REPORT

McAfee
Together is power.

Hacking the Skills Shortage

A study of the international shortage in cybersecurity skills

Center for Strategic and International Studies

Table of Contents

Executive Summary

Every day we read of another company being hacked. Attacks outpace defense, and one reason for this is the lack of an adequate cybersecurity workforce. The cybersecurity workforce shortfall remains a critical vulnerability for companies and nations. Conventional education and policies can't meet demand. New solutions are needed to build the cybersecurity workforce necessary in a networked world.

The deficit of cybersecurity talent is a challenge for every industry sector. The lack of trained personnel exacerbates the already difficult task of managing cybersecurity risks. Our study quantifies the global cybersecurity workforce shortage and analyzes how companies and governments should approach cybersecurity workforce development to build a robust and sustainable pipeline of skills.

The eight countries selected for this study—Australia, France, Germany, Israel, Japan, Mexico, the United Kingdom (UK), and the United States (US)—reflect a diversity of sizes, educational systems, income levels, and political structures. We looked at four dimensions of their cybersecurity workforce development efforts: total cybersecurity spending, education programs, employer dynamics, and public policies. Our findings are based on open-source data, targeted interviews with experts, and an eight-nation survey of information technology (IT) decision makers in both public and private sector organizations.

Each country has unique factors that shape their cybersecurity posture. These can be leveraged to develop a stronger cybersecurity workforce. We outline potential improvements to training and education programs to build and sustain critical skills for cybersecurity professionals. Our survey of employer dynamics highlights the critical role that employers play in recruiting, retaining, and training their workforce. Looking to future developments in cybersecurity, we examine how technological improvements can reinforce cybersecurity skills. We conclude with recommendations on how to improve these four dimensions of the cybersecurity workforce to enhance global cybersecurity.

Hacking the Skills Shortage

Key Findings

- Respondents in all countries surveyed said cybersecurity education was deficient. Eighty-two percent of respondents report a shortage of cybersecurity skills. More than three out of four (76%) respondents believe their government is not investing enough in cybersecurity talent.
- This shortage in cybersecurity skills does direct and measurable damage, according to 71% of respondents. One in three say a shortage of skills makes their organizations more desirable hacking targets. One in four say insufficient cybersecurity staff strength has damaged their organization's reputation and led directly to the loss of proprietary data through cyberattack.
- High-value skills are in critically short supply, the most scarce being intrusion detection, secure software development, and attack mitigation. These skills are in greater demand than soft skills in communication and collaboration. A majority of respondents (53%) said that the cybersecurity skills shortage is worse than talent deficits in other IT professions.
- About half the companies surveyed prefer a bachelor's degree in a relevant technical subject as the minimum credential required for entry into the field. The utility of a degree, however, is more in its market signal than its effectiveness in honing cybersecurity skills. Respondents ranked hands-on experience and professional certifications as better ways to acquire cybersecurity skills than a degree. Sixty-eight percent also said that hacking competitions (capture the flag exercises) play a role in developing critical cybersecurity skills within their organization.
- Almost nine out of 10 respondents said that cybersecurity technology could help compensate for skill shortages. More than half (55%) of respondents believe that, in five years, cybersecurity solutions will be able to meet the majority of their organization's needs. They also say they will respond to in-house talent shortages by expanding their outsourcing of cybersecurity. The solutions most likely to be outsourced are ones that lend themselves to automation and include threat detection (networking monitoring and access management).
- More than three out of four (76%) respondents said their government is not investing enough in building cybersecurity talent, and the same percentage said the laws and regulations for cybersecurity in their country are insufficient. There is a public demand for political leaders to improve cybersecurity legislation.
- Countries can change this shortfall in critical cybersecurity skills by increasing government expenditure on education, promoting gaming and technology exercises, and pushing for more cybersecurity programs in higher education.

The cybersecurity workforce shortfall remains a critical vulnerability for companies and nations.

Connect With Us

Diagnosing the Problem: The Cybersecurity Workforce Deficit

Demand for cybersecurity professionals is outpacing the supply of qualified workers in all countries surveyed. This conclusion is supported by market studies, our survey results, and the significant salary premiums commanded by cybersecurity professionals.

Estimates of the global cybersecurity workforce shortfall range from one to two million positions unfilled by 2019.[1] In 2015, about 209,000 cybersecurity jobs went unfilled in the United States alone.[2]

In our survey of information technology (IT) professionals in Australia, France, Germany Israel, Japan, Mexico, the UK, and the US, 82% of respondents agree that there is a large shortage in their own organization as well as their country as a whole.

This shortage is felt most acutely in Mexico and Australia. Eighty-eight percent of respondents in both countries believe there is a shortage of cybersecurity skills. Highly technical skills are most in demand in all eight countries surveyed. Intrusion detection, secure software development, and attack mitigation were most frequently in the top three skills in demand. These skills were in greater demand than softer skills, such as the ability to collaborate, manage a team, or communicate effectively. Fifty-three percent of respondents say that the talent shortage in cybersecurity is somewhat or far worse than in other IT professions.

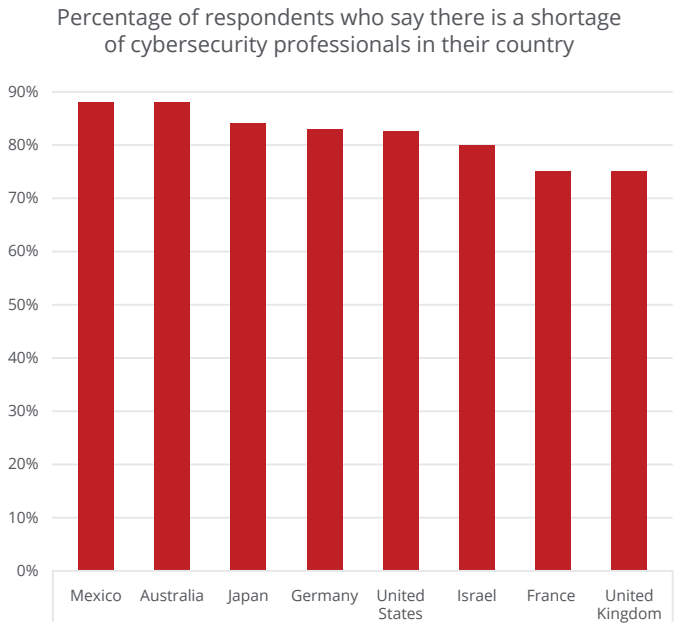

Figure 1. Cybersecurity workforce shortages by country and skillset.

Figure 2. Cybersecurity workforce shortage relative to IT workforce shortage.

