23%
Financial
Services

74%
Cyber Security/
Information Security
Manager

11%
Government/Military
National/State/Local

26%
Cyber Security/
Information Security
Practitioners

49%
Employed in an
enterprise with at least
1,500 employees

While the norms of the sample population are interesting to consider, it is important to note some characteristics that reflect the population's diversity. Among those surveyed, respondents hailed from more than 20 industries (**figure 1**) and all five major global regions (**figure 2**).

FIGURE 1—INDUSTRY SECTORS

In which of the following industries are you employed?

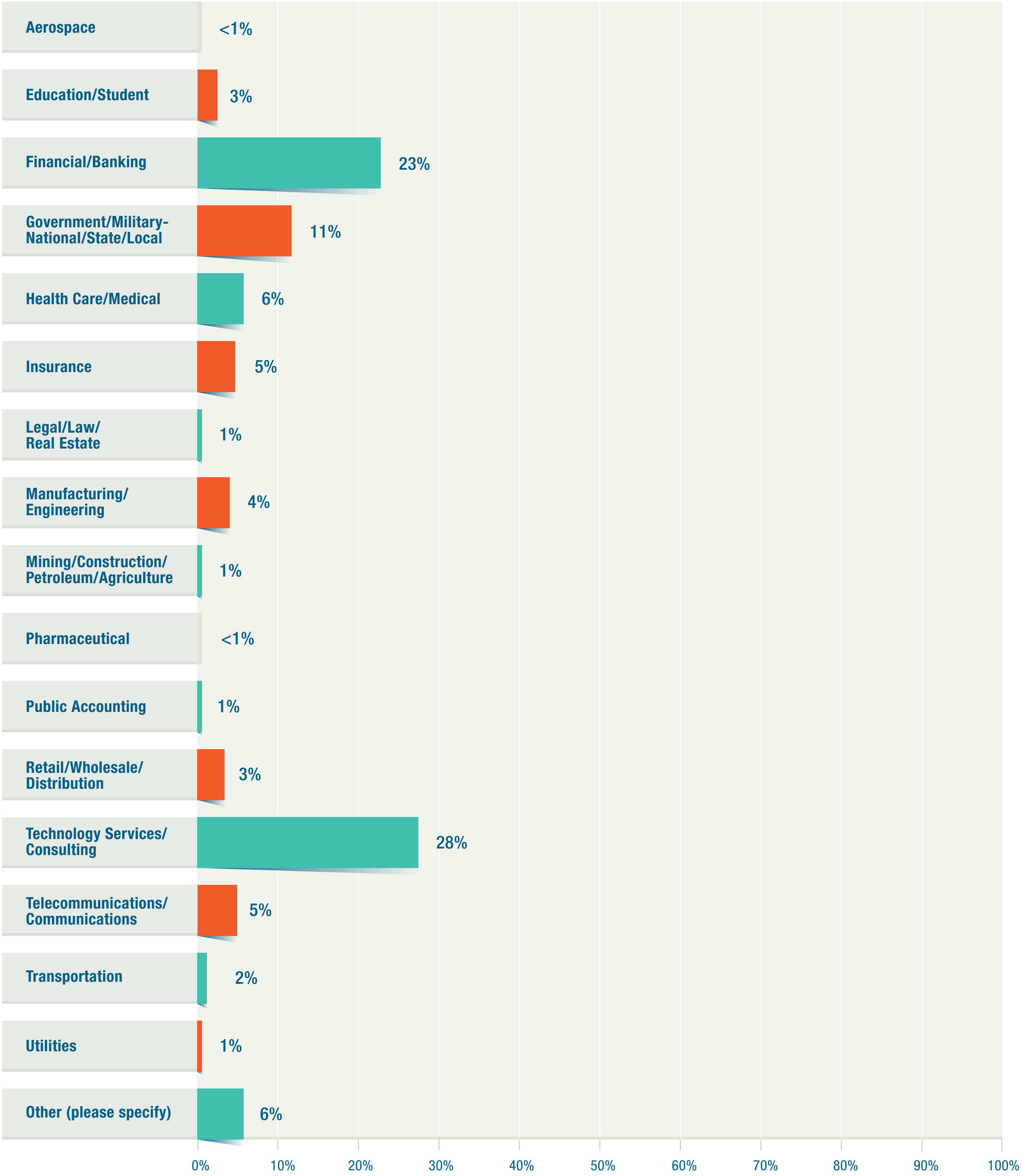
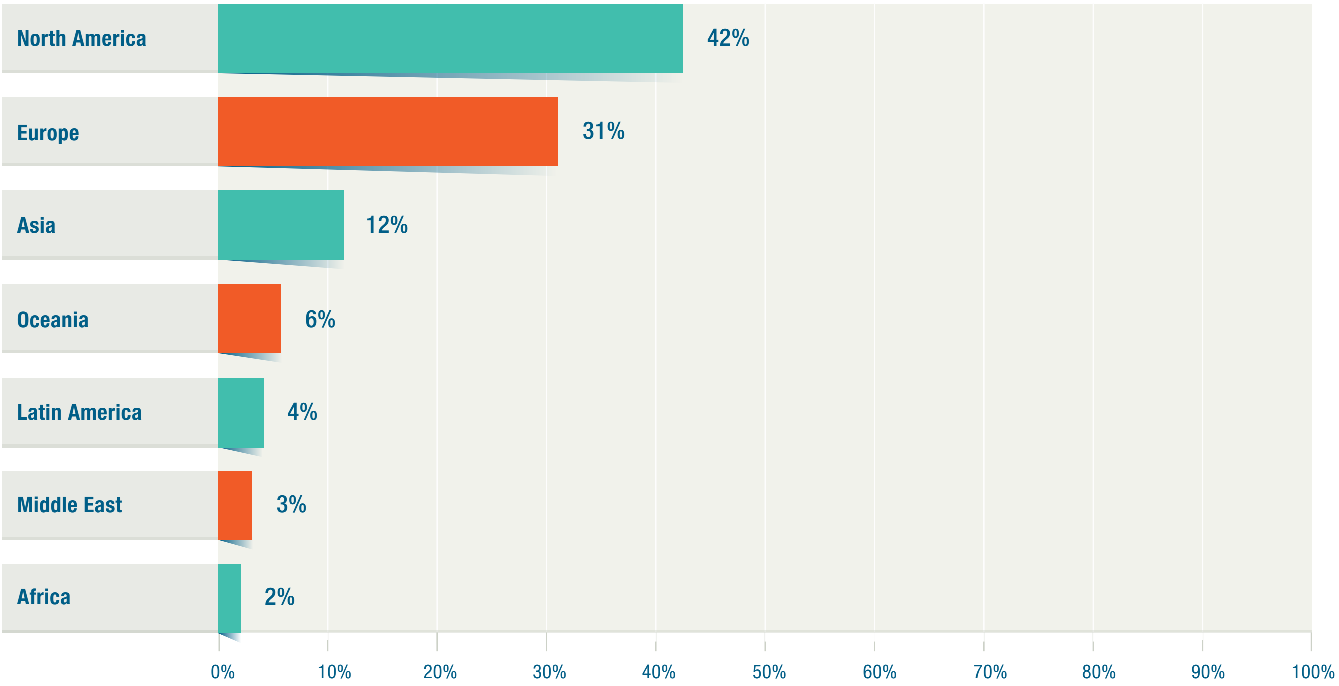


