CSX™
CYBERSECURITY NEXUS

State of Cybersecurity 2019

Part 1: Current Trends in Workforce Development

Abstract

State of Cybersecurity 2019 reports the results of the annual ISACA global *State of Cybersecurity Survey*, conducted in November 2018. While some findings pointed to unforeseen trends, many survey results reinforce previous years' findings—specifically that the need for trained and experienced cybersecurity professionals vastly outweighs the supply. *State of Cybersecurity 2019* provides a distinctive view of cybersecurity from the perspective of those who define the field—cybersecurity managers and practitioners. This is the first report based on the survey, which focuses on the current trends in cybersecurity workforce development, staffing, budget and gender diversity.

HCL

ISACA®

CONTENTS

Executive Summary

This year's global *State of Cybersecurity Survey* identifies several challenges in the maturing cybersecurity field. This white paper analyzes the survey findings regarding cybersecurity workforce development, staffing, retention, budget implications and gender diversity. In a second white paper, ISACA examines the survey results relating to cyberattacks, cybersecurity awareness training programs, and organizational cybersecurity and governance.

Key Findings

Because enterprises continue to struggle with cybersecurity staffing, it is important to analyze in detail the factors contributing to the skills gap. This year, ISACA research identifies missing talent and expertise and pinpoints potential contributing factors.

The truism "good help is hard to find" is exemplified in the cybersecurity field. This fact continues to be reinforced by ISACA's research and other third-party research and analysis.

The following are key findings relating to the cybersecurity workforce:

- **Technically proficient cybersecurity professionals continue to be in short supply and difficult to find.** This fact is compounded when coupled with the realization that the greatest skill needed in the field is business acumen. Currently, the most-prized hire in a cybersecurity team is a technically proficient individual who also understands business operations and how cybersecurity fits into the greater needs of the enterprise.
- **Retaining cybersecurity professionals is exceptionally difficult, and the current enticement of employer-paid training and certification are not ensuring retention.** Cybersecurity personnel are leaving most often for greater pay, career advancement and perceived healthier work environments.
- **Gender diversity programs may be declining, and their effectivity is directionally lower.** Less than half of the survey-respondent enterprises have a gender diversity program. The perception of their effectiveness, when compared to previous years, is trending downwards.
- **Cybersecurity budget increases are expected to slow slightly.** Most survey respondents continue to expect cybersecurity budgets to increase, but not as much as in the previous year.

The struggle to fill open cybersecurity positions, especially technical roles, remains great. Additionally, retention of qualified individuals is proving to be difficult, with traditional retention tactics seemingly less effective.

"While the number of high-profile cyberattacks are on the ascent on one side, so are the number of cybersecurity vacancies going unfilled. The creation of industry and academic programs to introduce the latest industry, technology, process and effective use of automation to address the shortage of skilled resources will have to be taken on war-footing."

RENJU VARGHESE, FELLOW & CHIEF ARCHITECT, CYBERSECURITY & GRC, HCL TECHNOLOGIES

Survey Methodology

In the final quarter of 2018, ISACA sent survey invitations to a global population of cybersecurity 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 were collected anonymously via SurveyMonkey. A total of 1,576 respondents completed the survey and their responses are included in the results.[1]

The survey, which used multiple-choice and Likert scale formats, was organized into six major sections:

- Hiring and Skills
- Diversity in Cybersecurity
- Cybersecurity Budgets
- Cyberattacks and Threats
- Cyberawareness Training Programs
- Organizational Cybersecurity and Governance

Due to the nature of the survey, the targeted population consists of individuals who have cybersecurity job responsibilities. Of the 1,576 respondents, 1,020 indicate that their primary professional area of responsibility is cybersecurity. **Figure 1** shows additional survey-respondent demographic norms.

It is important to note some characteristics that reflect the survey population's diversity. Among those surveyed, respondents hailed from over 17 industries (**figure 2**).

Technically Proficient Cybersecurity Professionals Continue to Be in Short Supply

Filling Positions

In a constantly changing, ever connected threat landscape, staffing cybersecurity positions appropriately and efficiently becomes one of the most important objectives to any enterprise. Ensuring that business operations remain secure, functional and predictable is a hallmark of an appropriately staffed and trained cybersecurity organization. Like previous years, however, a large hiring gap remains in the cybersecurity field. Specifically, 58 percent of survey respondents report that their enterprises have unfilled cybersecurity positions (**figure 3**). This reflects a one percentage point decrease from last year's survey findings[2] (59 percent), indicating that, although the need may have decreased, the actual change is minuscule.

Furthermore, it is taking longer, on average, for enterprises to find and hire qualified cybersecurity professionals. Enterprises that are languishing at least six months before they are able to fill open cybersecurity positions increased six percentage points, from 26 percent last year[3] to 32 percent this year (**figure 4**). Compounding the issue, 30 percent of this year's survey

1 Certain questions included the option to choose "Don't know" from the list of answers. Where appropriate, "Don't know" responses were removed from the calculation of findings. Result percentages are rounded to the nearest integer.
2 ISACA, *State of Cybersecurity 2018, Part 1: Workforce Development*, April 2018, https://cybersecurity.isaca.org/state-of-cybersecurity#0-part-1-april
3 *Ibid.*