The cybersecurity shortage is also observed in second-order effects, namely in higher compensation for cybersecurity positions. Scarcity drives up the value of cybersecurity personnel. The median cybersecurity salary reported in surveyed countries is at least 2.7 times the average wage, according to the OECD. Cybersecurity jobs in the United States pay an average of $6,500 more than other IT professions, a 9% premium.[3] The premium for technical skills appears to be greater than management skills. In the United States, the highest paying technical security job in is a lead software engineer at $233,333 a year; which is around $8,000 more annually than the salary of a chief information security officer (CISO), a role with greater managerial responsibilities.[4]

Figure 3. Cybersecurity salary premium (annual average salary from survey compared to OECD average annual wages).[8]

There are no signs of the cybersecurity workforce shortage abating in the near term. Respondents estimate an average of 15% of cybersecurity positions in their company could go unfilled by 2020. Those in Japan and Mexico are most concerned about not meeting future cybersecurity demand.

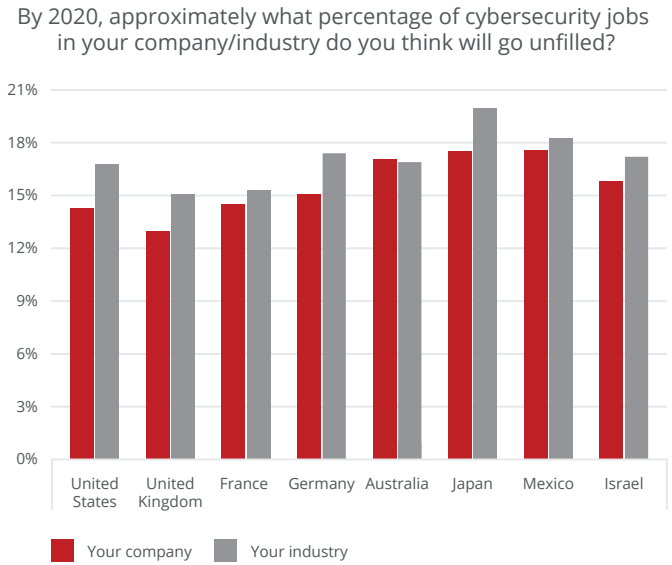

Figure 4. Future cybersecurity workforce gap.

The Changing Role of the CISO

As corporate board members worry more about cybersecurity, the role of the chief information security officer is changing. Ninety-seven percent of survey respondents say their organization's board of directors now views cybersecurity as important. The elevated importance of cybersecurity is a stark shift, as five years ago cybersecurity was not even in the top 10 risks prioritized by boards according to Lloyds' annual risk survey.[5] More than 76% say that their board considers cybersecurity skills very or extremely important. This elevated role for cybersecurity sometimes elevates the status of the CISO, who in many organizations now reports directly to the board rather than the chief information officer (CIO).[6] A study by IDC predicts that by 2018, 75% of CISOs and chief security officers (CSOs) will report directly to the CEO or board of directors.[7]

The continued skills shortage creates tangible risks to organizations, and companies say they have already incurred damages as a result of this workforce gap. Respondents say their organizations, unable to maintain adequate cybersecurity staff, have been targeted by hackers who suspect a shortage of cybersecurity skills at their organization. One in four respondents say their organizations have lost proprietary data as a result of their cybersecurity skills gap.

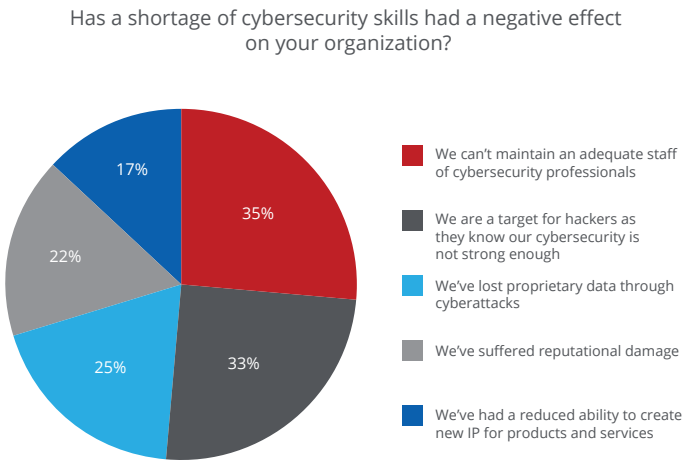

Figure 5. Impact of cybersecurity workforce shortage.

Many students in higher level technical degree programs in the United States are from outside the country. As many as 68% of US computer science students pursuing master's degrees come from outside the United States.[11] While the proportion of foreign students in higher education is largest in the US, other countries could also benefit from this pool of foreign talent through flexible immigration and visa policies.

Diversify the Cybersecurity Workforce

Expanding the cybersecurity workforce could be facilitated by pursuing opportunities to create a larger, more diverse talent pool.

In North America, a dearth of women and minorities in the cybersecurity industry mirrors trends in academia, according to a survey of academic institutions that provide degrees in computer science and engineering or information security.[9] In this study, only 2.6% of doctoral graduates of these programs in 2014 were non-Asian minorities, a decrease from 3% in 2013. Women comprise only 17 to 18% of doctoral graduates in computer science, engineering, and information security. This mirrors industry trends, as an (ISC)² study of 14,000 professionals in cybersecurity revealed only 11% were women.[10] Anecdotal evidence from our interviews suggests that while relevant technical programs are slowly adding more women, black and Hispanic students remain in short supply.

Four Dimensions of Analysis

We studied four dimensions of the problem that affect the cybersecurity workforce pipeline in Australia, France, Germany, Israel, Japan, Mexico, the UK, and the US.

Cybersecurity Spending

The size and growth of cybersecurity spending correlates with the size and growth of the cybersecurity workforce and reveals how countries or companies prioritize cybersecurity. The United States government and the financial services industry, as big cybersecurity spenders, are uniquely positioned to pioneer recruitment and development practices for others to emulate. Similarly, the US and Israel, as large exporters of cybersecurity products and services, have established

expertise and thus have a head start on improving their workforce.

Market reports estimate total annual global cybersecurity spending ranged from $75 billion to more than $100 billion in 2015 and project annual spending increases between 7.4% and 16% over the next five years.[12]

The banking industry has been particularly active in increasing cybersecurity spending, reflecting its prominence as a target—banks are three times more likely to be targeted than non-financial institutions.[13] Five banks alone spend more than $1.5 billion on cybersecurity.[14] According to Bank of America's CEO, cybersecurity is the company's only business unit with no budget limit.[15] Finance consumes more cybersecurity products and services than any other private sector industry, and thus could help drive best practices for training and hiring cybersecurity talent. Unsurprisingly, countries and industry sectors that spend more on cybersecurity are better placed to deal with the workforce problem.