FIGURE 2—REGIONS

In which reigon do you reside?



Cyber Security Employment: A Growing Need Meets a Stubborn Shortage

Applicable cyber security talent is becoming increasingly difficult to find in today's ever growing cyber security field. Recent reporting from the Center for Strategic and International Studies states that the "shortage in cyber security skills does direct and measurable damage"[1] to enterprises operating in today's interconnected world. Furthermore, "[h]igh-value skills are in critically short supply,"[2] creating an employment environment in which enterprises experience difficulty filling positions. Impacting these issues is the reality that security fatigue, "weariness or reluctance to deal with computer security,"[3] as defined by the National Institute of Standards and Technology (NIST), is taking hold of many individuals in the workplace. Therefore, it is not surprising that survey respondents say that enterprises are struggling when trying to fill important cyber security positions.

[1] Intel Corporation, "Hacking the Skills Shortage: a study of the international shortage in cybersecurity skills," 2016, *www.mcafee.com/us/resources/reports/rp-hacking-skills-shortage.pdf*

[2] *Ibid*.

[3] National Institute of Standards and Technology (NIST), "'Security Fatigue' Can Cause Computer Users to Feel Hopeless and Act Recklessly, New Study Suggests," 4 October 2016, *www.nist.gov/news-events/news/2016/10/security-fatigue-can-cause-computer-users-feel-hopeless-and-act-recklessly*

Key Findings

The main problem of obtaining key talent in the realm of cyber security stems from a lack of qualified applicants. This report identifies that the key factors that enterprises consider when hiring individuals for cyber security positions are practical skill competency and certification attainment. Therefore, an appropriate hiring strategy that emphasizes performance-based certifications that require practical applicant cyber security skills is key to successfully filling open positions. Following are the key workforce development findings from the study:

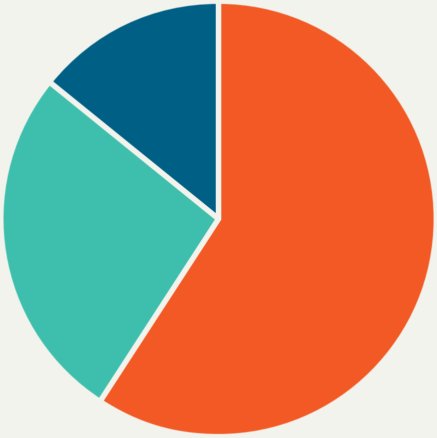
- Over a quarter of enterprises report that the time to fill cyber security and information security positions is one-half year.
- On average, 59 percent of enterprises get at least five applicants for each open cyber security position, but most of these applicants are unqualified.
- Practical hands-on experience is the most important cyber security candidate qualification to 55 percent of enterprises.
- Enterprises consider personal endorsements and formal education to be the least important cyber security candidate qualifications.
- Close to 70 percent of hiring enterprises require a security certification for open cyber security positions.

Filling Positions

One of the most important elements of hiring personnel is the rate at which enterprises can fill open positions. Ideally, hiring personnel desire to fill open positions with the most qualified individuals as quickly as possible. However, in the cyber security field, this goal proves difficult. Filling open cyber security/information security positions is difficult for over a quarter of the survey respondent enterprises. Almost 27 percent of respondents state that they are unable to fill open cyber security positions in their enterprises—with another 14 percent of respondents unaware as to whether their enterprises could fill these positions or not (**figure 3**). This leaves a quarter of cyber security positions unfilled.

FIGURE 3—ABILITY TO FILL OPEN CYBER SECURITY/INFORMATION SECURITY POSITIONS

Are you able to fill your open cyber security/information security positions?



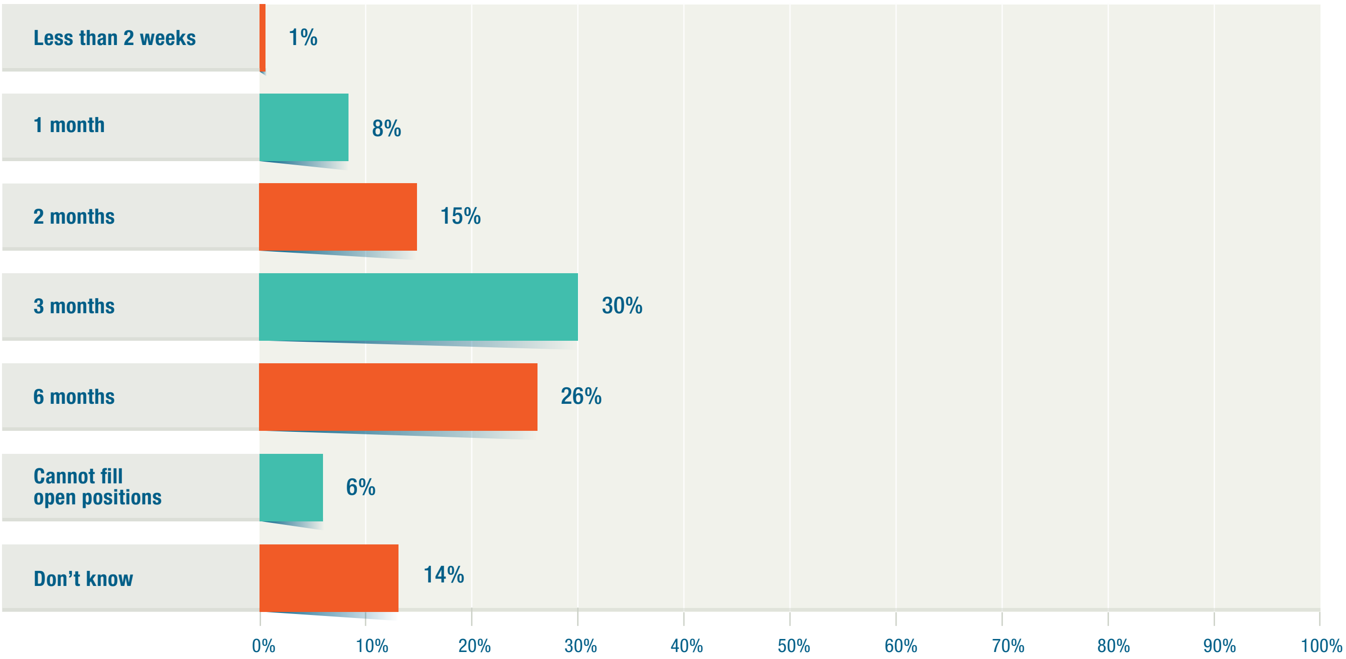
Answer Choices	Responses
Yes	**59%** 375
No	**27%** 170
Don't know	**14%** 88

These statistics change based upon the geographic location of the surveyed individuals. Although North American respondents state that they are unable to fill open positions around 26 percent of the time, respondents in Asia have an easier time finding new hires, with only 22 percent of these respondents indicating that they are unable to fill open positions. Meanwhile, almost one-third of European cyber security job openings remain unfillable, with 30 percent of cyber security job openings remaining open and unfilled.

