Securing Our Future: Closing the Cybersecurity Talent Gap

October 2015 results from the Raytheon-NCSA survey of young adults in 12 countries about cybersecurity career interest and preparedness

NATIONAL CYBERSECURITY ALLIANCE

Raytheon

Overview

As stories in the news of digital attacks against individuals and companies are becoming a common reality, the high demand globally for cybersecurity professionals keeps growing as the threat increases. A record 79 percent of U.S. businesses reported a cybersecurity incident in the last year, and the 238,158 job postings for cybersecurity-related jobs in 2014 is an increase of 91 percent from 2010. In the U.S. alone, companies posted 49,493 jobs requiring CISSP certification last year, however, there are only 65,362 CISSP holders, the majority of whom are already employed.[1] This talent gap has serious implications for domestic and international economics and security and must be addressed.

To shed some new light on how we should tackle this worldwide issue, Raytheon and the National Cyber Security Alliance (NCSA) commissioned *Securing Our Future: Closing the Cyber Talent Gap*, a survey to understand the career interests and educational preparedness of millennials (ages 18 to 26) in 12 countries around the world. This study was fielded by Zogby Analytics, which also conducted the 2013 and 2014 surveys.

It is imperative for the national security of our country and its allies that the workforce pipeline for cybersecurity professionals be filled with a plentitude of qualified workers. This survey is intended to give insights into the root causes of the global cybersecurity talent gap.

Results from this year's survey indicate that millennials aren't acutely aware of cybersecurity job opportunities but they are generally interested. Schools are also not preparing young adults for these jobs, and there is a gap within the gap, with females less interested and informed about careers in cybersecurity than their male counterparts. With this knowledge and survey results, we can chart a course forward, which requires the active collaboration between business sectors, the government and our higher and lower education systems. This multifaceted approach is required if millennials and future generations are to become the sharp, aware and talented cyber defenders our societies need.

[1] Burning Glass Technologies (2015). Job Market Intelligence: Cybersecurity Jobs, 2015. Retrieved from http://burning-glass.com/research/cybersecurity/

Methodology and Sample Characteristics

Securing Our Future: Closing the Cyber Talent Gap was fielded by Zogby Analytics from July 29 to Aug. 10, 2015. The responses were generated from a survey of 3,871 adults in Australia, Estonia, France, Germany, Japan, Poland, Qatar, Republic of Korea, Saudi Arabia, U.K., United Arab Emirates and the U.S. from ages 18 to 26. Using trusted interactive partner resources, thousands of adults were invited to participate in this interactive survey. Each invitation is password coded and secure so that one respondent can only access the survey one time. Using information based on census data, voter registration figures, CIA fact books and exit polls, we use complex weighting techniques to best represent the demographics of the population being surveyed. Weighted variables may include age, race, gender, region, party, education and religion.

Based on a confidence interval of 95 percent, the margin of error for each region is shown in the table below. This means that all other things being equal, the identical survey repeated will have results within the margin of error 95 times out of 100.

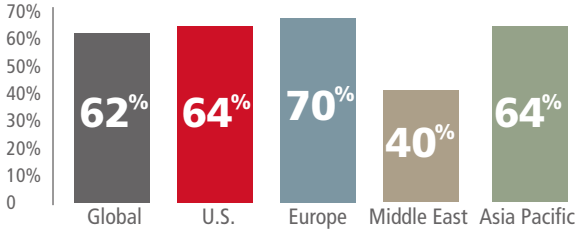
Country	Number of Respondents	Margin of Error
U.S.	1,005	+/- 3.2 Percentage Pts
Europe	1,256	+/- 2.8 Percentage Pts
Middle East	606	+/- 4.1 Percentage Pts
Asia Pacific	1,004	+/- 3.2 Percentage Pts

Note: The 2013, 2014 and 2015 surveys did not poll the same individuals.

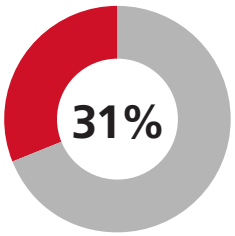
Low Awareness of the Cybersecurity Profession

Perhaps the most important step in solving the cybersecurity profession talent gap is making millennials aware of the issue and the opportunities available to them in this growing career field. Many simply do not know that the career field is an option.

The talent gap will not close without more millennials choosing a cyber-related degree. Most (69 percent) enter college or the workforce believing that their high school or secondary school had not offered them the classes or skills necessary, although this number is better in the Middle East than other parts of the world. Combine this with the number of millennials (62 percent) who say no teacher, guidance counselor or supervisory adult ever mentioned the career field to them, and it becomes clear why young adults are not considering cybersecurity careers.



No teacher or guidance or career counselor ever mentioned the idea of a career in cybersecurity



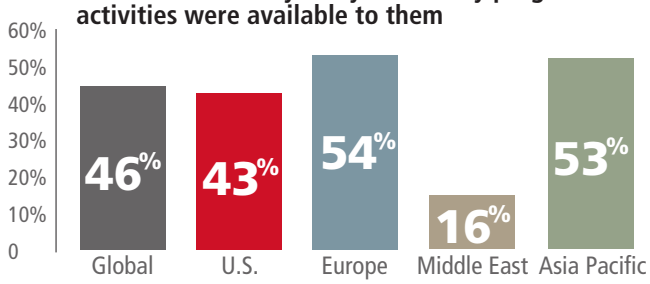
Young adults globally whose high school or secondary school computer classes prepared them to pursue a career in cybersecurity or a related degree.