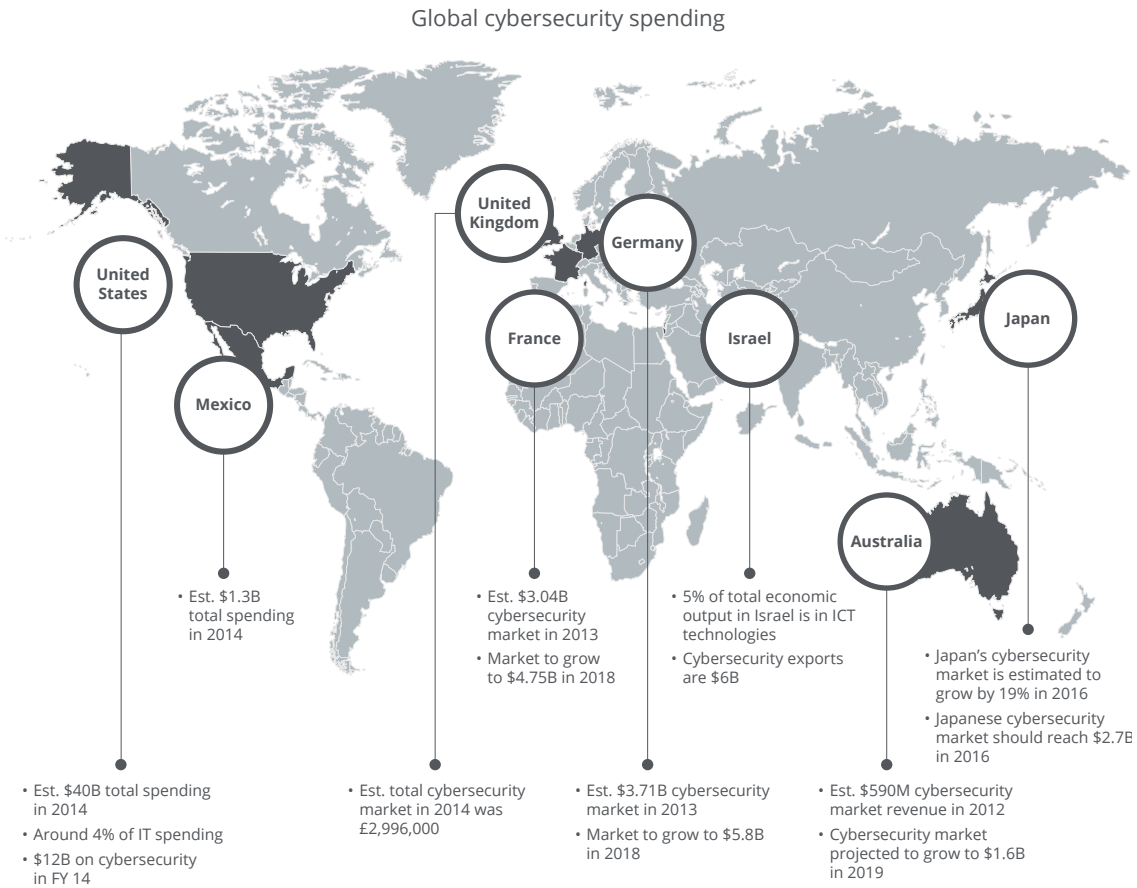

Figure 6. Global cybersecurity spending.[16]

Education and Training

Traditional academic institutions are the primary source of initial education and training for cybersecurity professionals, but non-traditional methods may be a better way to acquire and grow cybersecurity skills. Incorporating practical learning into academic programs would better prepare cybersecurity professionals for the real world.

To assess available educational capital, we created a ranking using the following metrics: overall spending on higher education, Science, Technology, Engineering and Mathematics (STEM) programs, technical cybersecurity curricula in higher education, performance in internationally recognized capture the flag exercises, and our survey data.

The US and UK rank highest in current investment in cybersecurity education and are best situated to institute educational reforms. Mexico, France, and Japan rank lowest in cybersecurity education, with low levels of government investment in education and a lack of STEM graduates. Countries with higher scores are better situated to institute reforms to improve the quality of cybersecurity education and training.

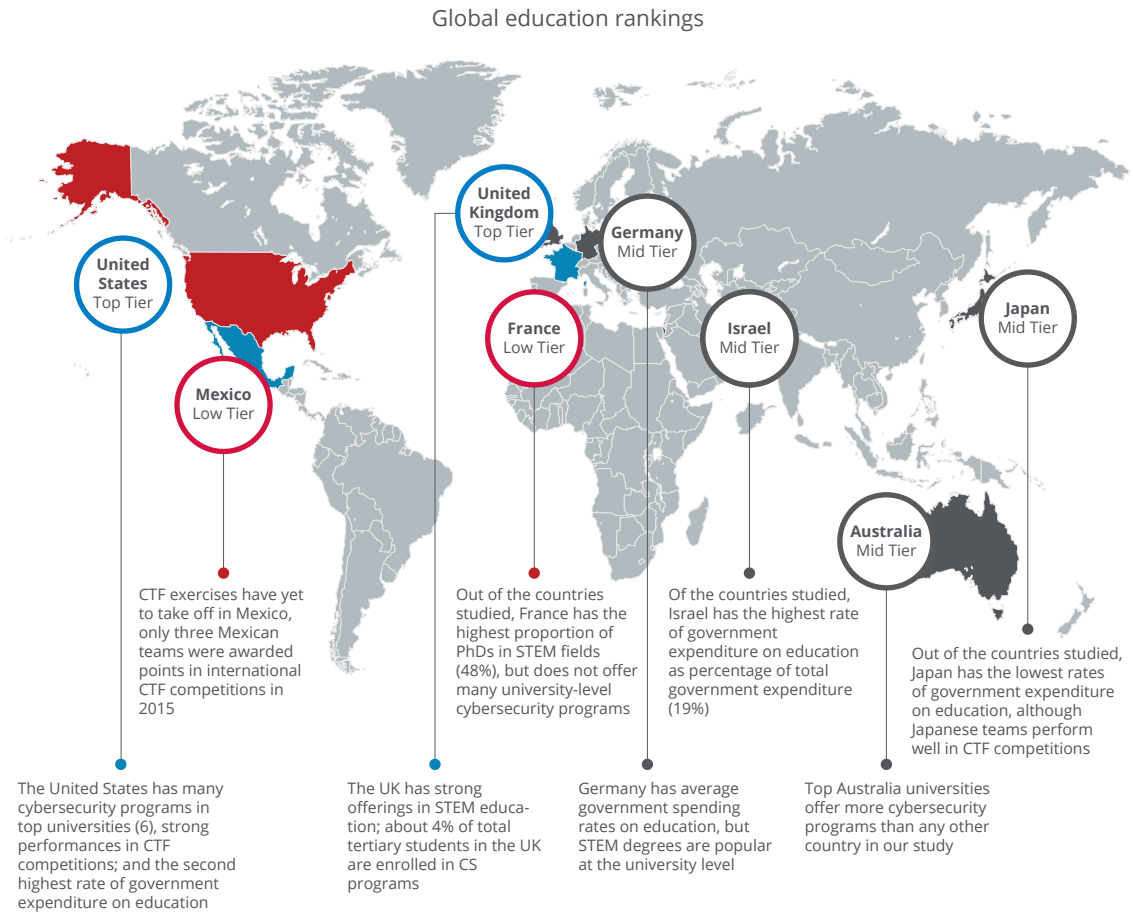

Figure 7. Education ranking by country.[17]

Around four in 10 respondents listed a bachelor's degree as the minimum credential for entry-level positions in their organizations, with significant variation among countries. Of the countries studied, France and Germany were more likely to require a master's degree; 38% and 32% of respondents, respectively, in these countries cite a master's degree as their minimum credential.