FIGURE 1—RESPONDENT DEMOGRAPHICS

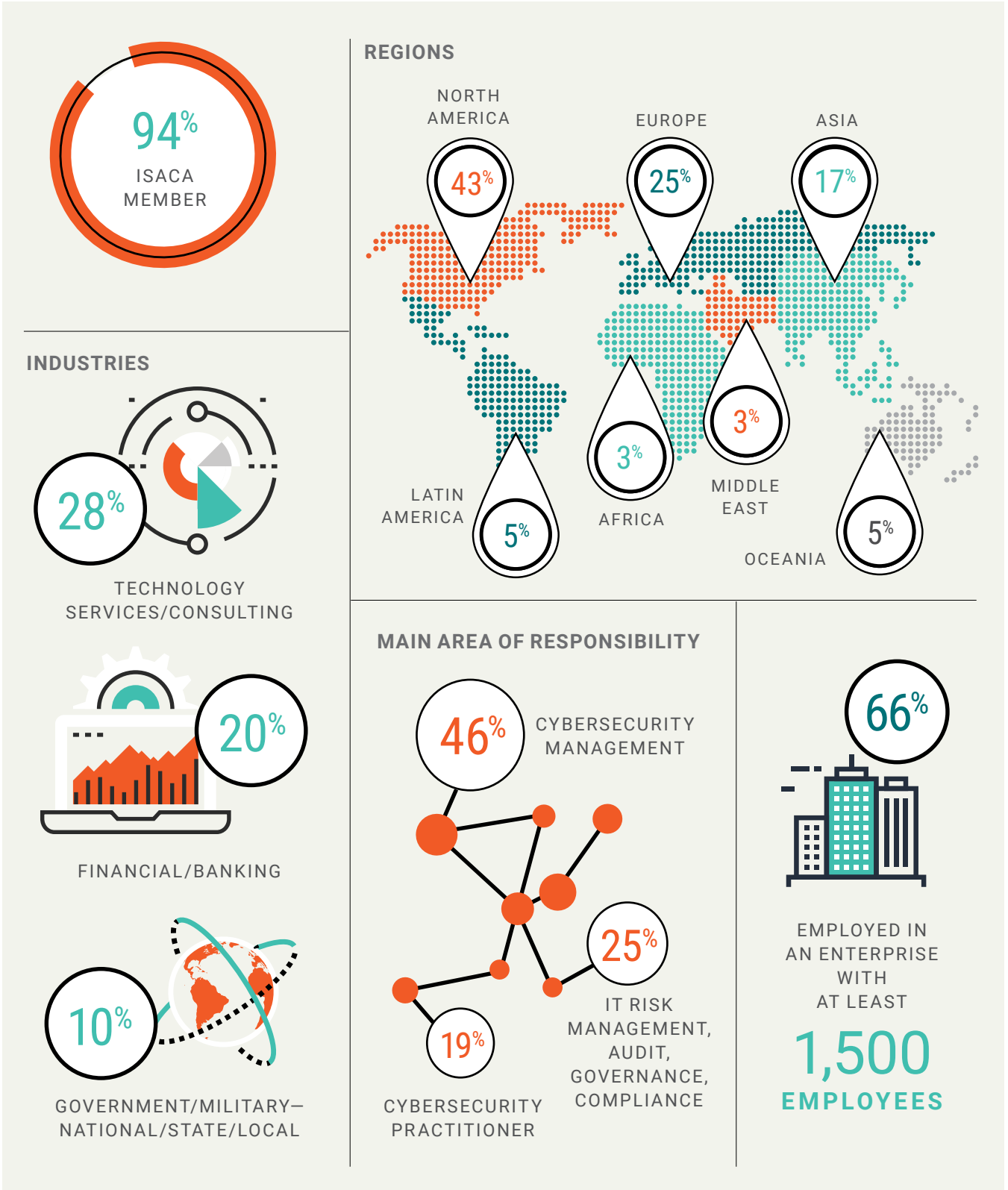
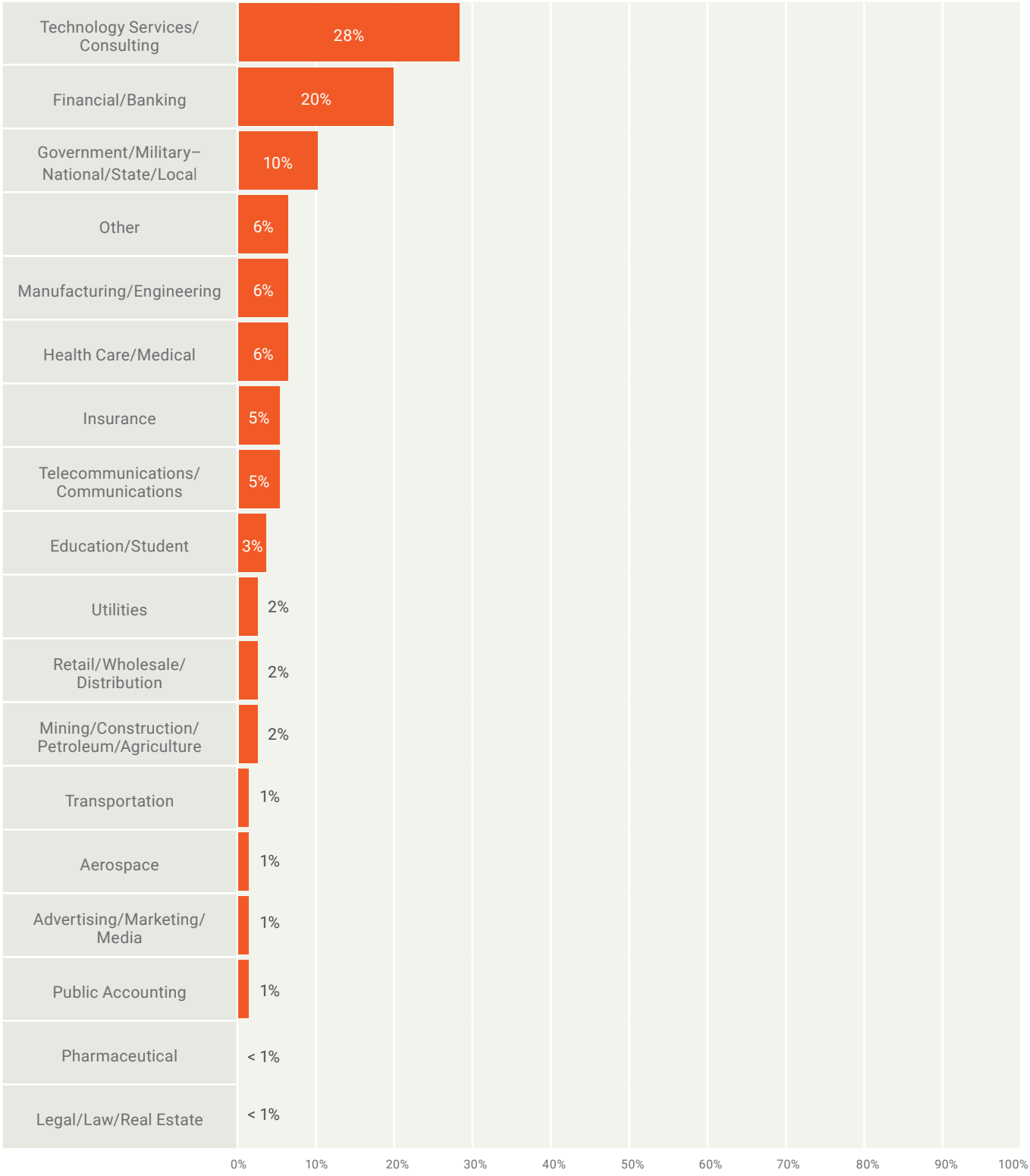


FIGURE 2—INDUSTRY SECTORS

In which industry are you employed?



respondents indicate that cybersecurity positions remain open at least three months before they are filled—representing a five percentage point increase from last year (**figure 4**). Analyzing this data holistically, over 60 percent of respondent organizations experience at least three months of unfilled cybersecurity positions when hiring new staff.

Unqualified and Insufficient Technical Applicants

One of the causes of cybersecurity roles remaining unfilled for many months is the lack of qualified professionals applying to open positions. Specifically, when asked, almost 60 percent of survey respondents indicate that only 50 percent or less of the applicants applying to open cybersecurity positions are qualified (**figure 5**). Compounding this discovery, 29 percent of

FIGURE 3—ORGANIZATIONS REPORTING UNFILLED CYBERSECURITY POSITIONS

Does your organization have unfilled (open) cybersecurity positions?

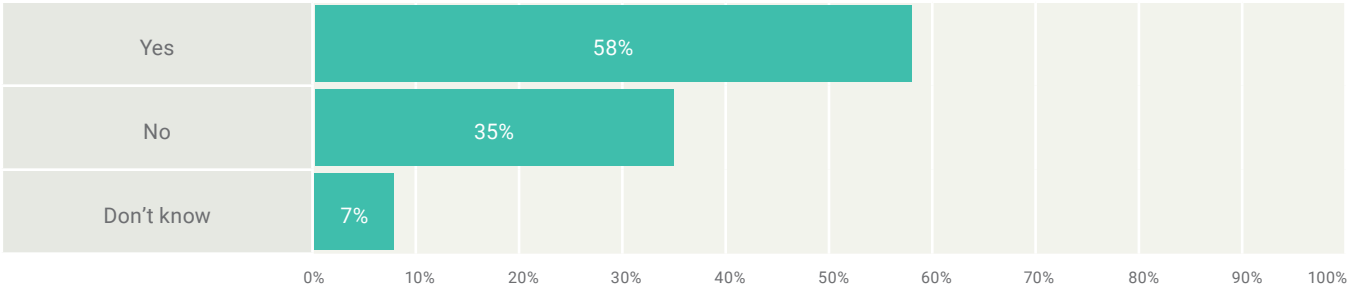
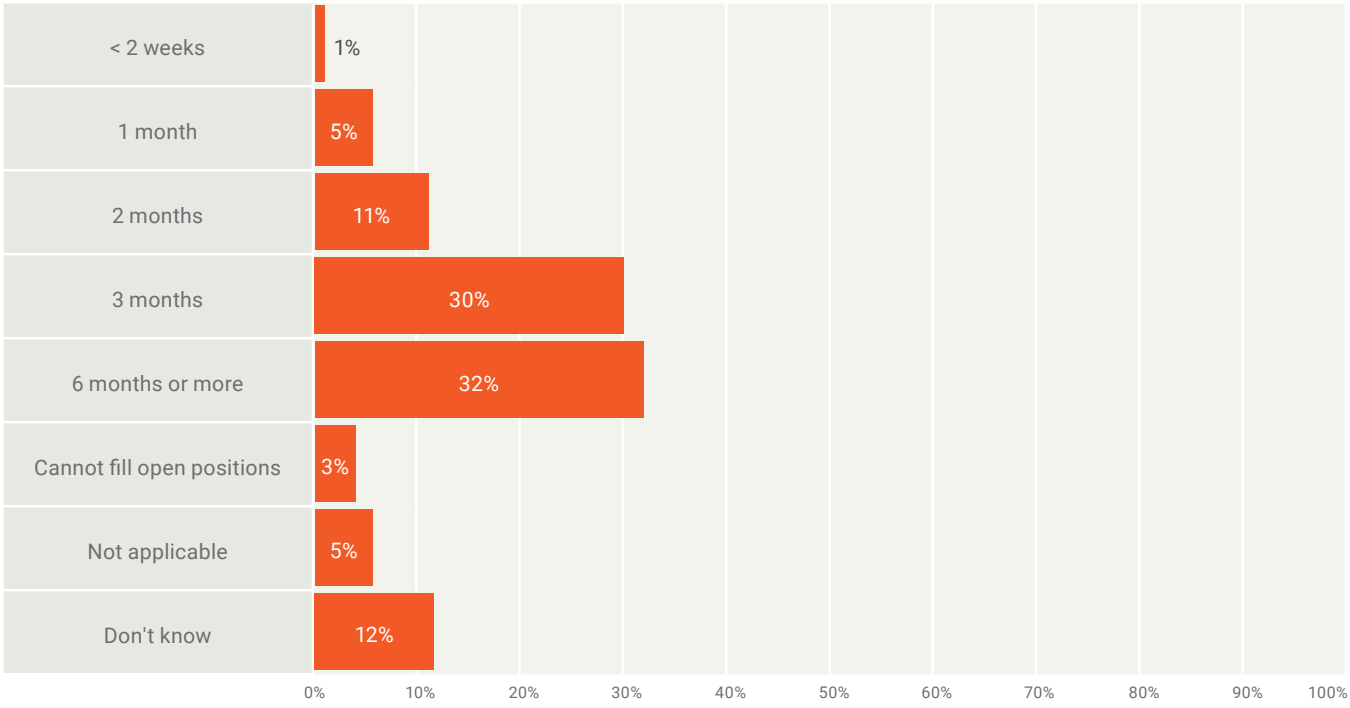


FIGURE 4—TIME TO FILL A CYBERSECURITY POSITION

On average, how long does it take your organization to fill a cybersecurity position with a qualified candidate?



the survey respondents note that less than one quarter of applicants have the sufficient qualifications to be considered for open cybersecurity positions (**figure 5**). Compared to data from last year's survey, these statistics are basically unchanged and indicate a static state of struggle in attracting qualified applicants.