The thought of one-quarter of cyber security positions remaining unfilled seems disheartening and, on closer evaluation of the data, the outlook does not improve. Although, when asked how long it takes for an enterprise to fill a cyber security/information security position, only six percent of respondents indicate that they cannot fill open positions, and most of the remaining respondents note that long-term vacancies are the norm. Coming with the cost of enterprise detriment, 55 percent of respondents indicate that open positions take at least three months to fill—with over one-quarter of respondents stating that finding an appropriate hire can take up to six months. See **figure 4**.

FIGURE 4—TIME TO FILL AN OPEN CYBER SECURITY/INFORMATION SECURITY POSITION

On average, how long does it take you to fill a cyber security/information security position?



Finding Applicants and Determining Qualification

Other elements of creating a capable workforce that cyber security organizations consider are the number of qualified individuals who apply to open positions and the aspects that designate applicants as qualified. When asked how many individuals apply to an enterprise's open security position, 59 percent of respondents note that at least five individuals apply to each open position (**figure 5**). In fact, when solely considering North American respondents, 16 percent indicate that, for each job opening, their enterprise has at least 20 applicants.

Although the number of applicants for an open position appears quantitatively impressive, understanding the perceived quality of applicants contextualizes the data—potentially explaining the difficulty in hiring cyber security practitioners. Sixty-four percent of respondents say that half, or less, of their applicants are qualified for an open security position, with over 35 percent of these respondents indicating that less than 25 percent of applicants are qualified (**figure 6**). By viewing this statistic geographically, the value remains barely changed, indicating that, in North America, Europe, and Asia, most applicants to cyber security jobs are viewed as unqualified.

Understanding the metrics of what respondents feel determines a "qualified" applicant provides some contextualization to the difficulty of finding appropriate hires. When asked to identify the most important attributes of a qualified applicant, most respondents indicate that practical verification (hands-on experience) is most important, with references and personal endorsements being the least important attributes (**figure 7**). Formal education is also viewed as unimportant, barely scoring higher than personal endorsements and recommendations.

Identifying the attributes of an unqualified applicant reinforces the group definition of a qualified candidate. When respondents are asked to identify the attributes that designate an applicant as unqualified, survey respondents specify that a lack of practical verification (hands-on) is the most cited reason (**figure 8**). When asked to identify the biggest skills gap that exists in today's security professionals, over 25 percent of respondents identify technical skills. This lack of technical skills is the second leading statistic, which is only behind the leading skills gap of the applicant's inability to understand the business of cyber security, which 45 percent of respondents identify.

The lack of a practical experience and hands-on capability in the field of cyber security presents a quagmire for most hiring managers in an enterprise. Although some people within the industry may view cyber security as a longstanding, entrenched career field, others view the field as relatively young. Supporting the argument that the field is relatively young are factors such as the 2009 establishment of the United States Cyber Command and the 2014 publication of the *National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)*. Thus, longstanding experience within the field of cyber security is in short supply.

FIGURE 5—NUMBER OF APPLICANTS FOR OPEN SECURITY POSITIONS

On average, how many applicants do you get for open security positions?