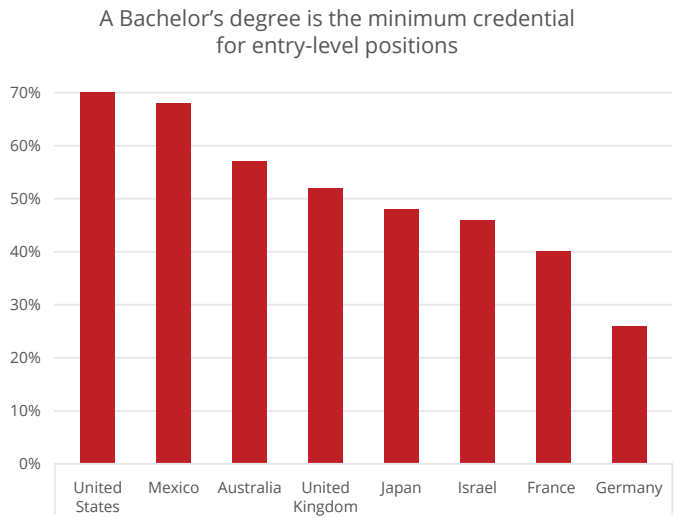

Figure 8. Minimum cybersecurity credentials.

While a bachelor's degree is typically considered necessary to enter this field, cybersecurity-specific offerings in higher education are rare. Cybersecurity as an academic discipline or program of study is often inaccessible to students. Only 7% of top universities in the countries we researched offer an undergraduate major or minors in cybersecurity. As for graduate work, about a third of top universities offer a master's degree in some cybersecurity field.[18]

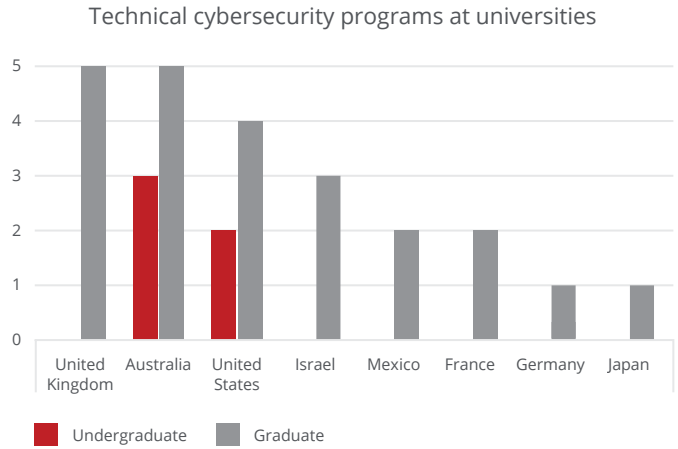

Figure 9. Cybersecurity education at top universities.

Despite our respondents' typical insistence on a bachelor's degree as a baseline credential for cybersecurity work, only 23% of respondents say education programs are preparing students to enter the industry. A bachelor's degree in a technical field is ranked third by survey respondents among most effective ways to acquire cybersecurity skills, behind hands-on experience and professional certifications. This contradiction indicates that a degree is more of a signal of general competence than an indicator of directly relevant cybersecurity skills. In the UK and Japan in particular, respondents are more likely to downgrade the value of traditional education programs for attaining cybersecurity skills. More than three-fourths of survey respondents cited professional certifications as an effective way to demonstrate skills, with respondents in the UK, Australia, Mexico, and Israel finding these credentials most useful.

How well do you think education programs (universities or vocational) are preparing cybersecurity professionals for the industry?

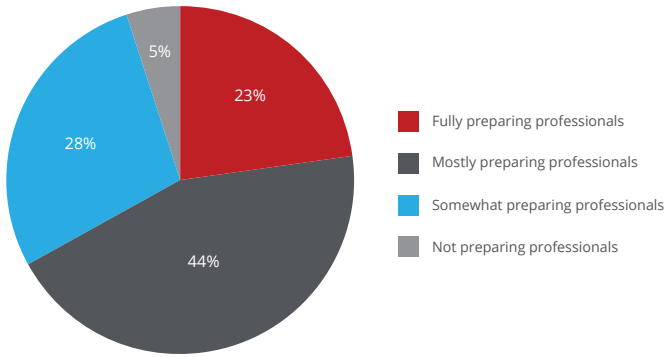

Figure 10. Education programs and skill development.

Hacking the Cybersecurity Workforce

Gaming can identify talent and cultivate cybersecurity skills. Computer games provide iterative learning examples and ways to develop skills at early levels. Some examples of cybersecurity games for younger audiences include MySecureCyberspace, a game for fourth and fifth graders by Carnegie Mellon; CyberCIEGE; and Control-Alt-Hacks.[19] The US Department of Defense is also stepping into this field and has produced CyberProtect, a game focused on resource management and countermeasure decision-making.[20] Cybersecurity storylines are increasingly a feature in more mainstream games. Popular games such as Watch Dogs, Deus Ex, Bioshock, and Fallout include some hacking element.[21] Incorporating cybersecurity plot lines and features in gaming can help more people appreciate computer networks and understand their vulnerabilities.

National hacking competitions provide an effective channel to identify talent and develop cybersecurity skills. Over three in five survey respondents say national hacking competitions play a key role in developing cybersecurity talent. Overall, two in five respondents cite hacking competitions as among the most effective way to acquire skills, with Australia and Israel most likely to agree. In Israel, 62% of respondents say that these competitions are among the top five most effective ways to acquire cybersecurity skills.

Do national hacking competitions (e.g. capture the flag competitions) help develop cybersecurity skills at your company?

