CSX™
CYBERSECURITY NEXUS

State of Cybersecurity 2018

Part 1: Workforce Development

Abstract

State of Cybersecurity 2018 reports the results of the annual ISACA global *State of Cybersecurity Survey*, conducted in October 2017. Overall results confirm that cybersecurity remains dynamic and turbulent as the field continues to mature.

To equip you with a comprehensive understanding of the cybersecurity industry through the lens of those who define it—the managers and practitioners—ISACA is presenting a series of white papers that focus on individual survey topics. This report is the first in the *State of Cybersecurity 2018* series. It highlights cybersecurity workforce development and current trends.

As cyberattacks continue to threaten enterprises of all kinds, executives are placing critical priority on building teams of experts for cyberdefense. As we know from prior surveys, many executives and managers encounter a skills gap as they search for the right resources—with the right expertise—to accomplish the goal. This year's paper explores the contours of the skills gap in more depth—which skills are missing, and at what levels in the organization they report. It further examines the characteristics of the security workforce, particularly women's opportunities for career advancement.

ISACA®

Table of Contents

Executive Summary

This year's global *State of Cybersecurity Survey* reveals several clear challenges for enterprises. In this first white paper of a three-part series, ISACA presents findings related to staffing, workforce development, budget and organization of security teams. In a second paper, ISACA examines survey results regarding the threat landscape, including types of threats that enterprises encounter, defense mechanisms and their success in meeting challenges in the field.

Enterprises continue to struggle with funding, staffing and retaining an adequate security workforce. This year, the ISACA survey explores the skills gap in greater detail to identify missing talent and expertise and locate the gaps organizationally. The survey traces characteristics of the security workforce, placing particular emphasis on women and their opportunities for advancement.

Key Findings

Practitioners know anecdotally that finding, acquiring and retaining a skilled workforce in security is challenging. Prior years' results of the ISACA survey (and numerous third-party surveys) have highlighted the issue. This year, ISACA's *State of Cybersecurity Survey* findings reveal additional characteristics of the skills gap; they also uncover several contributing or potentially exacerbating factors that impact security staffing, skill building and talent retention.

Following are the key findings related to acquiring and maintaining a robust workforce:

- **Skills challenges remain but are better understood.** The skills gap continues unabated. Enterprises still have open security positions, and the time to fill them appears to have decreased slightly. Demand is greatest for skilled technical resources at the individual-contributor level, rather than the management or executive level. For job seekers, technical skills are a strong differentiator—especially those that can be objectively demonstrated. For enterprises, automating security activities and better, more efficient vetting of security technical personnel may create competitive advantage.
- **Gender disparity is present but can be mitigated.** Men perceive similar opportunities in security careers, regardless of gender; however, their perceptions are not shared by women colleagues. Active enterprise diversity efforts help to equalize (but do not fully mitigate) this disparity.
- **Budgets are once again increasing.** Last year, survey results suggested that budgets were expanding, but more slowly relative to prior years. This year, the trend is reversed. Instead of further erosion in the rate of budget expansion, respondents predict that budgets will increase at a higher rate than last year. In ISACA's 2017 report, 50 percent of respondents predicted that budgets would grow, down from 61 percent in 2016. This year's data suggest a return to even higher levels—64 percent of respondents indicate that their security budgets will expand. Given that funding levels are increasing, investment in skill development (e.g., training) and talent retention may increase throughout 2018.
- **Confidence in preparedness is increasing, but organizational alignment is inconsistent.** Respondents are slightly more confident in how security is prioritized within their enterprises. There is a slight uptick in practitioner perception that the board of directors appropriately prioritizes security efforts. Despite the increasing confidence, however, results suggest a lack of consensus about organizational placement (i.e., reporting structure) for security teams, and a wide array of approaches are in active use.

Difficulty in finding and filling open positions decreased slightly over last year's survey findings. Given that security budgets are increasing, the staffing problem is logistical rather than financial; enterprises have budget to hire, but are challenged in recruiting talented practitioners because a large segment of the available workforce lacks the skills that enterprises need. Consequently, enterprises struggle to fill open positions and cannot readily backfill openings when employees leave.

Survey Methodology

ISACA sent the survey 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. A total of 2,366 individuals participated in the survey and their responses are included in the results.[1] A typical respondent is described in **figure 1**.

Survey data were collected anonymously through SurveyMonkey®. Results reveal positive and negative findings about the current state of cybersecurity. The survey, which uses multiple-choice and Likert-scale formats, is organized into four major sections:

Skills Challenges Remain But Are Better Understood

Gender Disparity Is Present but Can Be Mitigated

Budgets Are Increasing Once Again

Confidence in Preparedness Is Increasing, but Organizational Alignment Is Inconsistent

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.