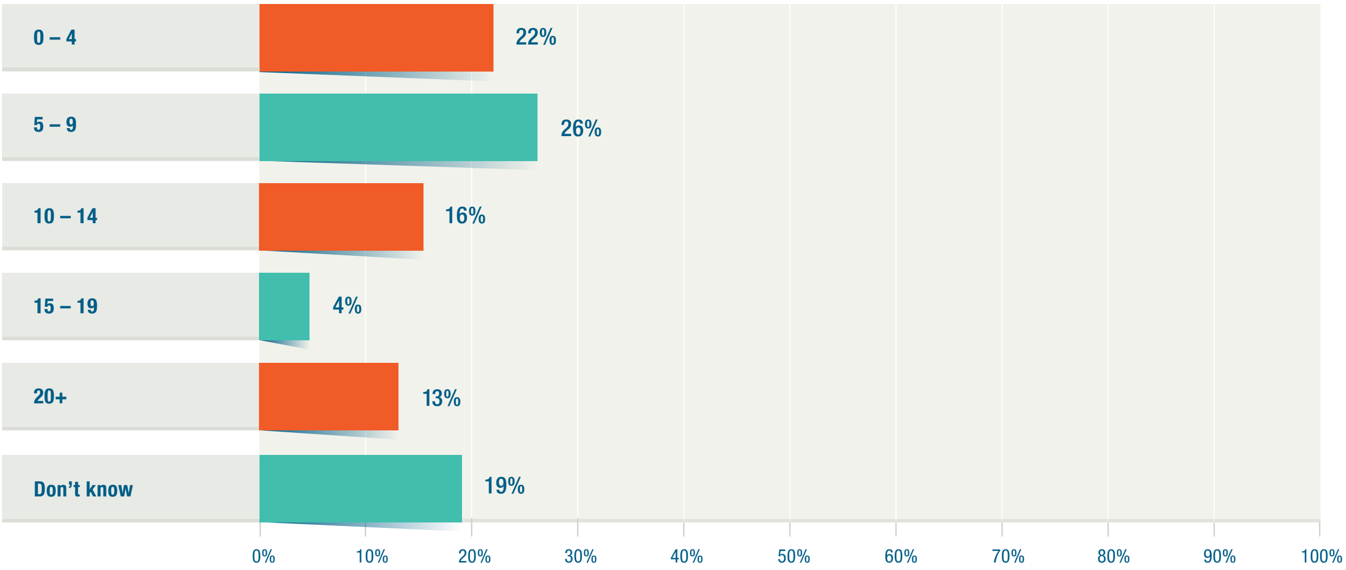


FIGURE 6—QUALIFIED SECURITY POSITION APPLICANTS

On average, how many of those security applicants are qualified?

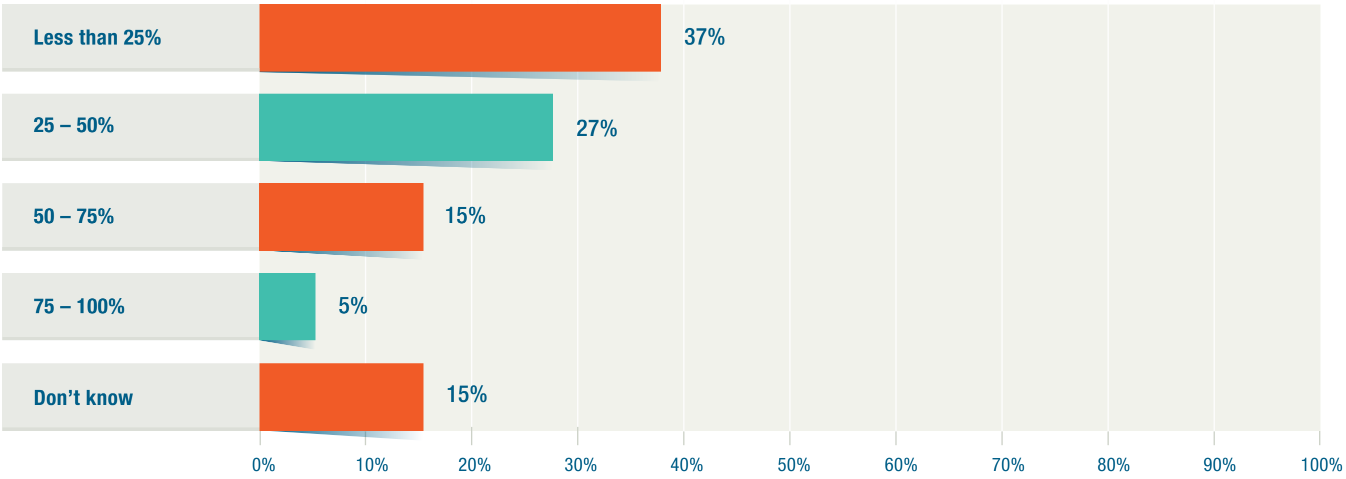


FIGURE 7—MOST IMPORTANT ATTRIBUTES OF A QUALIFIED APPLICANT

Which of the following applicant attributes are most important to the enterprise when designating a qualified applicant? Rank 1 as the most important reason and 5 the least important reason.