Examining the makeup of these types of unfilled cybersecurity positions aids in identifying the type of talent which is missing within the cybersecurity field overall. The majority of survey respondents report that most vacancies are in technical cybersecurity positions—52 percent of respondents indicate that

FIGURE 5—PERCENTAGE OF CYBERSECURITY APPLICANTS WHO ARE WELL QUALIFIED

On average, how many cybersecurity applicants are well qualified for the position for which they are applying?

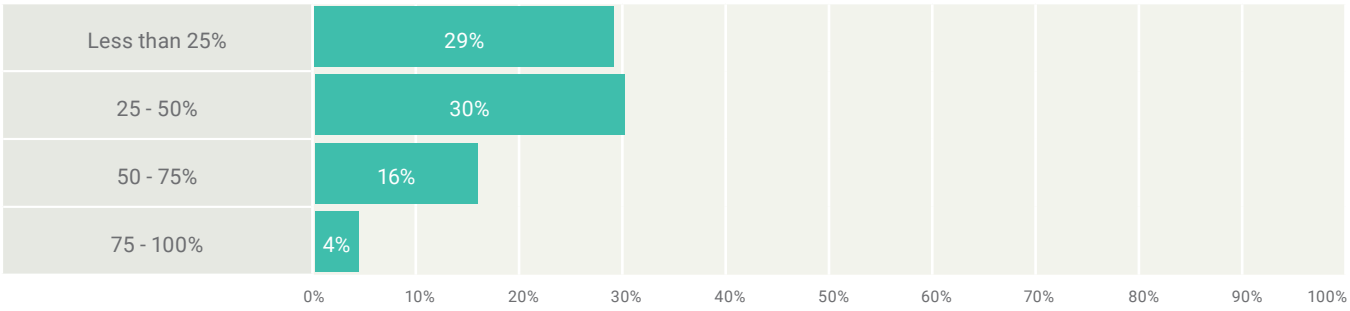
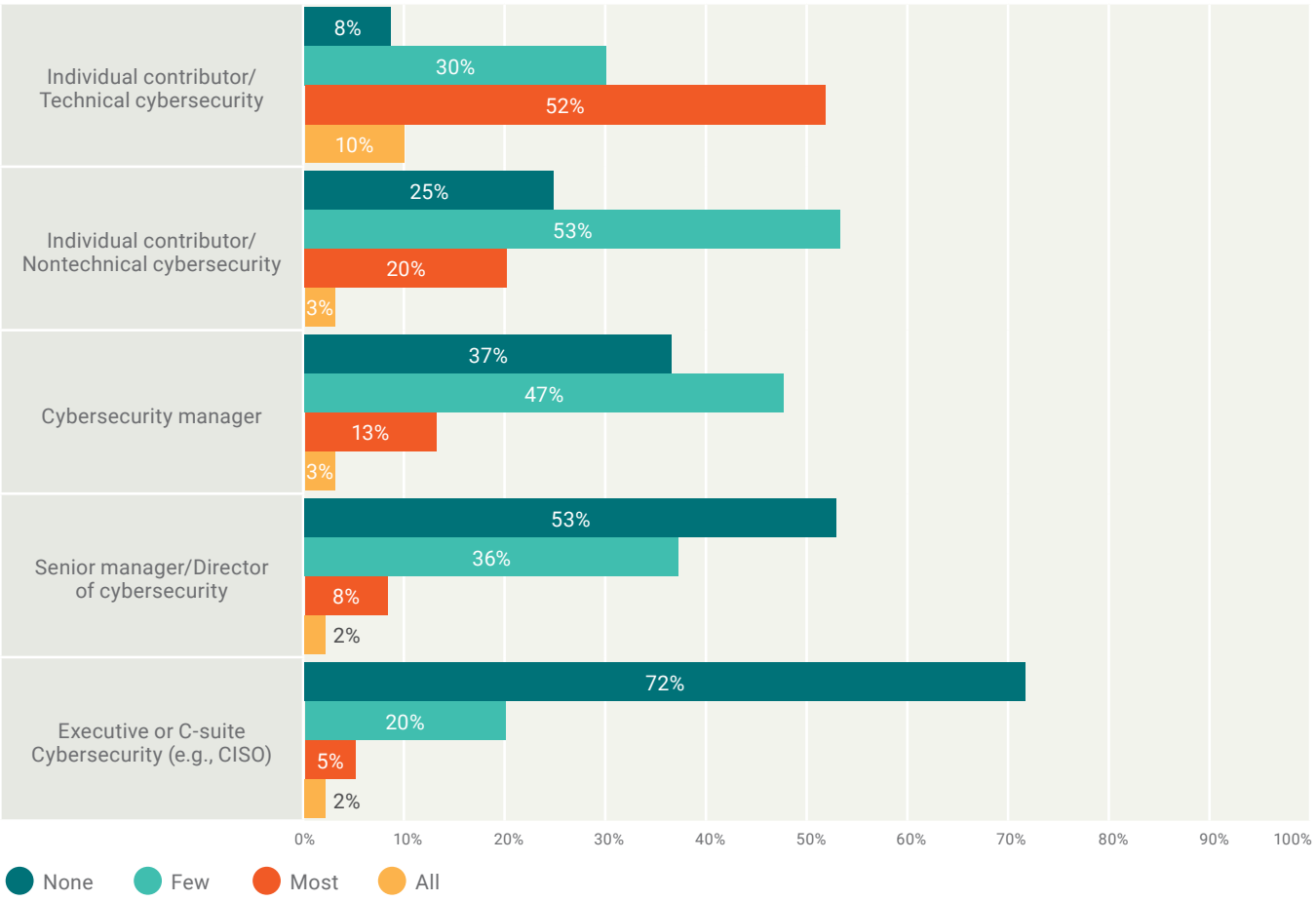


FIGURE 6—PERCENTAGES OF UNFILLED POSITIONS AT GIVEN ORGANIZATIONAL LEVELS

How many of your unfilled (open) cybersecurity positions are at the following levels?



most cybersecurity open positions at their enterprises are technical cybersecurity positions at the individual contributor level (**figure 6**). Conversely, few cybersecurity executive or C-suite positions are unfilled—72 percent of respondents indicate that their enterprises have no cybersecurity executive position openings (**figure 6**).

Adding to these hiring needs, 75 percent of survey respondents expect an increase in hiring demand for technical professionals, with no specific role or level experiencing a noteworthy decline in demand (**figure 7**). This is relatively inline with the 77 percent response from last year's survey, showing a minimal change. Comparing this year's survey responses to the previous year's data for the same question reveals negligible changes in trends, indicating that the need for cybersecurity technical personnel is still strong and growing across enterprises.

More Business Acumen Needed

Although the cybersecurity field has a great need for technical competence and qualifications, it also suffers from a lack of business comprehension. Specifically, the biggest skill gap in the average cybersecurity professional that survey respondents identified is the ability to understand the business. Forty-nine percent of respondents identify this ability as the biggest skill gap, and 34 percent report that the biggest skill gap is technical skills (**figure 8**). This data, combined with the large need for technically skilled individuals, helps to determine the ideal cybersecurity professional in today's

FIGURE 7—HIRING DEMAND PER ORGANIZATIONAL LEVEL

In the next year, which of these levels do you see the hiring demand increasing, decreasing or remaining the same?