FIGURE 1—TYPICAL RESPONDENTS

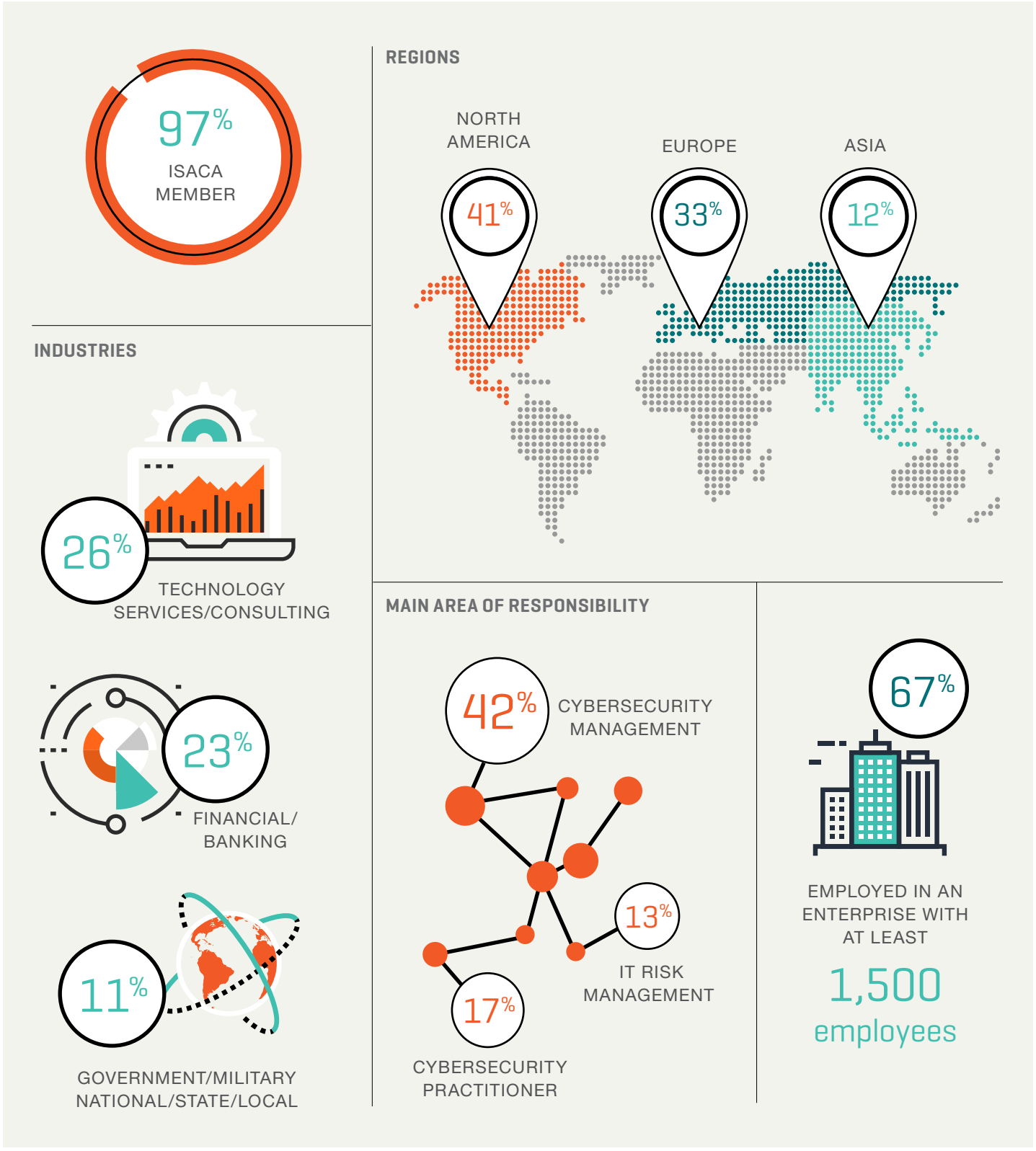


Figure 1 represents norms of the sample population. While typical patterns are interesting to consider, it is also important to note some characteristics that reflect the population's diversity. Among those surveyed, respondents hailed from 17 industries (**figure 2**) and all seven major global regions (**figure 3**).

FIGURE 2—INDUSTRY SECTORS

In which of the following industries are you employed?

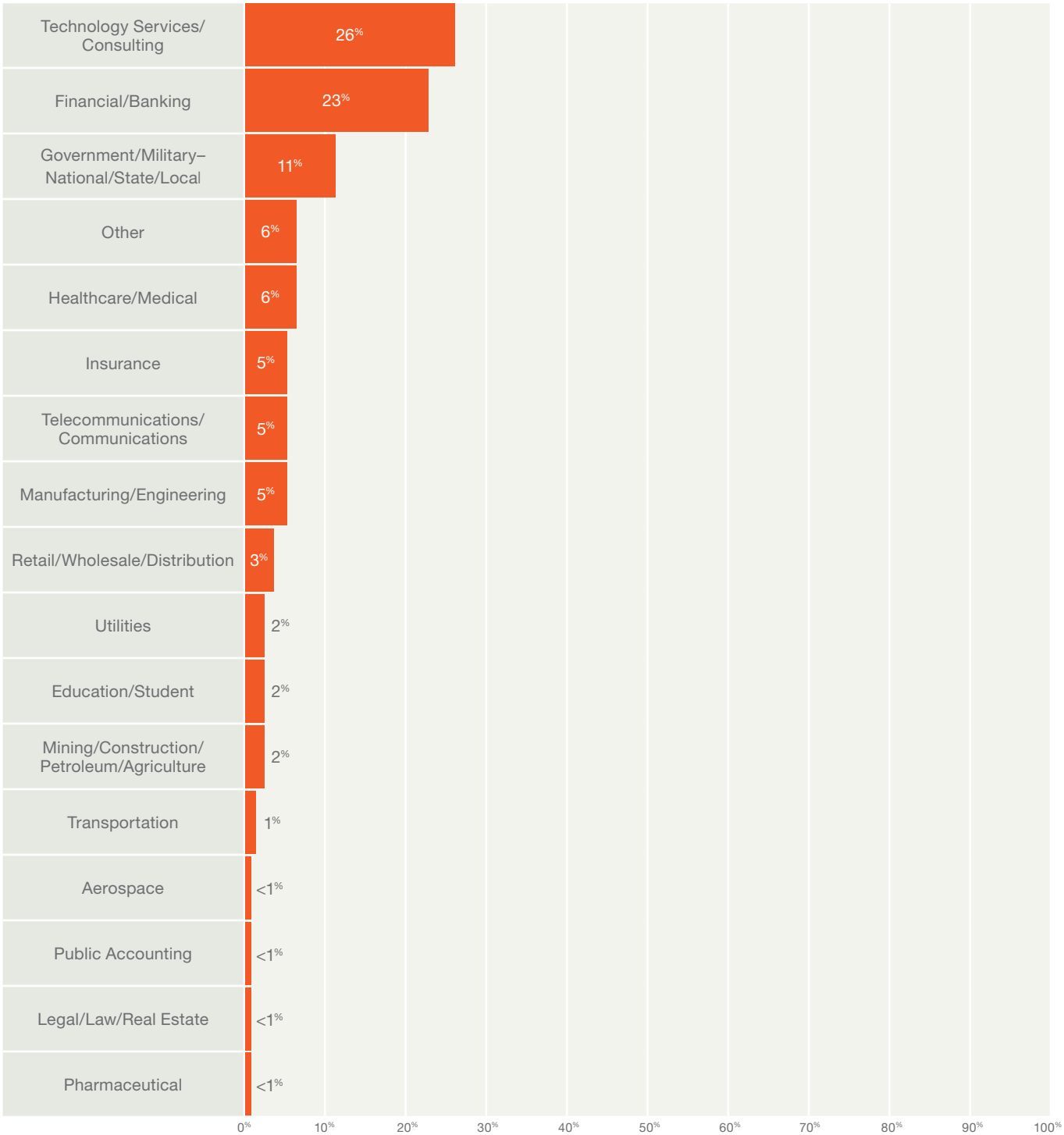
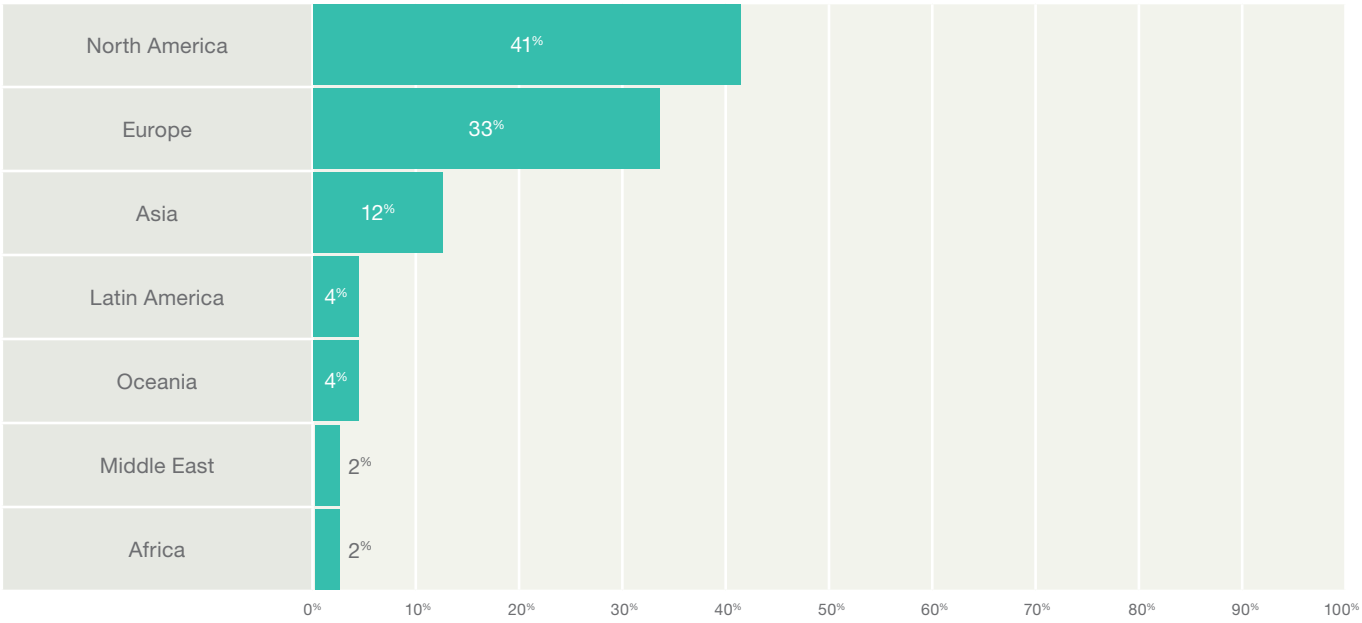


FIGURE 3—REGIONS

In which region do you reside?