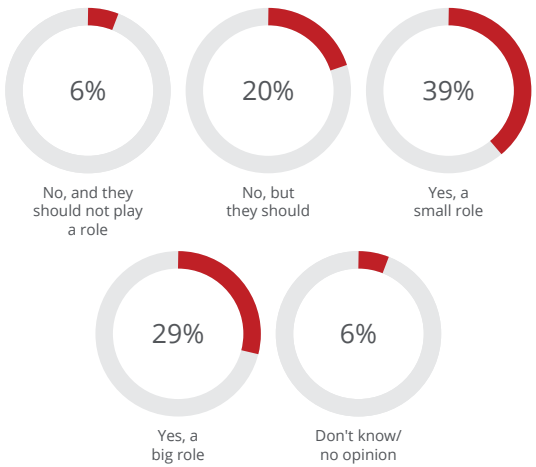

Figure 11. Role of hacking competitions.

Employer Dynamics

Employers need more effective strategies and incentives to recruit and retain top cybersecurity talent. While salary is, unsurprisingly, the number one motivating factor in recruitment, the second, third, and fourth are opportunities for training, reputation of the employer's IT department, and potential for advancement. For retention, the reputation for innovativeness of the company replaces the reputation of the IT department as the fourth most important factor.

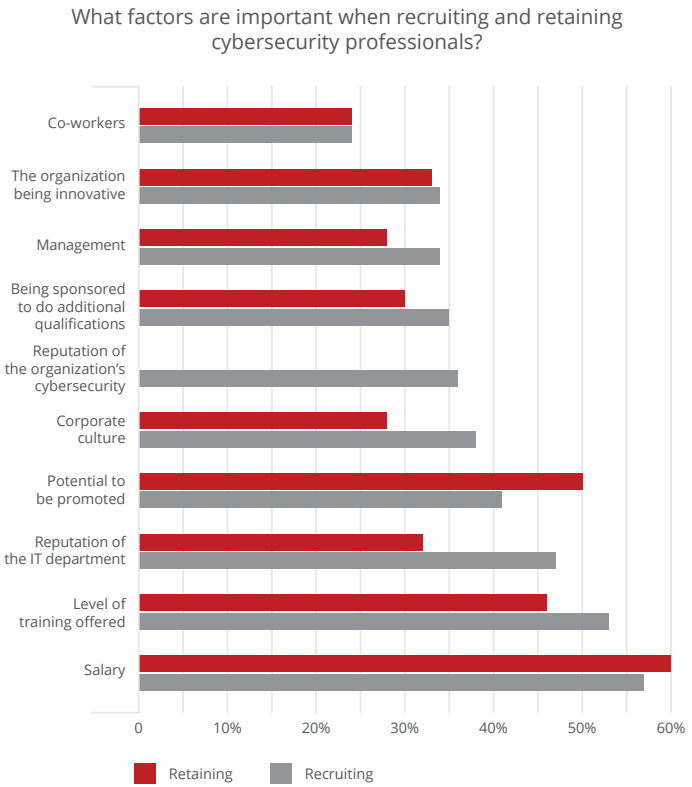

Figure 12. Recruiting and retaining cybersecurity professionals.

Companies need to be strategic in deciding what skills will be needed to combat future cybersecurity threats and how new technologies can offset workforce shortages. Recognizing that many new professionals lack necessary skills and that even proficient workers will require continuous skill development, employers are increasingly providing on-the-job training.[22] A failure to support their workforce through training can lead people to leave for another job. Almost half our survey respondents cite lack of training or sponsorship for qualifications as common reasons for talent departing their company. Some cybersecurity qualifications and certifications require training programs and tests that are often cost prohibitive for employees to fund themselves.

In addition to on-the-job training, employers are looking to invest in technology to improve cybersecurity. About nine out of 10 respondents say technological advancements in cybersecurity could compensate for a skills shortage. Given the long timeline to develop and train a robust workforce, technological improvements could help compensate for the cybersecurity skills gap in organizations.

More than 60% of survey respondents work at organizations that outsource at least some cybersecurity work. Organizations in Israel and Australia are most likely to outsource cybersecurity, while those in the US and the UK are most likely to keep these capabilities in house. The primary capabilities outsourced are risk assessment and mitigation, network monitoring and access management, and repair of compromised systems. These functions, in particular network monitoring and risk mitigation, are moving towards

automation to facilitate a faster response to malicious activities and more efficient network defense.[23]

Organizations say they will likely expand their outsourcing of cybersecurity functions. About one in five respondents believe that cybersecurity solutions will be able to meet all their organization's needs in five years. In addition to cost and efficiencies, 41% of respondents believe compatibility with pre-existing systems will be important when adopting new technologies. Additional factors that organizations use to assess the value of cybersecurity innovations include acquisition and implementation costs, management efficiency, and effectiveness at reducing cyberattacks. Efforts to enhance cybersecurity capabilities with technological solutions will require organizations to hire and train a workforce that can deploy and run these technologies efficiently.

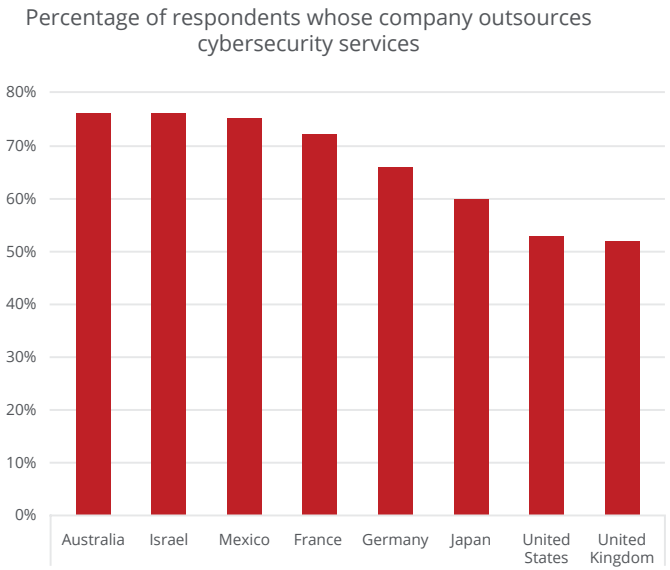

Figure 13. Outsourcing cybersecurity functions.

Imprecise job descriptions and lack of metrics to assess skills complicate the hiring process for cybersecurity jobs. There is often a mismatch between job descriptions and actual duties, which creates unhappiness in the workforce.[24] Efforts to introduce predictability and transparency in the cybersecurity job market include the NIST Cybersecurity Workforce Framework in the United States,[25] but in most countries job descriptions are not yet standardized across the public and private sectors.

Government Policies

Many countries have prioritized cybersecurity and are enacting legislation and national strategies, establishing coordinating bodies and cybersecurity agencies, and, in some cases, funding programs to cultivate a larger cybersecurity workforce. The cybersecurity talent gap has become a prominent political issue as heads of state in the US, UK, Israel, and Australia have all called for increased support for the cybersecurity workforce in the past year. Most countries we studied also have legislation specific to enhancing cybersecurity education.