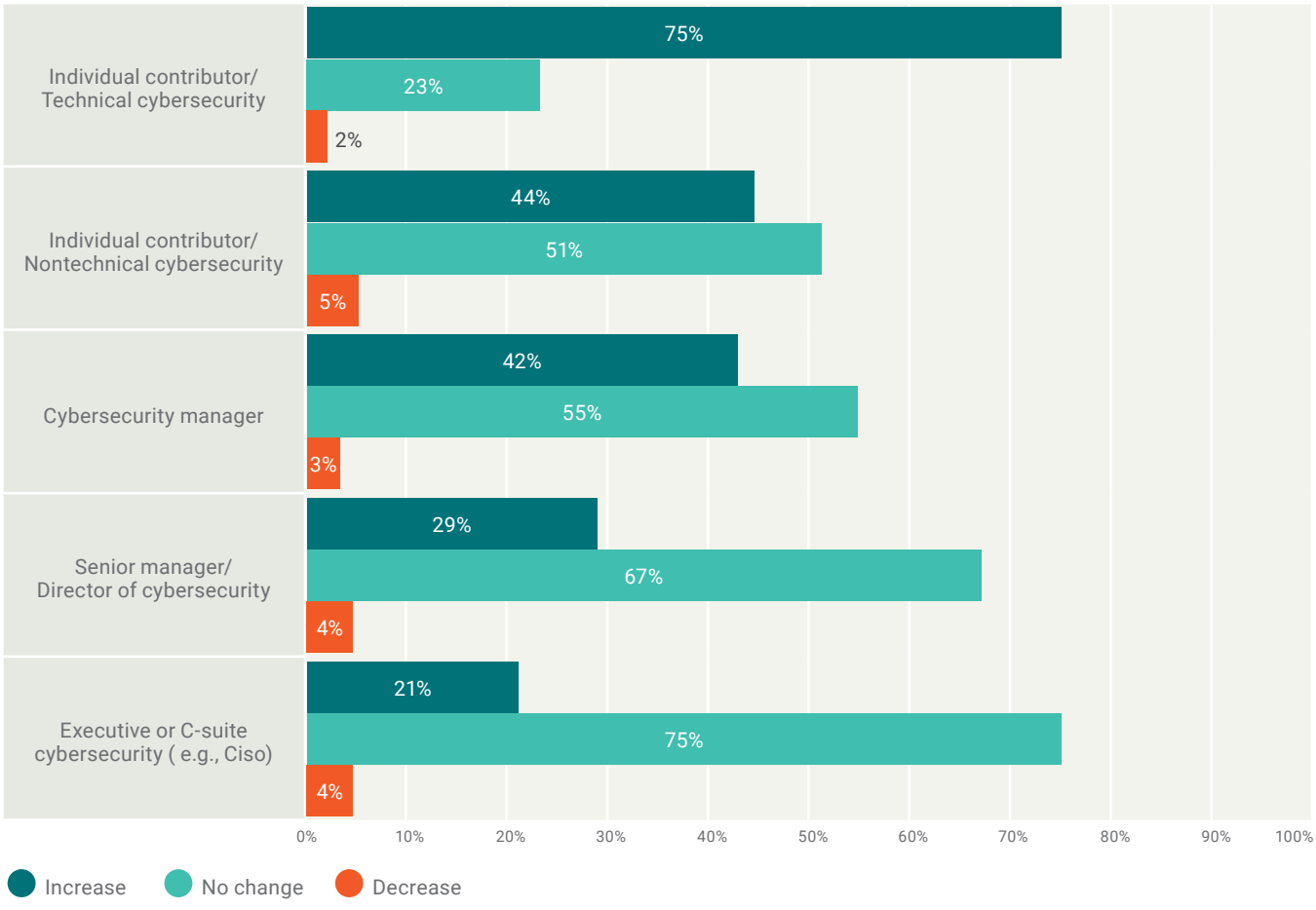
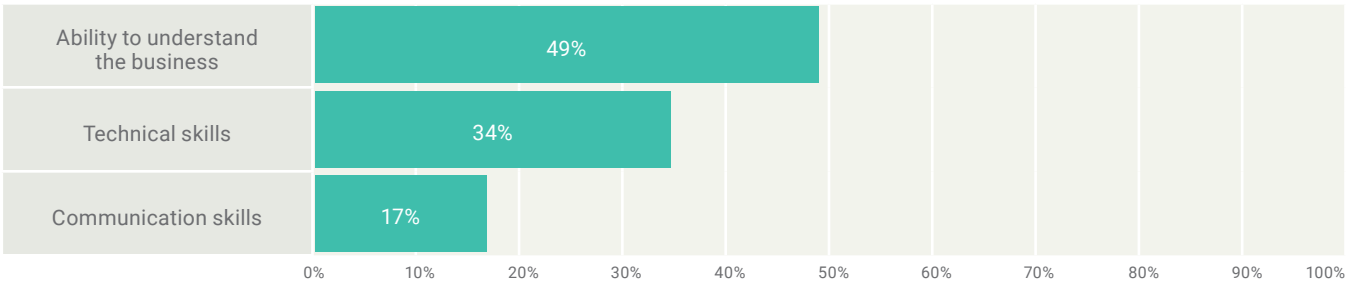


FIGURE 8—BIGGEST SKILL GAP

What is the biggest skill gap you see in today's cybersecurity professionals?

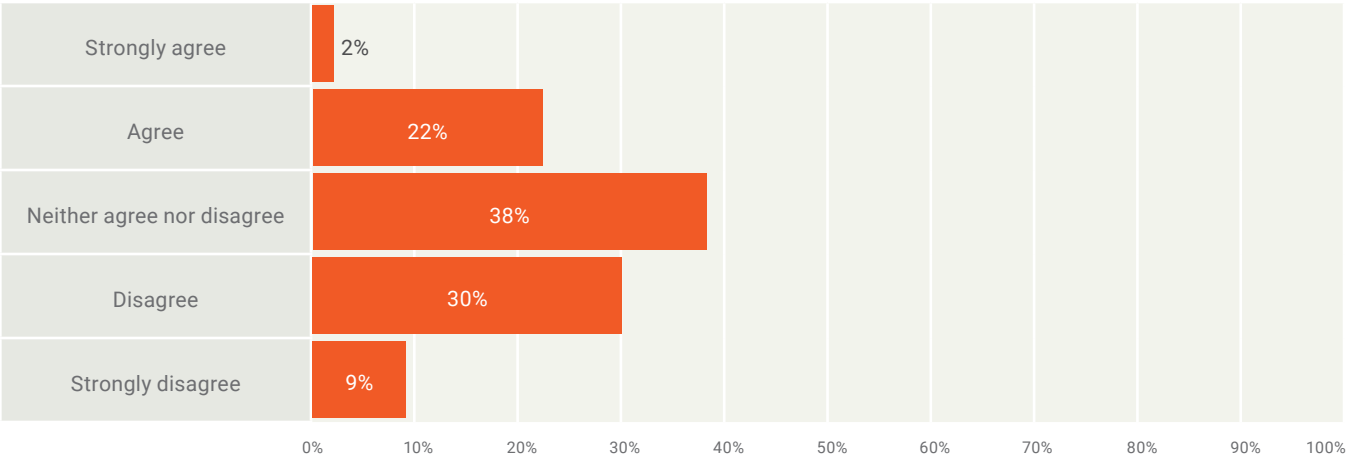


environment—a technically proficient cybersecurity professional who is able to understand an enterprise's business strategy. Indeed, an individual who can successfully apply his or her technical cybersecurity skillset to effectively enhance business goals and who can articulate that connection to counterparts at multiple organizational levels has a bright future in the field.

Discovering and hiring individuals to meet this great need within the cybersecurity field has received some help from more traditional academic institutions; however, additional work is required. Twenty-four percent of survey respondents agree or strongly agree that recent university graduates in cybersecurity are well prepared for challenges within an enterprise; 39 percent of respondents disagree or strongly disagree; and 38 percent neither agree nor disagree (**figure 9**). Analysis of this data can create multiple interpretations. First, like many fields of study, formal education alone does not necessarily provide turn-key-ready professionals. Second, although some academic institutions are implementing successful technical programs, most are still perceived as training cybersecurity in abstraction, rather than training it as a technical, hands-on field, which, by its very nature, requires some business intelligence.

FIGURE 9—DEGREE TO WHICH UNIVERSITY GRADUATES ARE WELL PREPARED FOR CYBERSECURITY CHALLENGES

To what extent do you agree or disagree that recent university graduates in cybersecurity are well prepared for the cybersecurity challenges in your organization?