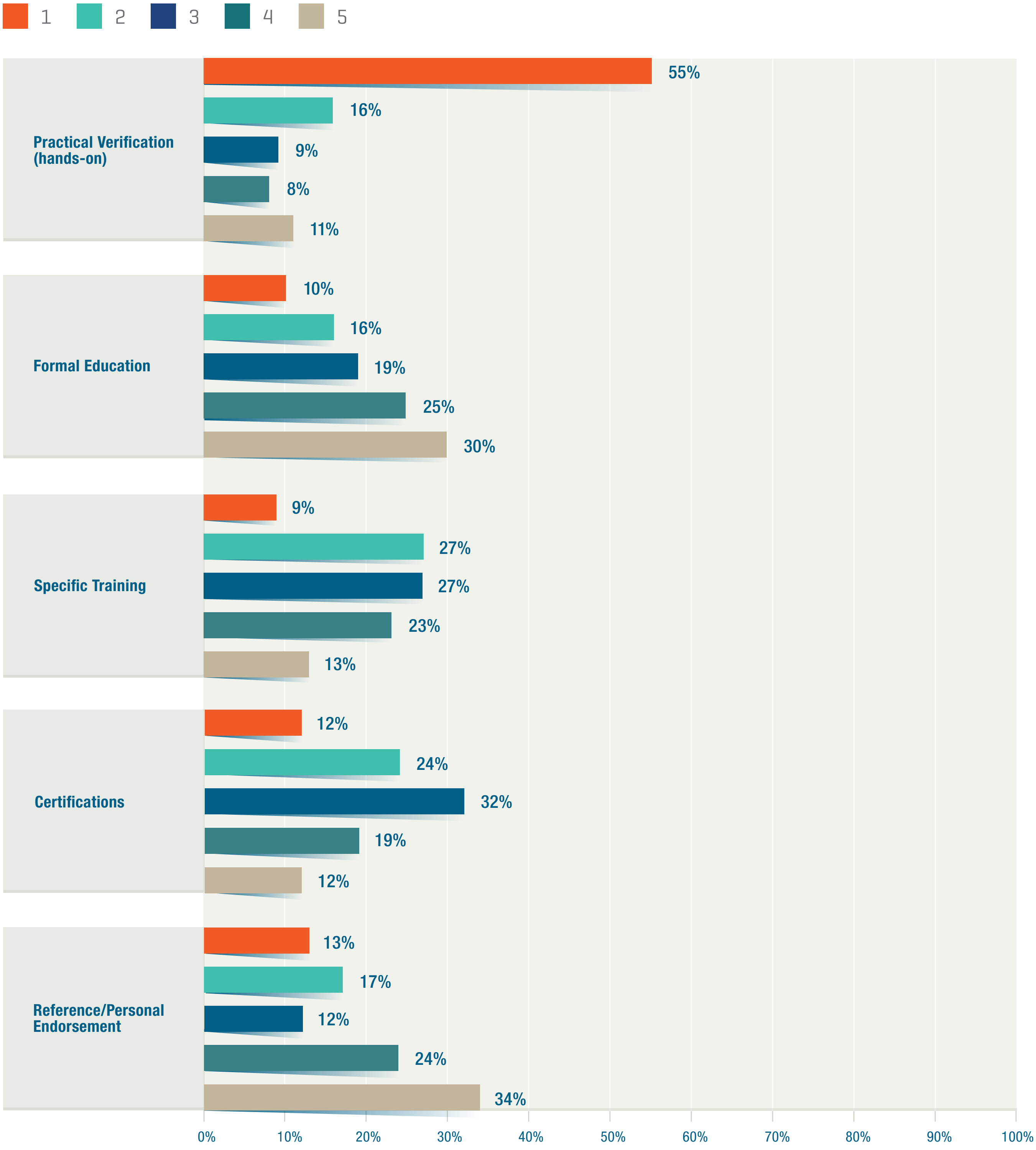
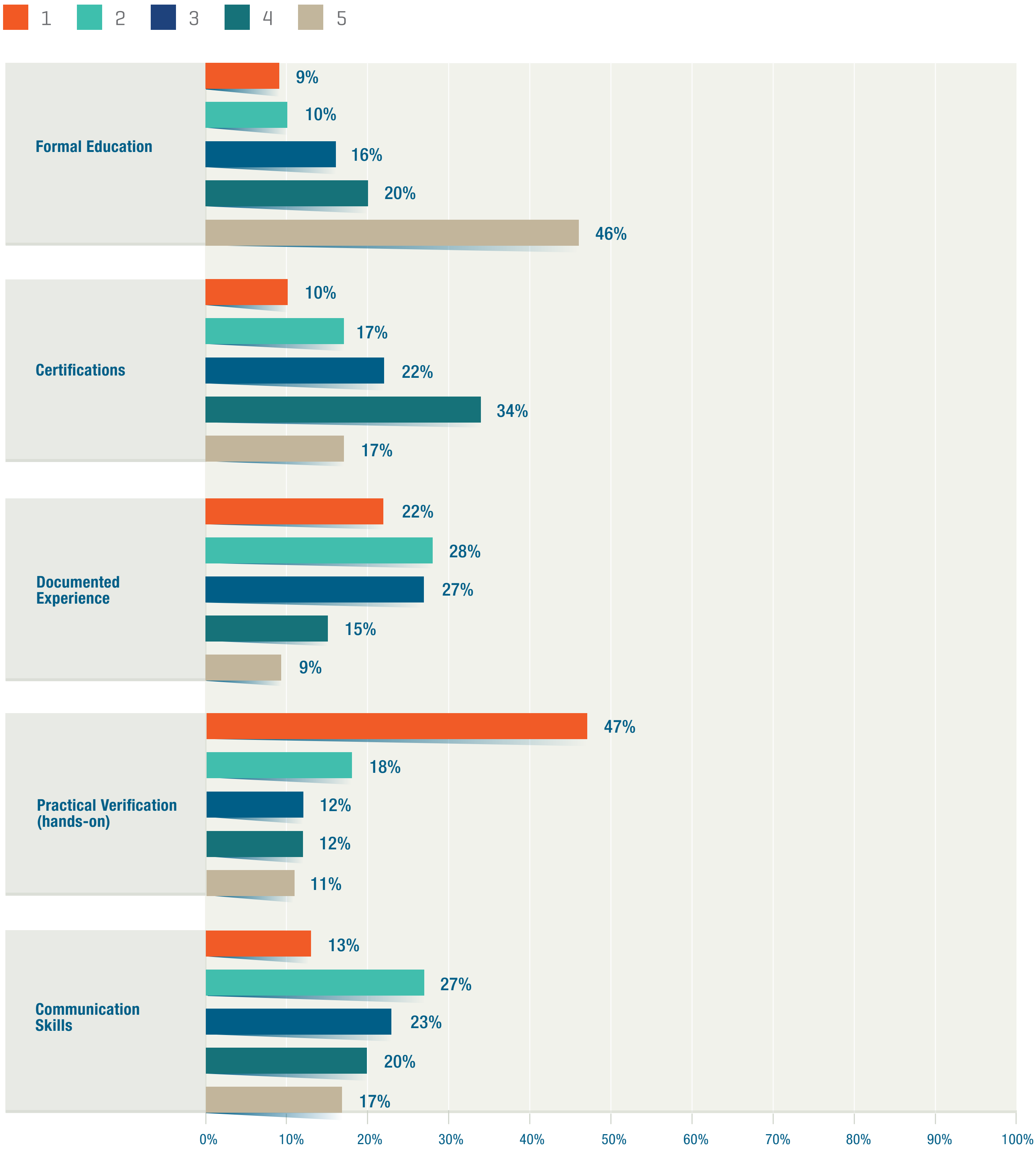