Skills Challenges Remain but Are Better Understood

The first trend identified in this year's survey results reflects the difficulty that enterprises continue to experience in recruiting qualified personnel to fill security positions. The security skills gap has been noted before (in this study and others). ISACA survey results show no signs that this trend is decelerating at anywhere near a rapid rate. Fifty-nine percent of enterprises report that they have open (unfilled) security positions (**figure 4**), and more than half (54 percent) report that it takes, on average, three months or longer to fill open positions (**figure 5**).

These results indicate that staffing and skill challenges continue despite efforts by individual enterprises (and the industry more broadly) to cultivate and develop a robust skill base. The astute observer may note that the responses to these questions are similar—but not identical—to those collected in prior surveys. Last year[2] the ISACA survey found that 62 percent of respondents reported the process taking at least three months to fill open positions.

One of the primary challenges associated with building a strong security team is finding the right skills. The ratio of qualified applicants to open positions leaves much to be desired from the point of view of an enterprise trying to recruit the right security team members. Specifically, 30 percent of those surveyed report that fewer than 25 percent of applicants are qualified; 31 percent report that between 25 to 50 percent of applicants are sufficiently qualified for the positions that the enterprise hopes to fill (**figure 6**).

Although the data continue to reflect a clear and demonstrable shortage of skilled personnel (in terms of bringing the right skills in house to staff security efforts), the 2018 data also suggest improvement over prior years, at least relative to the qualifications of candidates. In the ISACA 2017 report, for example, 37 percent of respondents indicated that fewer than 25 percent of applicants were qualified, with 27 percent saying that between 25 to 50 percent of applicants were sufficiently qualified. Relative to

2 ISACA, *State of Cyber Security 2017*, February 2017, *https://cybersecurity.isaca.org/csx-resources/state-of-cyber-security-2017*

last year's survey, this year's data indicate that those in the job market are potentially more qualified.

This could reflect one of two possibilities: either changes in the applicants (i.e., a more qualified professional workforce, reflecting development and expansion of skills that job seekers bring to the table) or changes in expectations about how those resources will be employed (i.e., how enterprises will utilize their skills once hired). For example, many enterprises have introduced automation as a strategy to offset shortages of technical skills in the job market; to the extent that enterprises are able to automate (or outsource) tasks requiring specialized technical skills, one would expect a corresponding decrease in the skills required among job candidates. It is not clear from the data which of these trends is responsible for the shift, but the most likely scenario reflects both advancement in the skill base of job seekers—as the professional space becomes more mature and educational/skill-building opportunities become more prevalent—and the development of enterprise mitigation strategies that presuppose (and attempt to offset) a continued lack of a robust skill base.

FIGURE 4—ORGANIZATIONS REPORTING UNFILLED CYBERSECURITY/INFORMATION SECURITY POSITIONS

Does your organization have unfilled (open) cybersecurity/information security positions?

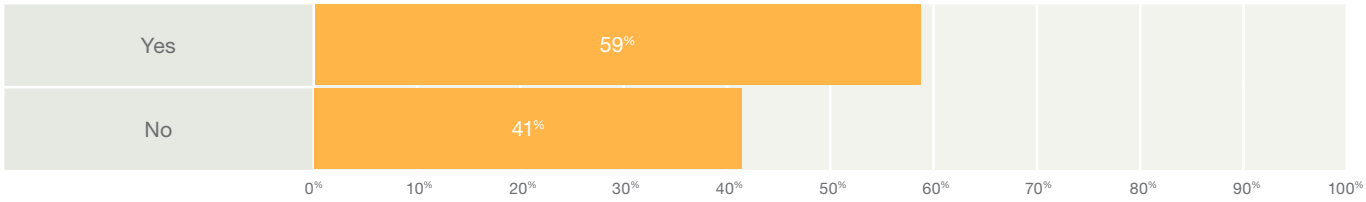


FIGURE 5—TIME TO FILL A CYBERSECURITY/INFORMATION SECURITY POSITION

On average, how long does it take your organization to fill a cybersecurity/information security position?

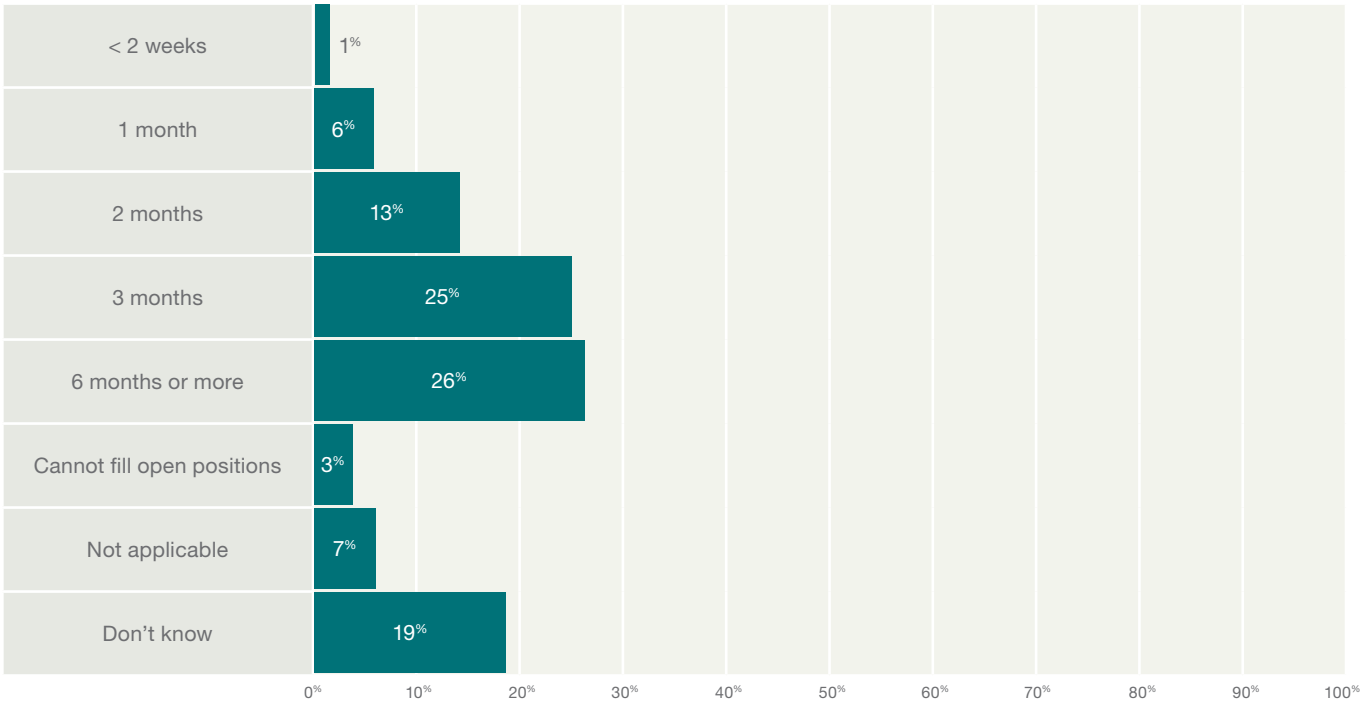
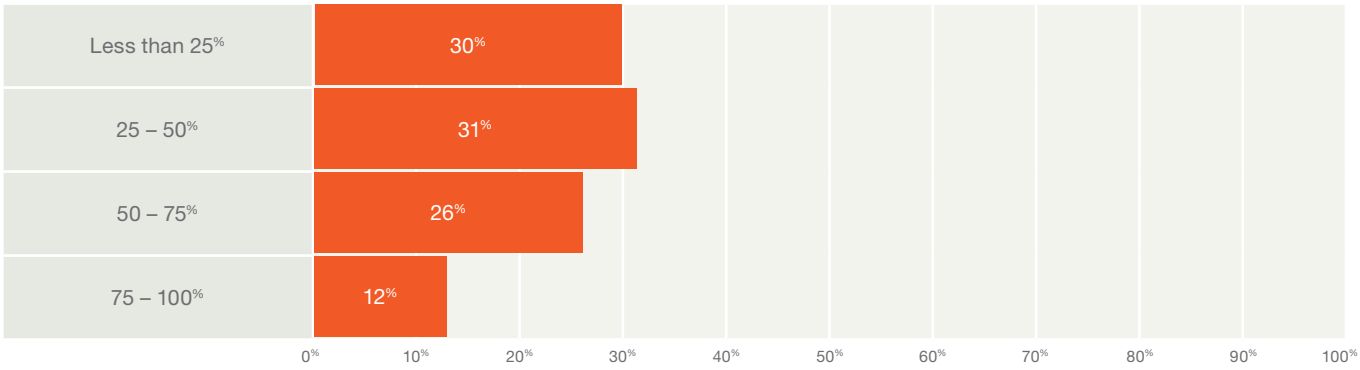