Despite increased political engagement on cybersecurity workforce issues, however, more must be done to build the cybersecurity talent pool. Slightly more than three quarters of survey respondents say their governments are not investing enough in building cybersecurity talent, and the same percentage said the laws and regulations for cybersecurity in their country are insufficient.

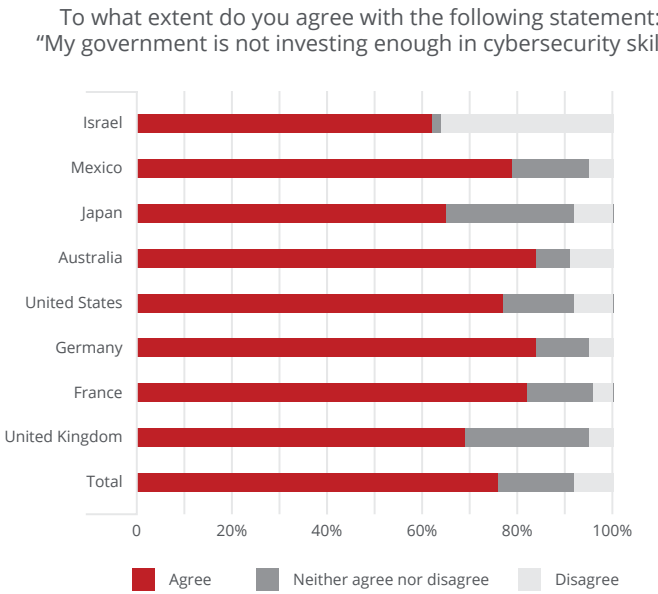

Figure 14. Government investment in cybersecurity.

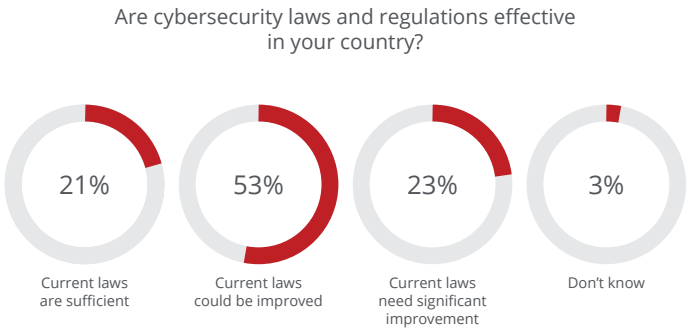

Figure 15. Cybersecurity laws and regulations.

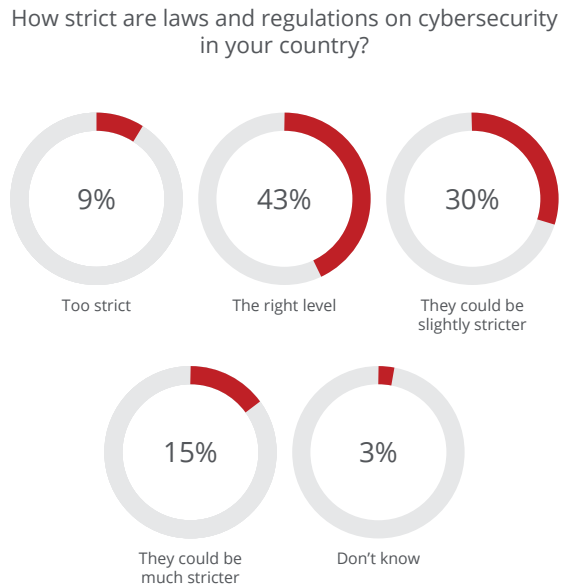

Figure 16. Cybersecurity laws and regulations.

Recommendations

Closing the gap in cybersecurity skills requires countries to develop critical technical skills, cultivate a larger and more diverse workforce, and reform education and training programs to include more hands-on learning. Our study revealed that Australia, France, Germany Israel, Japan, Mexico, UK, and the US face similar roadblocks to closing the skills gap, but each country also has distinct challenges. In light of our findings, we have the following recommendations.

Redefine Minimum Credentials for Entry-Level Cybersecurity Jobs: Accept Non-Traditional Sources of Education

Simply put, most educational institutions do not prepare students for a career in cybersecurity. Our research suggests that cybersecurity education should start at an early age, target a more diverse range of students, and provide hands-on experiences and training.

Most institutions of higher education do not offer cybersecurity concentrations and do not guide graduates to cybersecurity professions. Japan and Germany, in particular, have the fewest cybersecurity programs at the university level.

Our survey data suggests that employers should relax degree requirements for entry-level cybersecurity positions and place greater stock in professional certifications and hands-on experience for evidence of suitable skills. Universities should seek greater relevance in this field by adding cybersecurity courses and working with industry and government to tailor curriculum. Programs should focus on hands-on learning in the form of labs and classroom exercises to provide people with robust and practical skills in this field.

Early exposure to cybersecurity careers is crucial for developing interest in the field. Some countries have implemented programs targeting students at the high school level that could provide a model for others to emulate. In Israel, the Magshimim ("accomplishers") program develops cybersecurity skills and identifies talented high school students for recruitment by the Israel military.[26] Programs like these not only raise awareness of potential careers in cybersecurity, but identify promising recruits for cybersecurity professions. This is potential partnership opportunity for governments and the private sector: efforts to leverage private sector talent in training teachers, enhancing curricula, and offering internships and training opportunities to talented high school and college students would be mutually beneficial.

Diversify the Cybersecurity Field

Increasing the diversity of the cybersecurity workforce will also expand the talent pool. According to a number of studies and interviews with employers and educators, women and minorities are underrepresented in this field. Workforce enhancement efforts should aim to create a broader pool of cybersecurity talent.

Many people with advanced degrees in fields relevant to cybersecurity, including computer and information science, have international backgrounds. Rigid immigration policies shrink the pool of high-skilled workers critical to the cybersecurity workforce. The US stands to benefit the most from this recommendation,

as it has more than double the university students in STEM programs compared to any other country we studied. Many of these students are foreign nationals. The cybersecurity workforce can be rapidly expanded in the United States and other countries with similar immigration conditions by increasing the number of work visas.

According to our expert interviews, another barrier to expanding the cybersecurity workforce is a stigma that lingers with job candidates who have a history of hacking.[27] Employers should develop a more flexible attitude towards hiring people who have hacked.

Provide More Opportunities for External Training

Continued learning is vital to retaining cybersecurity talent. While employers may be wary of investing in expensive training programs that make employees more attractive in the talent marketplace, our survey shows the absence of such training is often a significant factor in people's decisions to seek alternative employment. Governments should consider creative ways to partner with the private sector to enhance training opportunities for students. Examples of such programs include private sector internships and co-ops for university students studying STEM subjects. Expanding the number of STEM scholarships should also be considered.