FIGURE 8—REASONS FOR DESIGNATING AN APPLICANT AS UNQUALIFIED

When designating an applicant as unqualified, which applicant attributes are most often cited as the reason why? Rank 1 the most often cited reason and 5 the least cited reason.

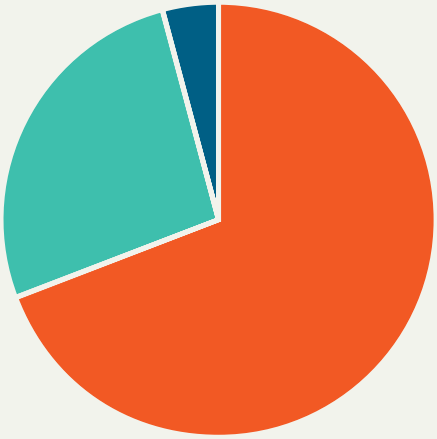


Filling the experience and skills gap within the cyber security industry proves difficult and has resulted in most job postings requiring a certification within the field. Sixty-nine percent of respondents indicate that their enterprises typically require a security certification for open positions (**figure 9**). Furthermore, most respondents view professional certifications as either equivalent to, or more important than, formal education. In each geographical region, more respondents view certifications as more important than formal education, and in no geographical location is that statistic overcome by the view that certifications and formal education are equally important.

Understanding which certifications are required for job openings also helps individuals who are evaluating the state of cyber security. Survey respondents indicate that the Certified Information Systems Security Professional (CISSP) certification is the most-relevant certification to their cyber security job openings, with 27 percent of respondents specifying that they require the applicants have the certification to be on a security team. Conversely, the Offensive Security Certified Professional (OSCP) certification is the least relevant certification to respondent enterprise security team needs. However, it should be noted that 26 percent of respondents are unfamiliar with the OSCP certification and, when also considering the Cybersecurity Nexus Practitioner (CSXP) certification, the two make up the majority of certifications with which the respondents are unfamiliar.

FIGURE 9—REQUIRED SECURITY CERTIFICATIONS

When looking for candidates to fill open security positions, do you typically require a security certification?



Answer Choices	Responses
Yes	**69%** 439
No	**27%** 169
Don’t know	**4%** 25

Conclusion

The adage “good help is hard to find” proves its universality when considering the field of cyber security. Based on the respondent data from the ISACA State of Cyber Security survey, one can assume that it is very difficult to find qualified applicants for open cyber security positions. Furthermore, the desire to hire experienced individuals who understand the business of cyber security and are technically proficient creates a perfect storm of frustration for hiring managers who are trying to fill openings in an arguably young industry.