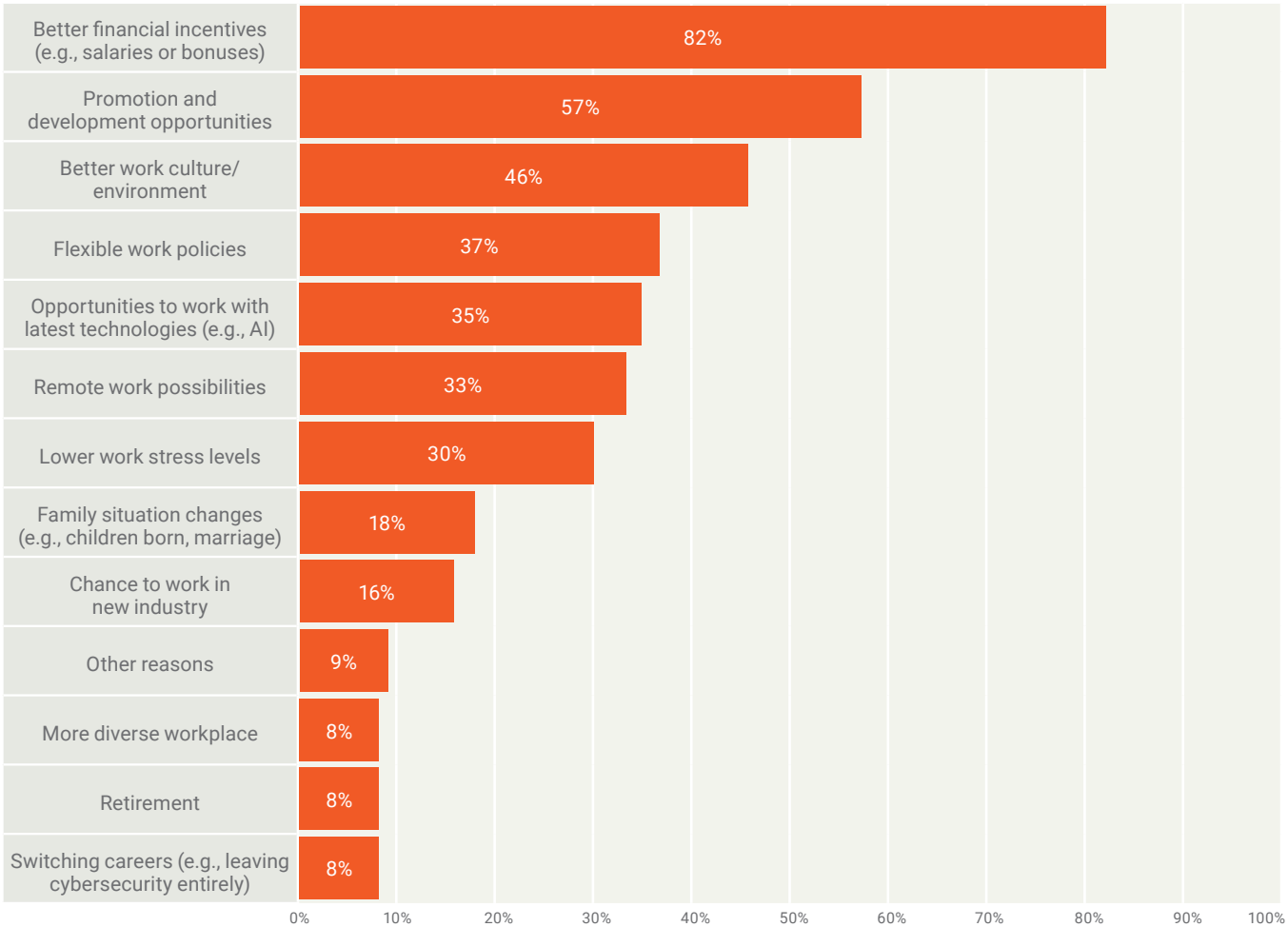
Retaining Cybersecurity Professionals Is Exceptionally Difficult

Retention Issues From a Seller's Market

The environment of need in the cybersecurity field has led to a strong seller's market for cybersecurity professionals, creating a retention problem for enterprises. When asked if their organization has experienced difficulties retaining qualified cybersecurity professionals, 64 percent of survey respondents replied affirmatively. An overwhelming 82 percent of survey respondents indicate that most cybersecurity professionals left their organizations for better financial incentives, such as salaries or bonuses, at other organizations. Over half of respondents also accredit promotion and development opportunities as contributing to retention struggles, and nearly half of respondents indicate that individuals left their organization for a better work culture or environment (**figure 10**).

FIGURE 10—WHY CYBERSECURITY PROFESSIONALS LEAVE THEIR JOBS

Which of the following factors do you feel are causing cybersecurity professionals to leave their job roles?



These findings indicate that a seller's market currently exits in the cybersecurity field. Enterprises are offering higher pay, career advancement and appealing work environments to lure proven cybersecurity talent away from other enterprises. These incentives are impactful for any work field; however, in the context of the large skill and capability gap in the cybersecurity field, it is understandable that the contributing factors are more prevalent when compared to other professions' trends in retaining skilled staff.

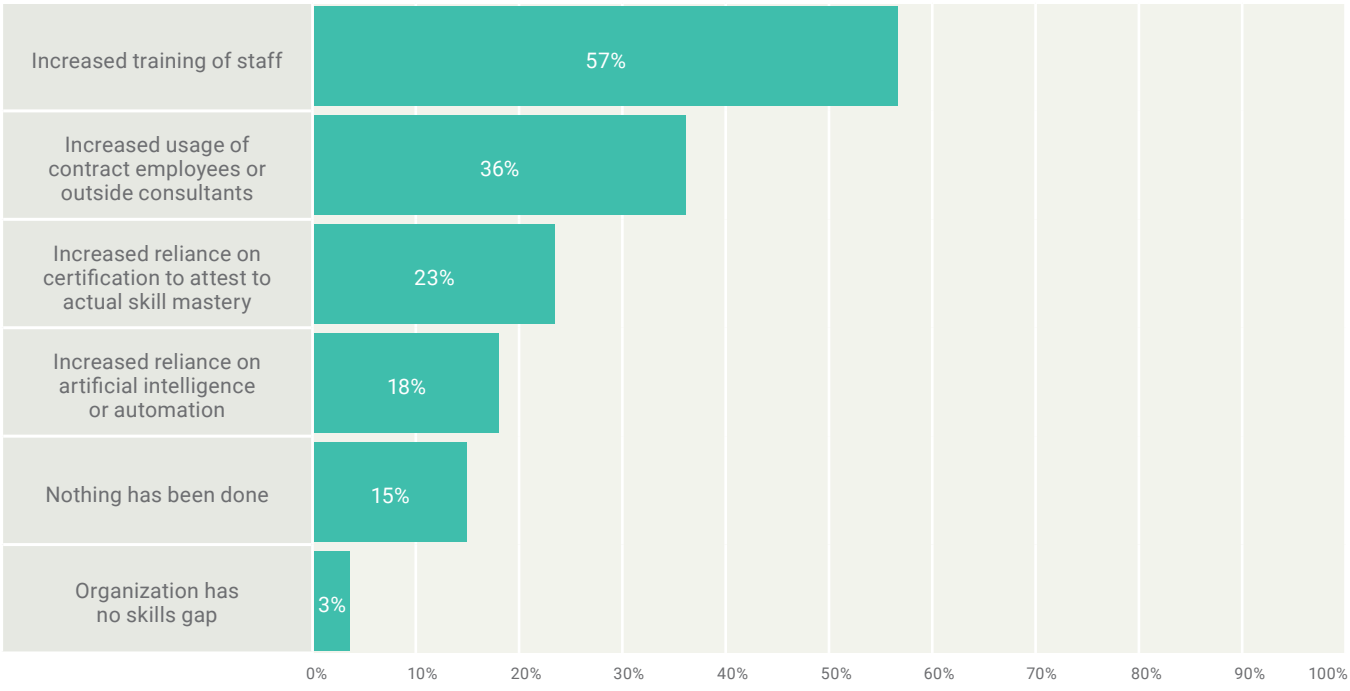
Strategies to Combat Loss

Enterprises are implementing multiple strategies to retain cybersecurity professionals. One frequently used incentive is providing additional training. Fifty-seven percent of respondents indicate that their enterprises undertake increased training as an incentive for employees to stay at their enterprises (**figure 11**). The prevalence of this retention tool is understandable, because both the individual and the enterprise benefit from more highly trained professionals. Additionally, some organizations mitigate the retention issue by requiring training agreements that include post-training term requirements, ensuring that employees do not leave immediately after receiving training; otherwise, they experience stiff financial penalties.

Other retention efforts utilized by respondents include increased use of contract employees and outside consultants (36 percent) and increased reliance on certification to attest to actual skill mastery (23 percent) (**figure 11**). These methods are also proven and commonplace in other professions. Leveraging a third party for cybersecurity purposes shifts the staffing requirements, including recruiting and retaining staff, to another organization. This method allows an enterprise to decrease any potential risk that may arise from attempting to obtain and maintain cybersecurity professionals natively. The use of certifications is also an understandable method of retention as individuals in the cybersecurity field find great professional pride and personal satisfaction in obtaining a certification in the field.

FIGURE 11—MEANS TO MITIGATE CYBERSECURITY SKILLS GAP

Which, if any, of the following has your organization undertaken to help decrease this cybersecurity skills gap?