FIGURE 6—PERCENTAGE OF SECURITY APPLICANTS WHO ARE WELL QUALIFIED

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



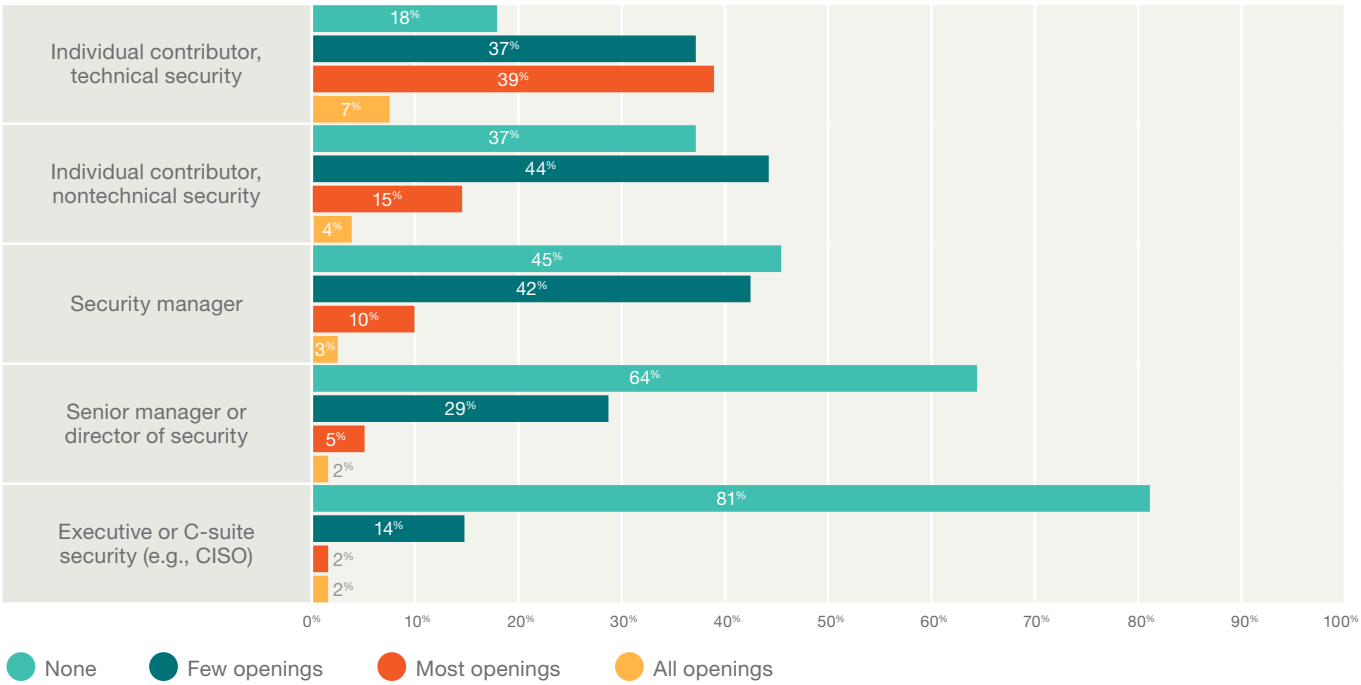
Contours of the Skills Gap

Based on previous survey data, knowledge of the skills gap has existed for years. However, to better understand the contours of the gap (i.e., its specific characteristics) and extrapolate the long-term impact to the job market and profession, new questions are included in this year's ISACA survey. These new questions are designed to reveal where in the enterprise open positions are located, the skill levels that are in the greatest demand and where (in terms of required skills) future growth is likely to be.

Results clearly show that the most unfilled (open) security positions fall organizationally at the level of individual-contributor technical staff members. There is some—though not as much—demand for nontechnical individual contributors and management-level personnel. Comparatively few openings occur at the senior manager/director level or at the executive level (**figure 7**).

FIGURE 7—PERCENTAGES OF UNFILLED SECURITY POSITIONS AT GIVEN ORGANIZATIONAL LEVELS

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



The level at which most security positions remain unfilled (i.e., the single- or individual-contributor level) is perhaps not surprising given the historical demand for technical skills and the tendency of technical resources to be less managerially inclined. However, the disparity in demand for technical individual contributors relative to managers is noteworthy and striking.

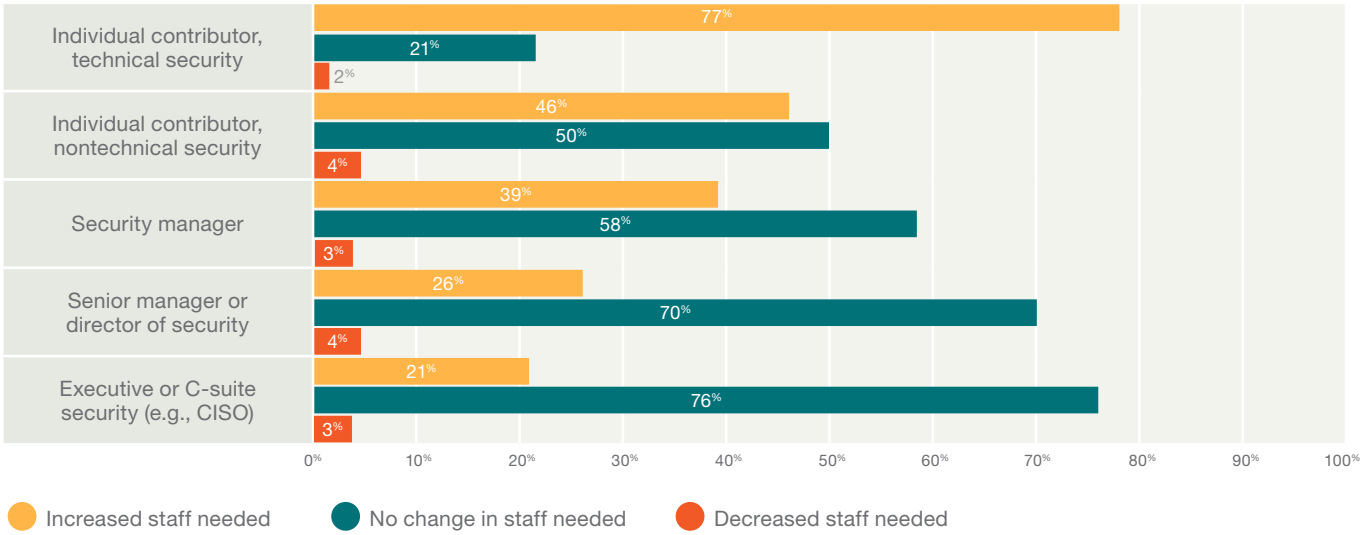
The implication for those in the job market—i.e., those practitioners seeking to maximize their competitiveness as job candidates—is obvious. Maximizing technical skills is likely to have the greatest return in the short term. The implication for enterprises is perhaps more useful. To the extent that enterprises can optimize hiring processes and vet technical applicants more easily, the enterprises can realize a potential advantage relative to peers in filling positions. Likewise, automation as a strategy continues to have advantages, particularly when it reduces demand for technical resources.