The ISACA State of Cyber Security survey results identify the key applicant attributes that influence cyber security manager hiring decisions, which are helpful to hiring managers and practitioners who are seeking cyber security positions. The ISACA study identifies that practical skill competency and certification attainment are the key attributes that hiring managers consider when making cyber security position hiring decisions. Therefore, an appropriate hiring strategy that emphasizes performance-based certifications that require practical applicant cyber security skills is key to successfully filling open positions. Certifications, which can be garnered in less time than a formal degree, have become a prevailing consideration when filling an open cyber security position. ISACA’s CSXP certification aims to tackle this discrepancy as the preeminent, award-winning, performance-based cyber security certification program. However, to do that it will need to overcome the currently domineering CISSP.

Trust in, and value from, information systems

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA

Phone: +1.847.253.1545

Fax: +1.847.253.1443

Email: info@isaca.org

Web site: www.isaca.org

Provide feedback:
www.isaca.org/state-of-cyber-security-2017

Participate in the ISACA Knowledge Center:
www.isaca.org/knowledge-center

Follow ISACA on Twitter:
https://twitter.com/ISACANews

Join ISACA on LinkedIn:
http://linkd.in/ISACAOfficial

Like ISACA on Facebook:
www.facebook.com/ISACAHQ

ISACA®

ISACA (*isaca.org*) helps global professionals lead, adapt and assure trust in an evolving digital world by offering innovative and world-class knowledge, standards, networking, credentialing and career development. Established in 1969, ISACA is a global nonprofit association of 140,000 professionals in 180 countries. ISACA also offers the Cybersecurity Nexus™ (CSX), a holistic cyber security resource, and COBIT®, a business framework to govern enterprise technology.

Disclaimer

This is an educational resource and is not inclusive of all information that may be needed to assure a successful outcome. Readers should apply their own professional judgment to their specific circumstances. ISACA nor this publication is associated with or sponsored by Amazon Technologies, Inc.

Reservation of Rights

ACKNOWLEDGMENTS

ISACA would like to recognize:

Lead Developer

T. Frank Downs
CEH, ECSA, LPT, CEI, ISACA, USA

Expert Reviewers

Josh Angichiodo
Lieutenant Commander, US Navy

Michael Marano
CEH, CWTS, CWNA, CWNP, CEI, OSWP, INNOPLEX, LLC, USA

ISACA Board of Directors

Christos K. Dimitriadis
Ph.D., CISA, CISM, CRISC, INTRALOT S.A., Greece, International Chair

Theresa Grafenstine
CISA, CGEIT, CRISC, CIA, CGAP, CGMA, CPA, US House of Representatives, USA, Vice-chair

Robert Clyde
CISM, Clyde Consulting LLC, USA, Director

Leonard Ong
CISA, CISM, CGEIT, CRISC, CPP, CFE, PMP, CIPM, CIPT, CISSP ISSMP-ISSAP, CSSLP, CITBCM, GCIA, GCIH, GSNA, GCFA, Merck, Singapore, Director

Andre Pitkowski
CGEIT, CRISC, OCTAVE, CRMA, ISO27kLA, ISO31kLA, APIT Consultoria de Informatica Ltd., Brazil, Director

Eddie Schwartz
CISA, CISM, CISSP-ISSEP, PMP, USA, Director

Jo Stewart-Rattray
CISA, CISM, CGEIT, CRISC, FACS CP, BRM Holdich, Australia, Director

Tichaona Zororo
CISA, CISM, CGEIT, CRISC, CIA, CRMA, EGIT | Enterprise Governance (Pty) Ltd., South Africa, Director

Zubin Chagpar
CISA, CISM, PMP, Amazon Web Services, UK, Director

Rajaramiyer Venketaramani Raghu
CISA, CRISC, Versatilist Consulting India Pvt. Ltd., India, Director

Jeff Spivey
CRISC, CPP, Security Risk Management Inc., USA, Director

Robert E Stroud
CGEIT, CRISC, Forrester Research, USA, Past Chair

Tony Hayes
CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, Queensland Government, Australia, Past Chair

Greg Grocholski
CISA, SABIC, Saudi Arabia, Past Chair

Matt Loeb
CGEIT, FASAE, CAE, ISACA, USA, Director

Cybersecurity Working Group

Eddie Schwartz
CISA, CISM, CISSP-ISSEP, PMP, USA, Chair

Niall Casey
Johnson & Johnson, USA

Stacey Halota
CISA, CISSP, CIPP, Graham Holdings, USA

Tammy Moskites
CISM, Venafi, USA

Lisa O’Connor
Accenture, USA

Ron Ritchey
JPMorgan Chase & Co., USA

Marcus Sachs
North American Electric Reliability Corporation, USA

Greg Witte
CISM, CISSP-ISSEP, PMP, G2 Inc., USA

Rogerio Winter
Brazilian Army, Brazil