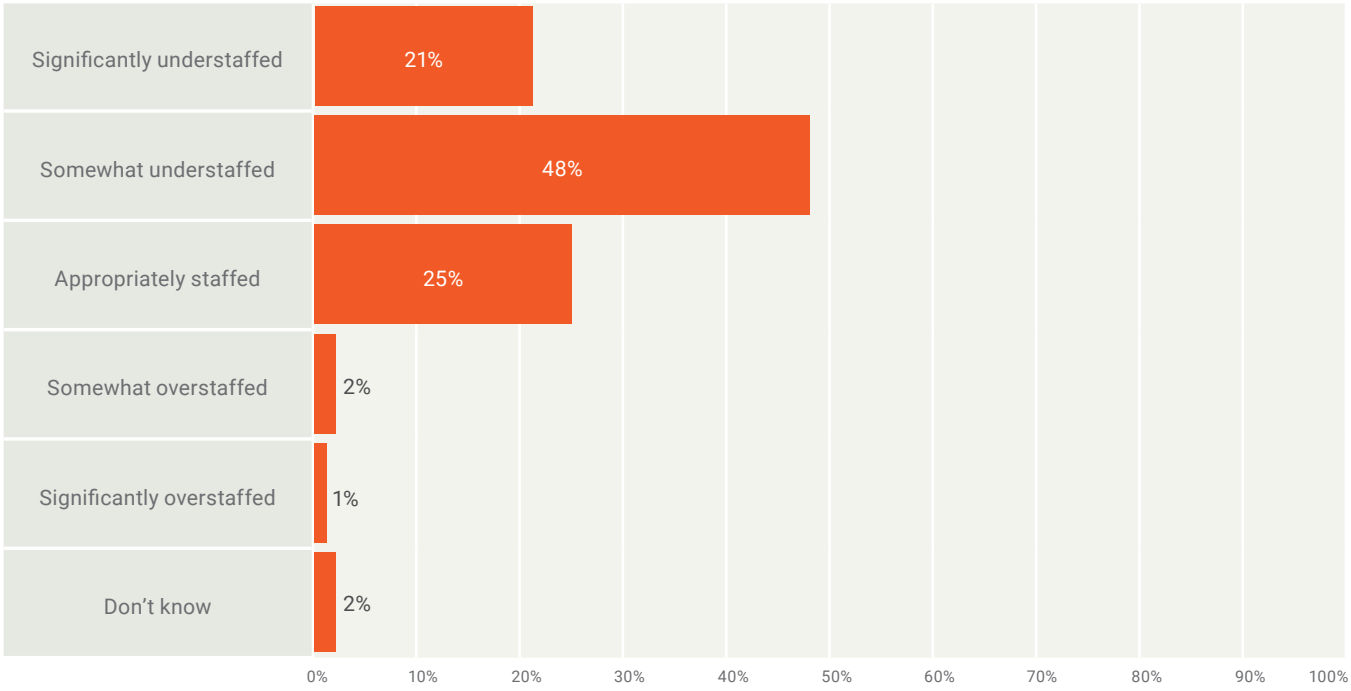
Eighteen percent of respondents indicate that their enterprises are relying more heavily on artificial intelligence to decrease the cybersecurity skills gap (**figure 11**). Although these software solutions and networked algorithms are becoming more prevalent in all fields, they have yet to prove themselves as capable of complete workforce replacement. Respondents were not asked to indicate the effectiveness of these artificial intelligence tools as replacements for trained and experienced human beings.

Perception of Under-Preparedness

The lack of trained cybersecurity professionals profoundly impacts enterprises and the professionals within them. Almost 70 percent of respondents believe that their enterprise's cybersecurity team is understaffed, with over 20 percent of respondents indicating that they perceive their enterprise as significantly understaffed (**figure 12**). Despite leveraging incentives, such as education and certification opportunities, these enticements are seemingly insufficient in the current market to retain individuals. As a result, an overall perception of under-preparedness arises.

FIGURE 12—PERCEPTION OF CYBERSECURITY STAFFING LEVELS

Do you feel that your organization's cybersecurity team is currently:



Gender Diversity Programs Are Declining, and Their Effectivity Is Directionally Lower

Gender Diversity and Disparity

The survey results identify a male dominant field in cybersecurity—89 percent of respondents indicate that there are more men than women in cybersecurity roles within their enterprise (**figure 13**). Of note, 15 percent of respondents indicate that their entire cybersecurity group is comprised of men and 51 percent report that there are significantly more men that women occupying cybersecurity roles within their enterprise (**figure 13**).

While this trend of a male-dominated cybersecurity work field is noteworthy, most respondents believe that women are offered the same opportunities for career advancement as men, with 80 percent responding that opportunity is equally distributed (**figure 14**). However,

FIGURE 13—PROPORTION OF MEN VS. WOMEN IN CYBERSECURITY ROLES

How would you describe the current proportion of men versus women in cybersecurity roles in your organization?

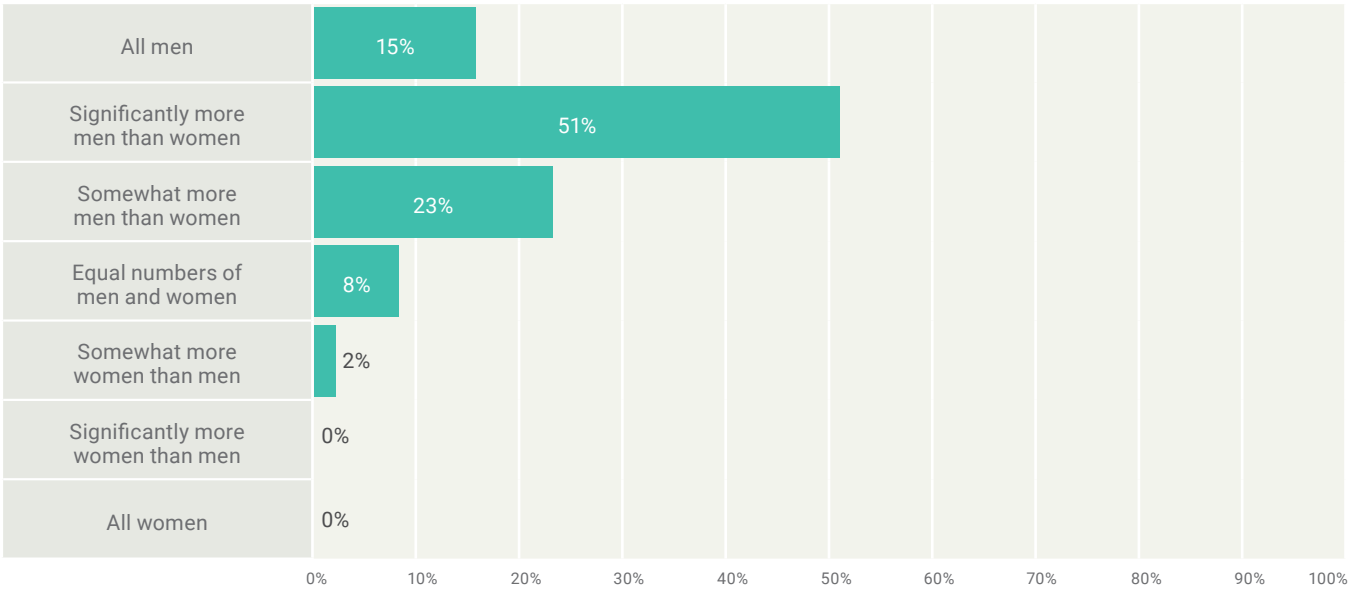
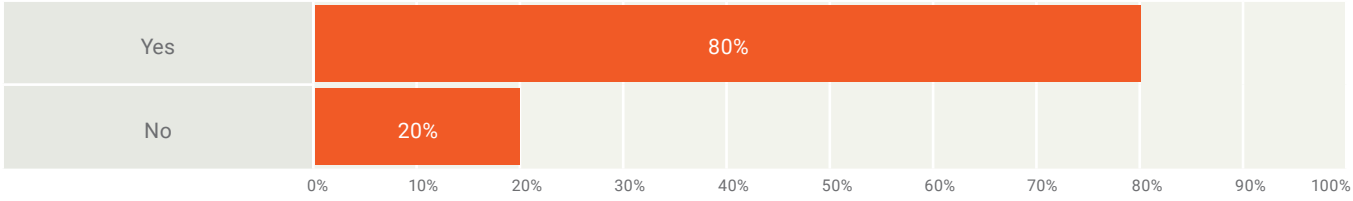


FIGURE 14—GENDER DISPARITY

Do you believe that women are offered the same opportunities for career advancement as men are offered in the field of cybersecurity in your organization?



further analysis provides potentially more meaningful insight. Of respondents who identify as female, only 41 percent believe that opportunity for career advancement is equally distributed (**figure 15**). This response represents a downward trend from last year's survey, which indicated that 51 percent of female respondents believed career advancement opportunities were equally distributed.

Compounding the downward trend of opportunity perception, just over half of the survey respondents (56 percent) indicate that their organization does not currently have a goal of increasing the number of women in cybersecurity roles. This result may be due to the fact that 71 percent of respondents indicate they have no difficulty in retaining women in cybersecurity roles (**figure 16**).

Gender Gap Mitigation

Some cybersecurity organizations establish diversity programs to support women in the field. These programs take many forms, most often with the goal to ensure that women have the same level of access to training and advancement opportunities as men. Compared to last year, however, the ISACA survey

FIGURE 15—BREAKDOWN OF GENDER DISPARITY RESPONSES

Do you believe that women are offered the same opportunities for career advancement as men are offered in the field of cybersecurity in your organization?