This trend is likely to continue. Survey responses indicate that anticipated growth in demand is commensurate with current demand (**figure 8**). Seventy-seven percent of respondents see a need for increased demand among technical, individual-contributor staff members, with a correspondingly smaller need for increased staff at other levels: executive (21 percent reporting need for increase at this level), senior manager/director (26 percent) and manager (39 percent). Those in nonmanagerial positions (i.e., individual contributors) clearly indicate demand for technical practitioners in other than management roles. Seventy-seven percent of respondents indicate the greatest need for technical staff, yet only 46 percent see a need to increase nontechnical staff. By a wide margin, the skill areas most sought after—and those that are the most difficult to find and retain—are technical security skills.

Although it is not entirely clear from the data, it appears that the most demand is disproportionally at the lower end of the experience spectrum. Over the very long term (a decade or longer), it is possible—although by no means certain—that this lower-end demand will ultimately lead to increased competitiveness for positions, as those who are entering the field now seek to move upward later. This increased competitiveness for positions, in turn, may lead to downward pressure on salaries, given disparities between demand at differing experience levels and increasingly constricted upward mobility for practitioners who are entering the workforce. If trends in automation continue, that downward salary pressure may expand to include less-experienced practitioners, as automation of technical tasks displaces demand for technical resources.

FIGURE 8—HIRING DEMAND PER ORGANIZATIONAL LEVEL

In 2018, for which of these levels do you see the hiring demand increasing, decreasing or remaining the same?



Implications for Enterprises

As a practical matter, these findings, taken together, have several implications for security managers who are looking to build out the skill base in their enterprises. A persistent skills gap increases the importance of talent retention and development of existing personnel. Relative to other disciplines, attrition may affect security organizations disproportionately, and exacerbate the already considerable impact of scarce technical skills. Investments in developing existing security personnel, e.g., through education or skill building, are likely to play a more critical role—and may have a higher return—as enterprises seek to maximize productivity and effectiveness of existing security staff. Because most of the skill shortage is observed to be in technical roles, skill building in technical areas is a clear win for practitioners and for enterprises. Development of or investment in security automation tools can also be particularly valuable whenever they facilitate or optimize efficient execution of technical tasks. Improvements in hiring—particularly in vetting technical skill and ability of candidates—can prove cost effective and also increase enterprise competitiveness.

Key enterprise takeaways:

- **Value can be derived from automation in technical areas, to the extent that automation of technical security tasks is practicable.**
- **The impact of security resource losses can have disproportionate effects on the enterprise due to the security field skills shortage.**
- **The increasing need for skilled security personnel validates investment in existing staff, including education, training, skill development and certification, particularly in technically relevant areas.**

Gender Disparity Is Present But Can Be Mitigated

To many practitioners in the security field, it can often seem that there is a preponderance of men compared to women. Prior surveys of security practitioners confirm that this disparity is actual rather than merely perceived. For example, the recent Frost & Sullivan survey, commissioned by (ISC)²® and the Executive Women's Forum (EWF), found that women comprise only 11 percent of the global security workforce.[3]

Considering this known disparity, it is not surprising that ISACA survey respondents report a gap between career-advancement opportunities for men and women. Although the majority of respondents (77 percent) indicate that women are offered the same opportunities for career advancement in the cybersecurity field as men (**figure 9**), a much more nuanced story emerges when considering the breakdown of respondents by gender.

Among responses to the question in **figure 9**, a 31-point gap exists between men and women who answered affirmatively. Men, overall, report parity in advancement opportunities—82 percent of men responded 'yes,' indicating the belief that women have the same advancement opportunities as men. Only 51 percent of women report the same perception of parity. Although a slight majority of women (by one percentage point) believe that advancement opportunities are equal, this difference in perception between men and women should not be discounted, given the striking difference in overall perception between genders (**figure 10**).

FIGURE 9—GENDER DISPARITY

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

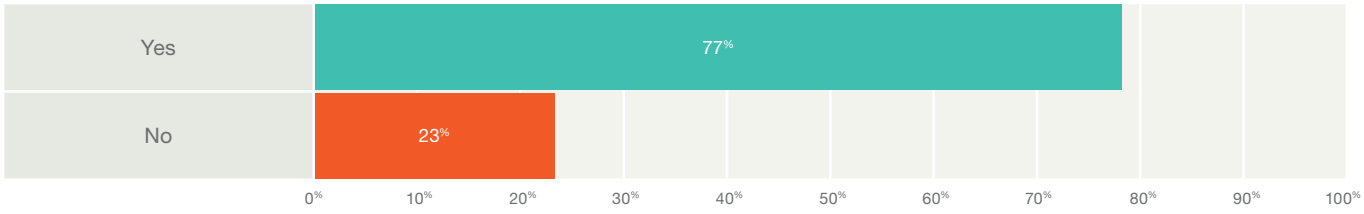
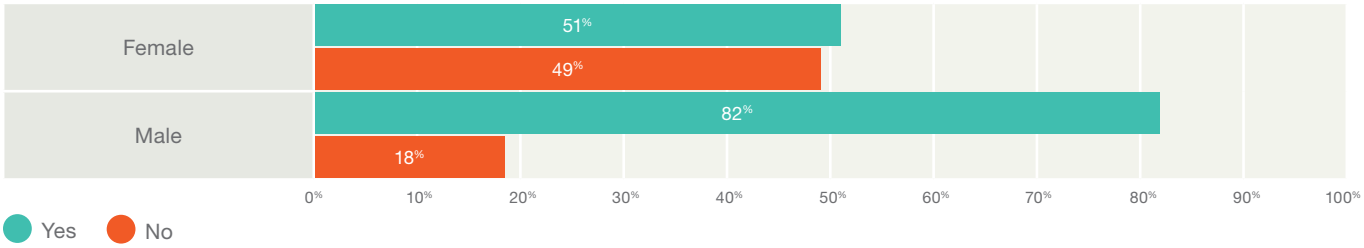


FIGURE 10—BREAKDOWN OF GENDER DISPARITY RESPONSES

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



3 Reed, Jason; Yiru Zhong; Lynn Terwoerds; Joyce Brocaglia; "The 2017 Global Information Security Workforce Study: Women in Cybersecurity," Frost & Sullivan, 2017, USA, *https://iamcybersafe.org/wp-content/uploads/2017/03/WomensReport.pdf*