Evolve Skills for Automation

Employers should evolve skills in response to anticipated needs. Our survey found that organizations are looking to automate cybersecurity functions to offset the skills shortage, as cybersecurity professionals will seek to improve their security environments by incorporating automation. This means the cybersecurity workforce will have to adapt its skills to increasingly automated environments, from "human in the loop" to "human on the loop" processes, reducing the burden on existing cybersecurity staff. While automation will never fully replace human judgment, it does create efficiencies, which allow cybersecurity professionals to focus their time and talent on the more advanced threats that require human intervention.

Collect Data and Develop Better Metrics

A dearth of data hampers our ability to develop targeted cybersecurity policies and strategies and to measure effectiveness. More national data on the cybersecurity labor market and standardized job functions will help drive more tailored solutions. Industry leaders, policy makers, and educators should also work to develop a common taxonomy of skills. There should be clearly defined and commonly understood lists of high-value cybersecurity skills applicable across industry sectors.

Conclusion

A secure cybersecurity environment requires a robust workforce, yet currently there are not enough cybersecurity professionals to adequately defend computer networks. Countries and companies have to act quickly to fix this problem by facilitating the entry of more people into this profession through improvements in education, workforce diversity, training opportunities, security technology, and data collection. These concurrent efforts are vital to defeating cybersecurity threats and creating a more secure network environment.

Appendix

Which of the following skill sets are most scarce?

	Mexico	Australia	Japan	Germany	United States	Israel	France	United Kingdom
Intrusion detection	79%	87%	68%	79%	74%	70%	73%	76%
Software development	76%	81%	68%	72%	77%	56%	78%	70%
Attack mitigation	69%	76%	75%	71%	74%	80%	65%	73%
Ability to communicate effectively	53%	68%	59%	78%	70%	54%	68%	67%
Fluency in programming languages	65%	67%	60%	59%	64%	46%	67%	52%
Ability to manage a team	52%	67%	48%	63%	55%	66%	67%	53%
Ability to collaborate with other team members	59%	44%	47%	57%	56%	78%	52%	56%

Figure 17. Cybersecurity workforce shortages by country and skillset.

What cybersecurity does your organization outsource?

	Australia	Israel	Mexico	France	Germany	Japan	United States	United Kingdom
Protection of networks: Risk assessment and mitigation	68%	80%	67%	49%	65%	57%	59%	52%
Detection of threats: Network monitoring, access management	77%	88%	74%	60%	68%	72%	67%	71%
Correction of threats: Repair of compromised systems	41%	68%	44%	39%	45%	57%	40%	23%

Figure 18. Outsourcing cybersecurity functions.

1. ISACA and CSX, "Global Cybersecurity Status Report," January 2015, http://www.isaca.org/cyber/Documents/2015Global-Cybersecurity-Status-Report-Data-Sheet_mkt_Eng_0115.pdf
"Cybersecurity Market Report," Cybersecurity Ventures. December 2015. http://cybersecurityventures.com/cybersecurity-market-report/; "The 2015 (ISC)² Global Information Security Workforce Study," *Frost and Sullivan*, April 16, 2015. https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/FrostSullivan-(ISC)%C2%B2-Global-Information-Security-Workforce-Study-2015.pdf
2. Ariha Setalvad, "Demand to fill cybersecurity jobs booming," *Peninsula Press*, March 31, 2015 http://peninsulapress.com/2015/03/31/cybersecurity-jobs-growth/
3. "Information Security Analysts," *Bureau of Labor Statistics*, 2015. http://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm
4. "May 2015: Top-Paying Tech Security Jobs", *Dice*, May 2015. http://media.dice.com/report/may-2015-top-paying-tech-security-jobs/
5. "Lloyd's Risk Index 2011," https://www.lloyds.com/~/media/files/news%20and%20insight/360%20risk%20insight/lloyds_risk_index_2011.pdf
6. Kathleen Richards, "The CISO role rises: How is it working out?" *Tech Target*, October 2015. http://searchsecurity.techtarget.com/feature/The-CISO-role-rises-How-is-it-working-out
7. Steve Morgan, "Cybersecurity job market to suffer severe workforce shortage," *CSO Online*, July 28, 2015, http://www.csoonline.com/article/2953258/it-careers/cybersecurity-job-market-figures-2015-to-2019-indicate-severe-workforce-shortage.html
8. "Average Annual Wages," *OECD*, Accessed June 7, 2016. https://stats.oecd.org/Index.aspx?DataSetCode=AV_AN_WAGE
9. Stuart Zweben and Betsy Bizot, "2014 Taulbee Survey," *Computing Research News*, May 2015 http://cra.org/wp-content/uploads/2015/06/2014-Taulbee-Survey.pdf
10. "Agents of Change: Women in the Information Security Profession," *ISC and Frost and Sullivan*, 2013,² https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/Women-in-the-Information-Security-Profession-GISWS-Subreport.pdf
11. Stuart Zweben and Betsy Bizot, "2014 Taulbee Survey," *Computing Research News*, May 2015 http://cra.org/wp-content/uploads/2015/06/2014-Taulbee-Survey.pdf
12. Reports include: Kim, Elizabeth, Christian Canales, Ruggero Contu, Sid Deshpande, Lawrence Pingree. "Forecast Analysis: Information Security, Worldwide, 2Q15 Update," *Gartner*, September 8, 2015 https://www.gartner.com/doc/3126418; Morgan, Steve. "Cybersecurity Market Reaches $75 Billion In 2015; Expected To Reach $170 Billion By 2020," *Forbes*, December 20, 2015, http://www.forbes.com/sites/stevemorgan/2015/12/20/cybersecurity%E2%80%8B-%E2%80%8Bmarket-reaches-75-billion-in-2015%E2%80%8B%E2%80%8B-%E2%80%8Bexpected-to-reach-170-billion-by-2020/#630225512191; "Cyber Security Market by Solution," *Markets and Markets*, June 2015, http://www.marketsandmarkets.com/Market-Reports/cyber-security-market-505.html; "Global Cyber Security Market Forecast and Opportunities, 2020," *TechSci Research*, May 2015 http://www.techsciresearch.com/report/global-cyber-security-market-forecast-and-opportunities-2020/429.html
13. Phil Muncaster, "Finance Hit by 300 Times More Attacks Than Other Industries," *Infosec Magazine*, June 24, 2015 http://www.infosecurity-magazine.com/news/banks-hit-300-times-more-attacks/; Websense, "2015 Industry Drill-Down Report: Financial Services", http://www.websense.com/assets/reports/report-2015-industry-drill-down-finance-en.pdf
14. Steve Morgan, "Cybersecurity Market Reaches $75 Billion In 2015; Expected To Reach $170 Billion By 2020," *Forbes*, December 20, 2015. http://www.forbes.com/sites/stevemorgan/2015/12/20/cybersecurity%E2%80%8B-%E2%80%8Bmarket-reaches-75-billion-in-2015%E2%80%8B%E2%80%8B-%E2%80%8Bexpected-to-reach-170-billion-by-2020/#37a4e9802191
15. Steve Morgan, "Bank of America's Unlimited Cybersecurity Budget Sums Up Spending Plans In A War Against Hackers," *Forbes*, January 27, 2016.
16. UK Data: "Competitive analysis of the UK cyber security Sector," A study by Pierre Audoin Consultants for the Department of Business, Innovation and Skills, July 29th, 2013, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/259500/bis-13-1231-competitive-analysis-of-the-uk-cyber-security-sector.pdf; Israel: Benjamin Netanyahu, "Full Remarks at CyberTech 2016, Tel Aviv, January 27, 2016., "Central Bureau of Statistics", Accessed 3/30/2016, http://www.cbs.gov.il/reader/cw_usr_view_Folder?ID=141; Germany data: "Germany Cyber Security Market," *Micromarket Monitor*, http://www.micromarketmonitor.com/market/germany-cyber-security-3119328409.html; Mexico data: "Cybersecurity Latin America," *Cyber Security Ventures*, 2015, http://cybersecurityventures.com/cybersecurity-latin-america-q4-2015/; France data: "France Cyber Security Market," *Micromarket monitor*, http://www.micromarketmonitor.com/market/france-cyber-security-5565159549.html; Japan data: William Roth, "Japan's Cybersecurity Market: Opportunities and Challenges," *Sasakawa USA*, February 12, 2016 http://spfusa.org/research/japans-cybersecurity-market-opportunities-and-challenges/ Australia data: "Cybersecurity Asia-Pacific," *Cybersecurity Ventures*, 2015, http://cybersecurityventures.com/cybersecurity-asia-pacific-q4-2015/v US data: Bureau of Labor Statistics, http://www.bls.gov/, Bureau of Economic Analysis, http://bea.gov, "Managing cyber risks in an interconnected world," PwC, September 30, 2014 http://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf, "Federal Information Security: Agencies Need to Correct Weaknesses and Fully Implement Security Programs," GAO, Report -15-714, September 2015, http://www.gao.gov/assets/680/672801.pdf.
17. World Bank Development Indicators, 2011, http://stats.oecd.org; Capture the Flag Exercises—Top 20 teams over time, https://ctftime.org/v, OECD Education and Training Data/Graduates by field—2013.
18. We researched cybersecurity programs in the top in the eight countries we studied using the QS rankings of top global universities ("QS Stars: Methodology," http://www.topuniversities.com/qs-stars/qs-stars-methodology). For every country, we took the top 10 schools as ranked in