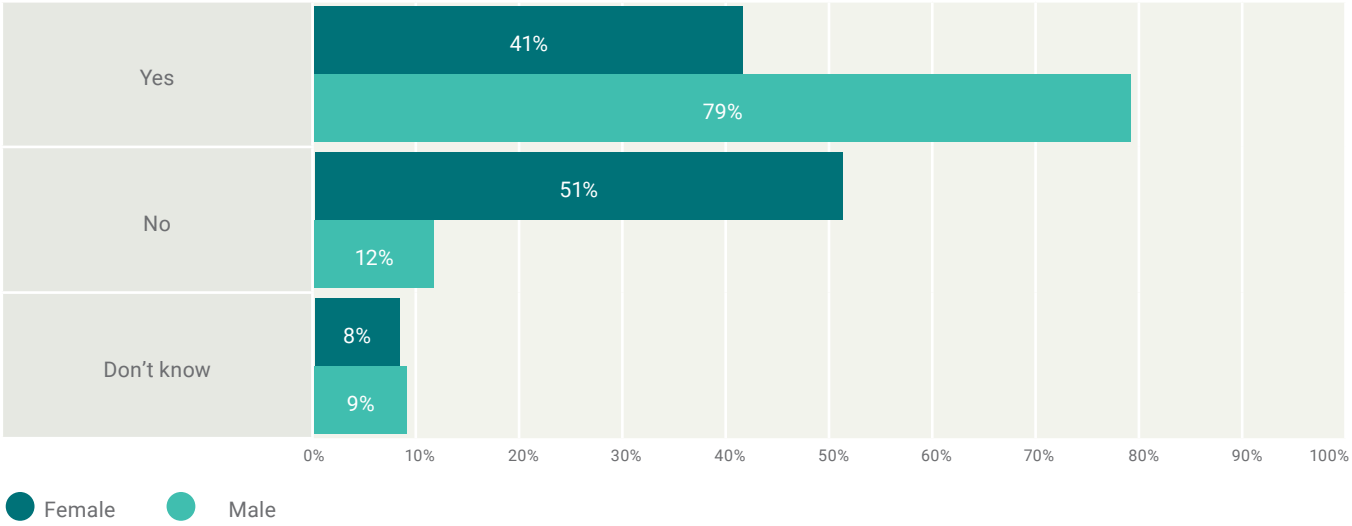


FIGURE 16—RETENTION OF WOMEN IN CYBERSECURITY ROLES WITHIN AN ORGANIZATION

Has your organization experienced difficulty in retaining women in cybsersecurity roles?

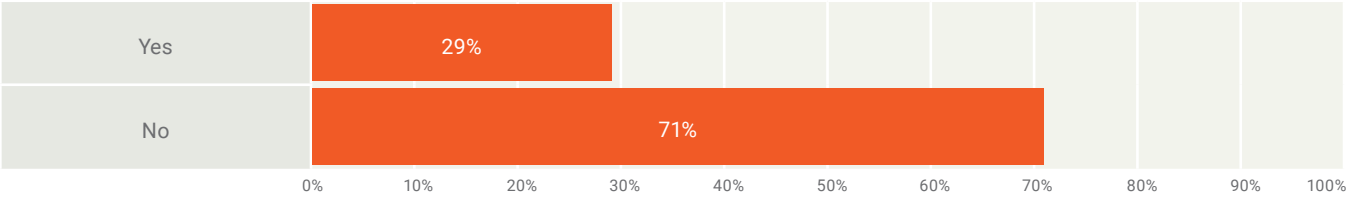
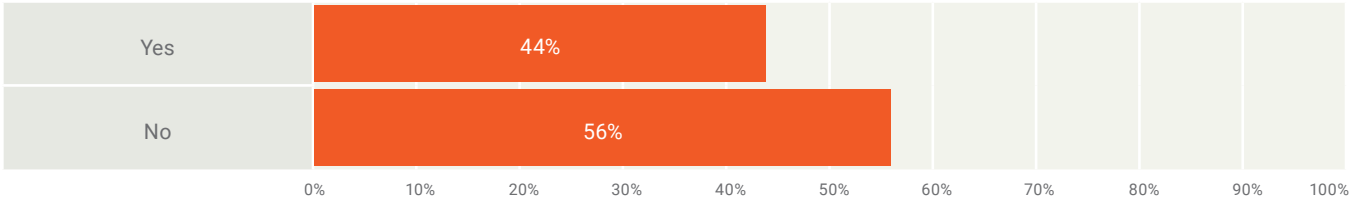


FIGURE 17—DIVERSITY PROGRAMS

Does your organization have in place specific diversity programs to support women cybersecurity professionals?



shows that these programs may be declining. Correlating directly to the question about whether an enterprise has a goal of increasing the number of women in cybersecurity roles (44 percent of this year's respondents report that this is a goal), when respondents were asked if their enterprises have specific diversity programs to support women cybersecurity professionals, 44 percent also report affirmatively (**figure 17**). This represents a seven-percentage-point decrease from the previous year.

In addition to the decline in the number of programs supporting women cybersecurity professionals, those that are in place are arguably decreasing in effectiveness. Among respondents in enterprises with a diversity program, 59 percent of women believe that women are offered the same opportunities for career advancement as men. This represents an 18-percentage-point decrease compared to last year, the first year that diversity data was collected. In contrast, this year, 90 percent of men respondents in enterprises with a diversity program believe equal opportunity for advancement exists within their enterprise (a three-percentage-point increase from last year). The gap between men's and women's perceptions in organizations that have a diversity program has increased from 10 percentage points last year to 31 percentage points this year. In short, when comparing last year's data to this year's data, the effectiveness of diversity programs appears to be trending downward, at least with regard to women's perceptions of these programs.

Enterprise Implications

Previous reporting and surveys have indicated that diversity programs may have aided in providing variety to the workforce. Analysis of the current data should prompt consideration and potential reappraisal of these programs' impact and effectiveness. However, those enterprises that do have female cybersecurity talent should find reassurance in the strong retention numbers of those professionals.

Cybersecurity Budget Increases Are Expected to Slow Slightly

Compared to last year, cybersecurity budgets are expected to decrease in 2019, but not to the lower levels of previous years. Specifically, when asked, 55 percent of respondents report that they expect an increase in cybersecurity budgets (**figure 18**), which is a decrease of nine points from last year's 64 percent. These results seem to align with a cyclical pattern where every other year cybersecurity budgets increase.

FIGURE 18—CHANGE IN ENTERPRISE SECURITY BUDGETS

How, if any, will your organization's cybersecurity budget change in the next twelve months?