Mitigation Factors

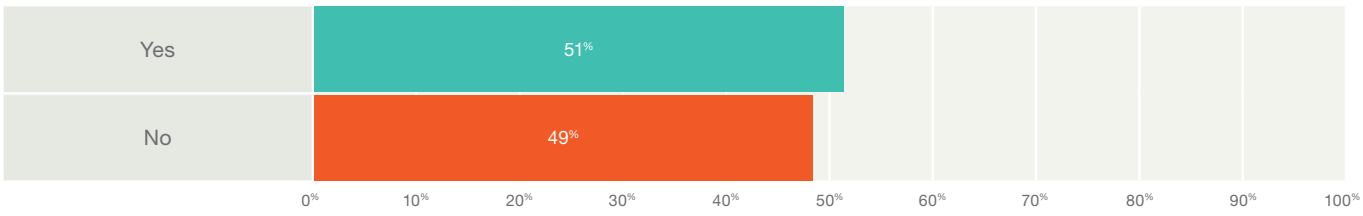
To mitigate disparity in career opportunities between men and women, enterprises may consider implementing diversity programs that specifically support gender equality. Among the enterprises that responded to the ISACA survey, about half (51 percent) have diversity programs in place to support women cybersecurity professionals (**figure 11**). This is the first year that ISACA asked about diversity programs, so the data do not yet indicate trends or offer historical perspective. These diversity programs may contribute to the results of survey questions that target gender diversity.

Among respondents in enterprises with a diversity program, 87 percent of men and 77 percent of women believe that women are offered the same opportunities for career advancement as men are offered; these numbers reflect a 10-point gap, in contrast to the 31-point gap noted above for all enterprises. Among respondents in enterprises without such programs, the gap increases: 73 percent of men and only 36 percent of women indicate that women are offered the same opportunities as men (a 37-point gap). Therefore, enterprises with diversity programs appear to be more successful in addressing gender bias and clearly achieve more favorable perceptions of equality in career advancement opportunities.

These results suggest that a diversity program, as a strategy, can partially offset gender disparity, although not fully remove it. It is important to note that it is unclear from the data whether diversity programs *actually* help balance opportunities for advancement between men and women or merely affect *perceptions* of such opportunities and their relative accessibility. Further study of the impact of diversity programs is required to establish their practical efficacy.

FIGURE 11—DIVERSITY PROGRAMS

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



Implications for Enterprises

Considering the skills gap, recruiting new security talent and retaining and developing talent already in-house are important considerations for enterprises. Given the strong correlation between diversity programs and the perception of career advancement for women, diversity programs can be a successful part of any strategy to maximize existing resources, optimize efficient use of existing staff and decrease the rate of staff leaving, in so far as gender inequality seems to translate directly into loss of talented female staff. A diversity program is not just good optics: It can have positive PR benefit externally and improve internal perception among staff.

Key enterprise takeaways:

- **Diversity programs can help offset skills shortages, optimize resource placement and lower potential for staff leaving the security organization.**
- **Rather than being merely a nice-to-have program, a diversity program can support competitive advantage; enterprises with such programs in place can realize advantages that others will forego in their absence.**

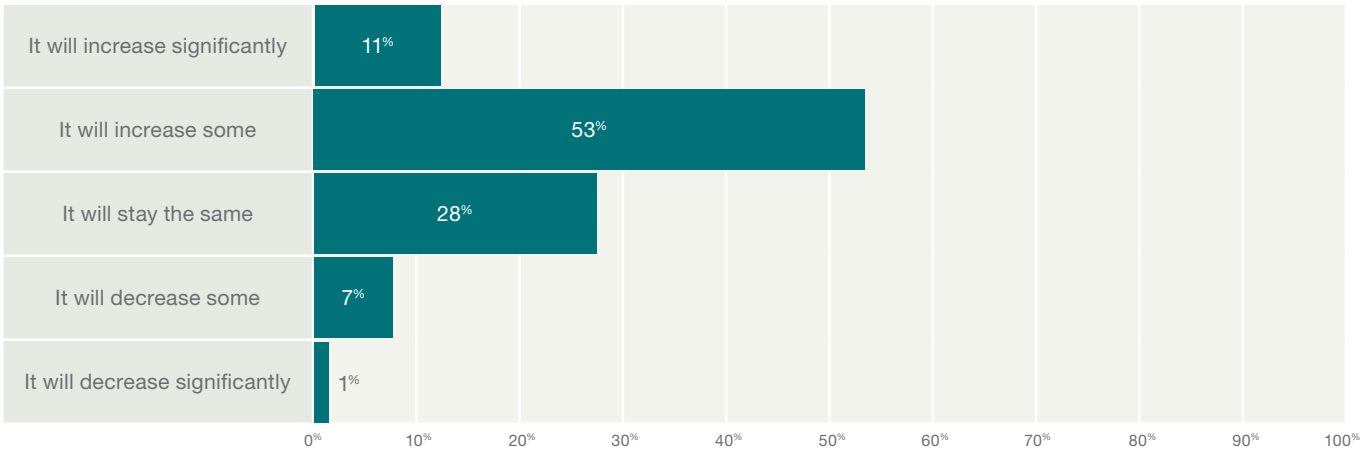
Budgets Are Increasing Once Again

Last year's ISACA report found that, although security budgets on the whole were increasing, their rate of expansion had slowed from prior years. This year, the ISACA *State of Cybersecurity Survey* results show that not only has the rate of budget expansion returned to its 2015 measure, but it has surpassed it. Specifically, 64 percent of respondents in this year's survey indicate that budgets will increase; for 11 percent of respondents, it will increase significantly, and for 53 percent of respondents, it will increase some (**figure 12**).

Last year, only 50 percent of those surveyed expected an increase in budget, down from 61 percent the prior year (2015). This year's measurement (64 percent) suggests that last year's slowdown was not only temporary, but that a rapid upswing in spending levels may be at work.

FIGURE 12—CHANGE IN ENTERPRISE SECURITY BUDGETS

How, if any, will your enterprise's security budget change in 2018?



This budgetary expansion aligns with expectations, given the growing rate of security attacks year over year. Fifty percent of responding enterprises experienced an increase in the number of attacks relative to a year ago; 25 percent reported the same number of attacks (**figure 13**). Likewise, those surveyed expect the trend of increasing attacks to continue into next year. Eighty percent of respondents indicate that it is either likely (38 percent) or very likely (42 percent) that they will experience a cyberattack in 2018 (**figure 14**). The overall percentage of respondents finding it likely vis similar to last year's data; however, this year a higher percentage of respondents found it very likely instead of likely (42 percent this year compared to 38 percent last year).

Data associated with threats, countermeasures, attacks and incidents are more fully explored in the other parts of the *State of Cybersecurity 2018* report.

FIGURE 13—NUMBER OF SECURITY ATTACKS YEAR OVER YEAR

Is your enterprise experiencing an increase or decrease in security attacks as compared to a year ago?