About CSIS

For 50 years, the Center for Strategic and International Studies (CSIS) has developed practical solutions to the world's greatest challenges. As we celebrate this milestone, CSIS scholars continue to provide strategic insights and bipartisan policy solutions to help decision makers chart a course toward a better world.

CSIS is a bipartisan, nonprofit organization headquartered in Washington, DC. Its 220 full-time staff and large network of affiliated scholars conduct research and analysis and develop policy initiatives that look to the future and anticipate change.

http://csis.org/

by these metrics and researched their cybersecurity program offerings and courses in cybersecurity. The results of this research are found in Figure 9. Other studies on the topic of cybersecurity programs in higher education yield similar results (e.g. "U.S. Universities Get "F" For Cybersecurity Education," *Cloud Passage*, April 7, 2016 https://blog.cloudpassage.com/2016/04/07/universities-fail-cybersecurity-education/).

19. Herr, Christopher, and Dennis Allen. "Video Games as a Training Tool to Prepare the Next Generation of Cyber Warrior," *Software Engineering Institute*, July 2015. https://resources.sei.cmu.edu/asset_files/Presentation/2015_017_001_442344.pdf
20. Ibid.
21. Drew Spaniel, "Hacking the Gaming Experience: The (Non-Virtual) Reality of Cybersecurity Video Gamification," *Education Review*, October 27, 2015, http://er.educause.edu/blogs/2015/10/hacking-the-gaming-experience
22. Interview with Rodney Peterson (Director, NICE, NIST), interview with Katrina Timlin on March 17, 2016.
23. Terrence Cosgrove, Colin Fletcher, Robert Naegle, "Cool Vendors in IT Automation, 2016," *Gartner*, May 2, 2016, https://www.gartner.com/doc/reprints?id=1-353BGRZ&ct=160504&st=sb; "4 Top Trends in IT Automation for 2016, December 1, 2015, http://info.advsyscon.com/it-automation-blog/4-top-trends-in-it-automation-for-2016
24. Simone Petrella (Chief Cyberstrategy Officer, CyberVista), interview by Katrina Timlin, March 10, 2016.
25. "National Cybersecurity Workforce Framework," National Initiative for Cybersecurity Education (NICE), November 2015, http://csrc.nist.gov/nice/framework/
26. John Reed, "Unit 8200: Israel's cyber spy agency," *Financial Times*, July 10, 2015 http://www.ft.com/cms/s/2/69f150da-25b8-11e5-bd83-71cb60e8f08c.html.
27. David Brumley (Director, CyLab), interview by Katrina Timlin, March 30, 2016.

About McAfee

McAfee is one of the world's leading independent cybersecurity companies. Inspired by the power of working together, McAfee creates business and consumer solutions that make the world a safer place. By building solutions that work with other companies' products, McAfee helps businesses orchestrate cyber environments that are truly integrated, where protection, detection and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices, McAfee secures their digital lifestyle at home and away. By working with other security players, McAfee is leading the effort to unite against cybercriminals for the benefit of all.

www.mcafee.com.

*Methodology
McAfee commissioned independent technology market research specialist Vanson Bourne to undertake the research upon which this report is based. A total of 775 IT decision makers who are involved in cybersecurity within their organization were interviewed in May 2016 across the US (200), the UK (100), France (100), Germany (100), Australia (75), Japan (75), Mexico (75) and Israel (50). The respondents were from organizations with at least 500 employees, and came from within both public and private sectors. Interviews were conducted online using a rigorous multi-level screening process to ensure that only suitable candidates had the opportunity to participate.

Vanson Bourne is an independent specialist in market research for the technology sector. Their reputation for robust and credible research-based analysis is founded upon rigorous research principles and their ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets.

62535rpt_cybersecurity_workforce_shortage_0716
JULY 2016

McAfee™
Together is power.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com