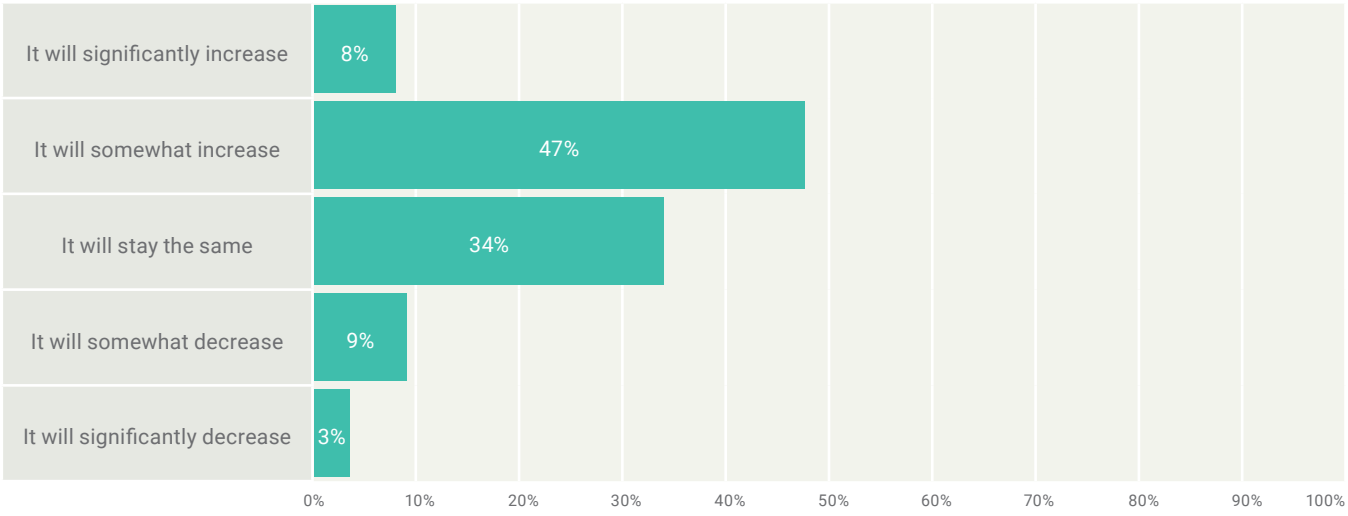
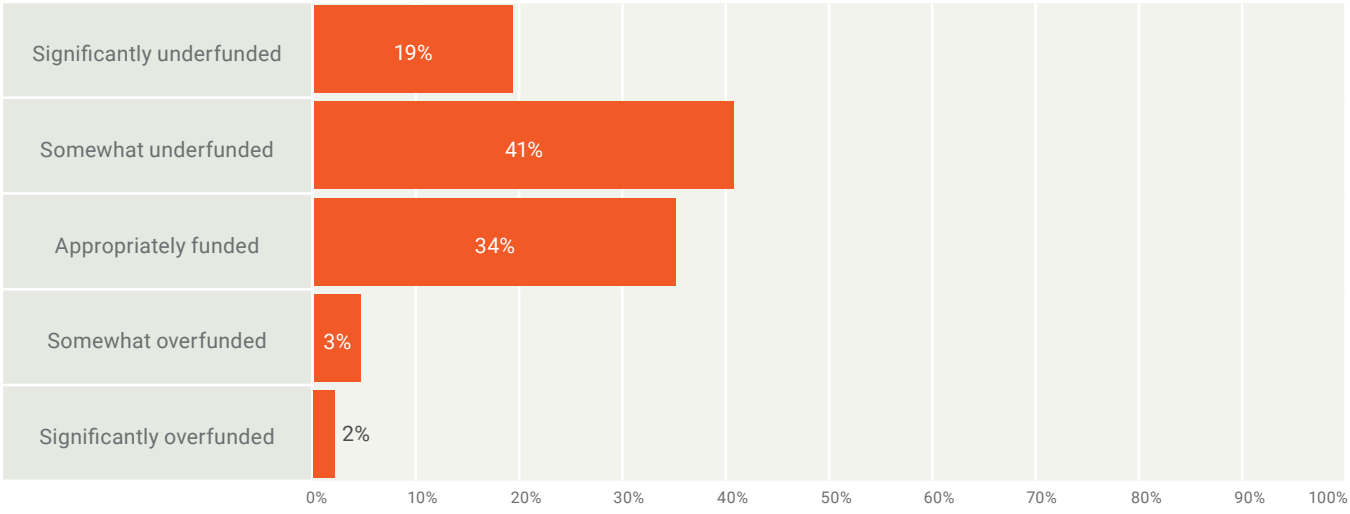


FIGURE 19—PERCEPTION OF CYBERSECURITY BUDGET FUNDING LEVEL

Do you feel your organization's cybersecurity budget is currently...



These changing financial projections may act as reflections of current budget perceptions. Sixty percent of survey respondents indicate that they feel that their cybersecurity budget is currently underfunded, with nearly 20 percent believing that their budgets are significantly underfunded (**figure 19**). Analysis of these statistics, in combination with the decreased budgetary expectations, may have the potential to create under-supported cybersecurity staff and tools, feeding the retention struggles of the previously identified findings.

Conclusion: Current Trends Present Opportunities for the Bold

The cybersecurity workforce gap is becoming more pronounced as talent becomes more difficult to find. These strong headwinds are compounded by a suppliers' market for the talent that exists, creating a highly competitive environment in which traditional retention strategies—such as education and certification incentives—lose out to incentives like greater pay and career advancement that entice individuals to seek employment at a different enterprise. Furthermore, organizational attempts to diversify the workforce and create greater gender inclusion are failing to meet the expectations of individuals within the field, many of whom those programs are designed to benefit. Finally, expectations of lower budgets will continue to feed the reality of underfunded security programs and insufficient staff.

Although these statistics may prove disheartening to some, they actually present great opportunity for enterprises with initiative. Today's skilled cybersecurity professionals are in high demand. Organizations that acknowledge the statistics shown in this research should be able to fill open positions quicker and retain their current talent. The successful hiring and retention elements are attractive pay, career growth opportunities and healthy work environments. However, enterprises that rely solely on old approaches and the status quo approach may continue to experience hiring and retention issues.

Acknowledgments

ISACA would like to recognize:

Lead Developer

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

Expert Reviewers

Dustin Brewer
CSXP, CEH, CHFI, CSIS
ISACA, USA

Marie Gilbert
ISACA, USA

Karen Heslop, J.D.
ISACA, USA

ISACA Board of Directors

Rob Clyde, Chair
CISM
Clyde Consulting LLC, USA

Brennan Baybeck, Vice-Chair
CISA, CRISC, CISM, CISSP
Oracle Corporation, USA

Tracey Dedrick
Former Chief Risk Officer with Hudson City Bancorp, USA

Leonard Ong
CISA, CRISC, CISM, CGEIT, COBIT 5 Implementer and Assessor, CFE, CIPM, CIPT, CISSP, CITBCM, CPP, CSSLP, GCFA, GCIA, GCIH, GSNA, ISSMP-ISSAP, PMP
Merck & Co., Inc., Singapore

R.V. Raghu
CISA, CRISC
Versatilist Consulting India Pvt. Ltd., India

Gabriela Reynaga
CISA, CRISC, COBIT 5 Foundation, GRCP
Holistics GRC, Mexico

Gregory Touhill
CISM, CISSP
Cyxtera Federal Group, USA

Ted Wolff
CISA
Vanguard, Inc., USA

Tichaona Zororo
CISA, CRISC, CISM, CGEIT, COBIT 5 Assessor, CIA, CRMA
EGIT | Enterprise Governance of IT (Pty) Ltd, South Africa

Theresa Grafenstine
ISACA Board Chair, 2017-2018
CISA, CRISC, CGEIT, CGAP, CGMA, CIA, CISSP, CPA
Deloitte & Touche LLP, USA

Chris K. Dimitriadis, Ph.D.
ISACA Board Chair, 2015-2017
CISA, CRISC, CISM
INTRALOT, Greece

About ISACA

Now in its 50th-anniversary year, ISACA® (isaca.org) is a global association helping individuals and enterprises achieve the positive potential of technology. Today's world is powered by information and technology, and ISACA equips professionals with the knowledge, credentials, education and community to advance their careers and transform their organizations. ISACA leverages the expertise of its 460,000 engaged professionals—including its 140,000 members—in information and cybersecurity, governance, assurance, risk and innovation, as well as its enterprise performance subsidiary, CMMI® Institute, to help advance innovation through technology. ISACA has a presence in more than 188 countries, including more than 220 chapters worldwide and offices in both the United States and China.

About HCL

HCL Technologies (HCL) is a leading global technology company that helps global enterprises reimagine and transform their businesses through digital technology. HCL operates in 44 countries and had consolidated revenues of US $8.4 billion for the 12 months ending 31 December 2018. HCL provides an integrated portfolio of services informed by its Mode 1-2-3 growth strategy. Mode 1 encompasses core services in the areas of applications, infrastructure, business processes outsourcing (BPO) and engineering, research and development services, leveraging DRYiCE™ Autonomics to transform clients' business and IT landscape, making them lean and agile. Mode 2 focuses on experience-centric, outcome-oriented, integrated offerings of Digital and Analytics, IoT WoRKS™, Cloud Native Services, and Cybersecurity and GRC services to drive business outcomes and enable enterprise digitization. Mode-3 strategy is ecosystem-driven, creating innovative IP-partnerships to build product and platform business. HCL leverages its global network of integrated co-innovation labs to provide holistic multiservice delivery in key industry verticals including financial services, manufacturing, telecommunications, media, publishing, entertainment, retail and consumer packaged goods, life sciences and healthcare, oil and gas, energy and utilities, travel, transportation and logistics, and government. With 132,328 professionals from diverse nationalities, HCL creates real value for customers by taking 'Relationships Beyond the Contract'. For more information, please visit www.hcltech.com.

Disclaimer

ISACA has designed and created *State of Cybersecurity 2019, Part 1: Current Trends in Workforce Development* (the "Work") primarily as an educational resource for IT professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, IT professionals should apply their own professional judgments to the specific circumstances presented by the systems or information technology environment.

RESERVATION OF RIGHTS

ISACA®

1700 E. Golf Road, Suite 400
Schaumburg, IL 60173, USA

Phone: +1.847.660.5505
Fax: +1.847.253.1755
Support: support.isaca.org
Web: www.isaca.org

Provide feedback:
www.isaca.org/state-of-cybersecurity-2019

Participate in the ISACA Online Forums:
https://engage.isaca.org/onlineforums

Twitter:
www.twitter.com/ISACANews

LinkedIn:
www.linkedin.com/company/isaca

Facebook:
www.facebook.com/ISACAHQ

Instagram:
www.instagram.com/isacanews

CyberSecurity & GRC Services
by HCL Technologies

HCL

INSPIRING BUSINESS CONFIDENCE THROUGH DYNAMIC CYBERSECURITY

21+ years of experience

Recognized by Gartner, Everest, IDC, ISG

350+ Client Relationships

www.hcltech.com