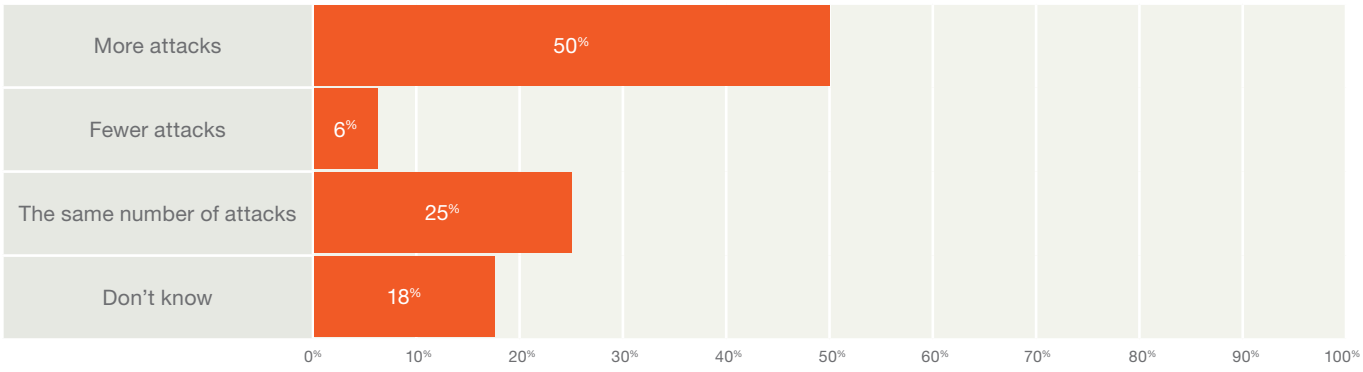
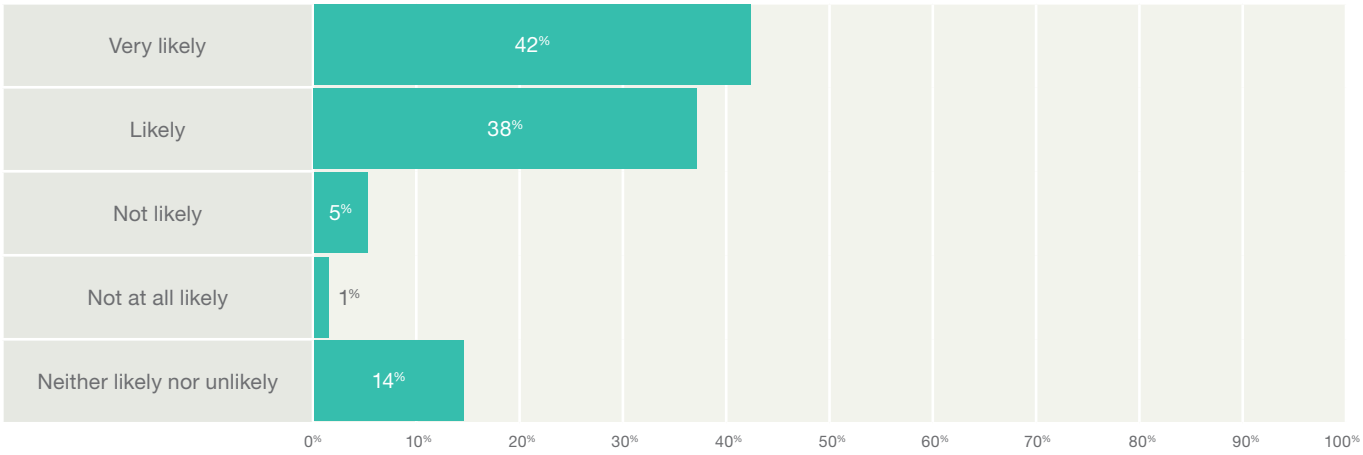


FIGURE 14—LIKELIHOOD OF CYBERATTACK

How likely do you think it is that your enterprise will experience a cyberattack in 2018?



Implications for Enterprises

The potential for an increase in enterprise security budgets will be welcome news for many practitioners. Not only does it bring opportunities to acquire necessary tools, but also boosts resources for talent acquisition, training and skill building. Last year's report noted with some concern that a drop-off in the rate of budget expansion exacerbates skill-related challenges: It becomes more difficult to compete effectively in the job market for talented resources, and it limits opportunities to invest in automation that could otherwise help offset challenges in acquiring skilled employees.

Because this year's survey shows that the trend has not continued year over year, these concerns proved to be unfounded. However, last year's decline in budget growth does highlight the fact that expanding security budgets are not inevitable or irreversible year over year. For enterprises seeking to make the best use of resources, investments made now in the security program (while resources are available) may prove wise considering the uncertainty ahead.

Key enterprise takeaway:

- **Investments made in the security program while resources are available can have long-term advantages and potentially help to mitigate constraints or reductions that may occur in the future.**

Confidence in Preparedness Is Increasing, but Organizational Alignment Is Inconsistent

Practitioners are slightly more confident about executive and board support of security efforts compared to last year. Sixty-nine percent of practitioners believe that the board of directors has adequately prioritized information security (**figure 15**). This percentage is up slightly from last year, when 67 percent of respondents believed that the board adequately prioritized enterprise security (**figure 16**).

FIGURE 15—PRIORITIZATION OF SECURITY BY BOARD OF DIRECTORS

Do you believe that your board of directors has adequately prioritized enterprise security?

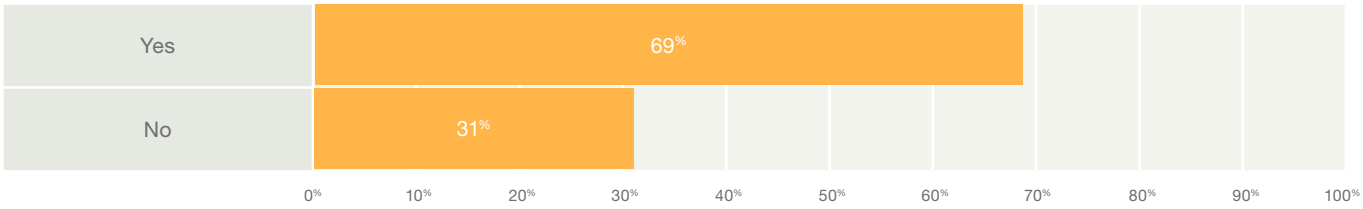
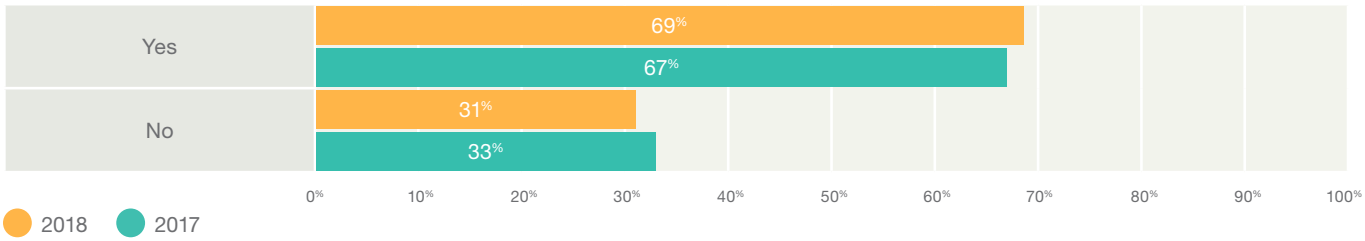


FIGURE 16—BOARD PRIORITIZATION: YEAR-OVER-YEAR COMPARISON

Do you believe that your board of directors has adequately prioritized enterprise security?



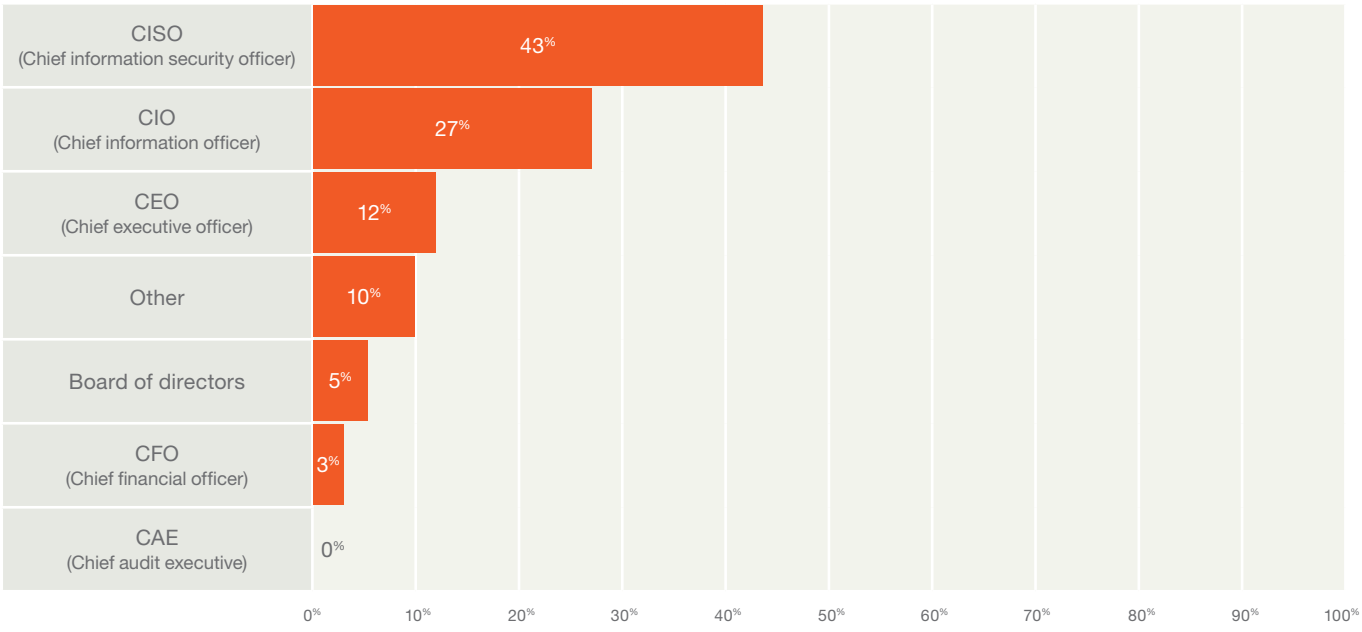
Organizational Placement

There is a striking lack of consensus among respondents to the question about reporting structure for security organizations. Forty-three percent of respondents indicate that their security function reports into a C-level security-specific position (i.e., a chief information security officer [CISO]). Twenty-seven percent indicate that the function reports to the chief information officer (CIO). The remaining 30 percent are split among other areas, including chief executive officer (CEO), board, chief financial officer (CFO), etc. (**figure 17**).

Seventeen percent of respondents indicate that the security function reports either to the CEO or to the board directly. Given the form of this question (which was modified this year to reflect updated professional practices and industry developments), it is difficult to compare this distribution directly with prior-year data for every reporting location. However, it can be observed that the percentage reporting to the board or CEO is down slightly this year relative to last year (when 24 percent indicated that security reported either to the CEO or board directly).

FIGURE 17—REPORTING STRUCTURE FOR SECURITY FUNCTION

To whom does security report in your enterprise?



Implications for Enterprises

Lack of consensus on organizational structure can represent potential risk—particularly when security teams have limited ability to communicate concerns upward about the prioritization process and overall strategy. Relative to board members, security practitioners are often more attuned to the threat environment and the enterprise's operational/technical ecosystem. Although practitioners are well positioned to observe potential security issues, if the enterprise has no reliable feedback mechanism to communicate issues upward, risk can result from incorrect or inappropriate prioritization at higher levels.

Conversely, the board has priorities that may not be fully visible to security team members. It would not make sense, for example, to bootstrap strategic security projects, establish new security priorities or channel effort and energy into security if the enterprise is drowning in debt, its competitiveness erodes quarter after quarter or it faces a crippling judgment in a class action lawsuit.

In any case, one strategy to help mitigate these concerns is to implement more objective, consistent and actionable reporting to the board about security concerns. To the extent that the enterprise can measure and track risk systematically and holistically—and respond appropriately—a summary snapshot of security risk (at an appropriate level of abstraction for board consumption) might help in part to mitigate this issue. From the board's point of view, it can help to receive information about security that might be unavailable otherwise. From the security team's point of view, it builds confidence to know that the board has heard and considered its viewpoint while assigning enterprise priorities.

Key enterprise takeaways:

- **A systematic and holistic risk program is not only valuable for security and risk efforts, but also provides a vehicle to communicate priorities upward to executive management and the board. Even in situations where an enterprise already has an enterprise risk management (ERM) or operational risk group, integrating cybersecurity into risk planning can be advantageous.**
- **Methods to articulate security concerns and communicate them upward more effectively can help alleviate perceived (or actual) issues in the board's prioritization of security efforts.**

Conclusion

Like previous ISACA cybersecurity surveys have noted, good help is hard to find. This is truer now than ever before in the security discipline. The new ISACA *State of Cybersecurity Survey* results not only show an expansion of the skills gap reported in the past, but also begin to trace its contours. Technical resources, particularly technical individual contributors, are in the most demand. That demand is likely to increase over the short-to-medium term.

These same resources are, perhaps not surprisingly, the most challenging to find and retain. They are also the most challenging to vet appropriately. Therefore, when these resources leave, their departure has a disproportionate impact on the enterprise's ability to achieve security objectives. An enterprise's ability to optimize recruitment and retention of these resources can become a keen competitive advantage.

Programs that help to maximize existing staff, such as automation and skill building, can help to alleviate some of the pressures from this skills gap. Developing a diversity program to help address gender disparity–along with other strategies designed to minimize attrition—can also provide direct value.

The observation that budgets are increasing once again means that many enterprises–although reluctant to invest last year—may now be able to reinvest in development of security teams. If, as the data suggest, the skills gap is expanding and widening, these investments can reap large rewards as talent becomes more difficult to find and retain.

Acknowledgments

ISACA would like to recognize:

Expert Reviewers

Larry Marks
CISA, CISM, CRISC, CGEIT, CFE, CISSP, CVPM, ITIL, PMP
USA

Tara Singh
CISA, CISSP
USA

ISACA Board of Directors

Theresa Grafenstine, Chair
CISA, CRISC, CGEIT, CGAP, CGMA, CIA, CISSP, CPA
Deloitte-Arlington, VA, USA

Robert Clyde, Vice-Chair
CISM
Clyde Consulting LLC, USA

Brennan Baybeck
CISA, CRISC, CISM, CISSP
Oracle Corporation, USA

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

Peter Christiaans
CISA, CRISC, CISM, PMP
Deloitte Consulting LLP, USA

Hironori Goto
CISA, CRISC, CISM, CGEIT, ABCP
Five-I, LLC, Japan

Mike Hughes
CISA, CRISC, CGEIT
Haines Watts, UK

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

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

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

Ted Wolff
CISA
Vanguard, Inc., USA

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

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

Robert E Stroud
ISACA Board Chair, 2014-2015
CRISC, CGEIT
XebiaLabs, Inc., USA

Tony Hayes
ISACA Board Chair, 2013-2014
CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA
Queensland Government, Australia

Matt Loeb
CGEIT, FASAE, CAE
ISACA, USA

About ISACA

Nearing its 50th year, ISACA® (isaca.org) is a global association helping individuals and enterprises achieve the positive potential of technology. Technology powers today's world and ISACA equips professionals with the knowledge, credentials, education and community to advance their careers and transform their organizations. ISACA leverages the expertise of itshalf-million engaged professionals in information and cyber security, 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 217 chapters and offices in both the United States and China.

Disclaimer

ISACA has designed and created *State of Cybersecurity 2018: Workforce Development* (the "Work") primarily as an educational resource for 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, professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

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-2018

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

Twitter:
www.twitter.com/ISACANews

LinkedIn:
www.linkd.in/ISACAOfficial

Facebook:
www.facebook.com/ISACAHQ

Instagram:
www.instagram.com/isacanews/