Low Awareness of the Cybersecurity Profession

With so many millennials saying they were unaware of the careers available to them in cyber, it should come as no surprise that 46 percent said that cybersecurity programs and activities were not available to them at all.

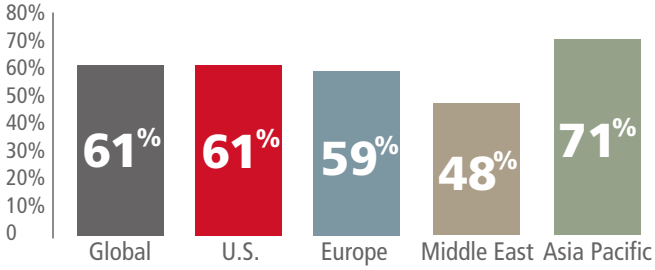
24% have not sought out cybersecurity programs and activities because they did not think they were qualified

Millennials who say no cybersecurity programs or activities were available to them



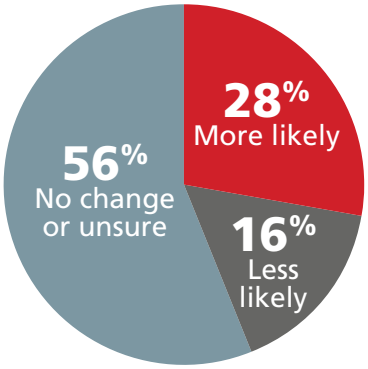
Seventy-nine percent of millennials say they have never spoken to a practicing cybersecurity professional or are unsure if they have. This lack of personal interaction with professionals also affects how much millennials know about the types of work involved in the field.

Young adults unaware or unsure of typical range of responsibilities involved in a cyber career



Millennials' Interest in Cyber

While many young adults are generally unaware of the cybersecurity job opportunities available, that does not necessarily equate to meaning they have no interest in the field. Compared with a year ago, 28 percent more millennials say they are more likely to choose a career to make the Internet safer for users.

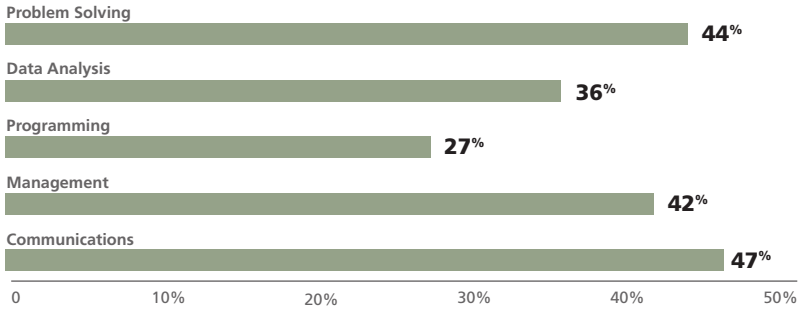


Likelihood of choosing a career to make the Internet safer versus a year ago

Millennials' Interest in Cyber

This is more than just a passing interest, as 38 percent of millennials say they have already participated in or sought out competitions, internships, scholarships, job fairs or mentoring programs related to cybersecurity. Also important to note is that millennials appear to possess a latent interest in skills used in the cybersecurity career field. They may just be unaware the field is about a lot more than ones and zeroes. Young adults say they want careers that use skills required for cyber careers.

Millennials want jobs using skills cyber professionals use:

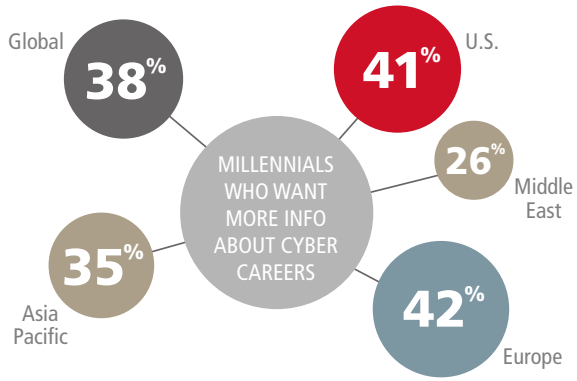


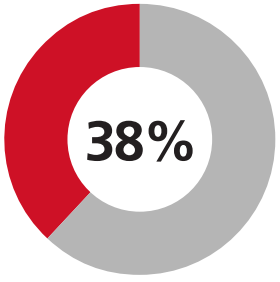
There are more positive takeaways as 50 percent say believing in their employer's mission is important to them, and 63 percent say salary is important. Cybersecurity careers offer both higher pay and the opportunity to ensure national and economic security.

Engaging Millennials

The survey has shown that millennials would likely pursue a cybersecurity career if they are aware of what the job entails. This leads to the question: How do we engage millennials so a career in cybersecurity isn't a foreign concept to them? Results from the survey indicate several ways that millennials can be engaged.

Thirty-eight percent of millennials would like more information on what a cybersecurity career entails.





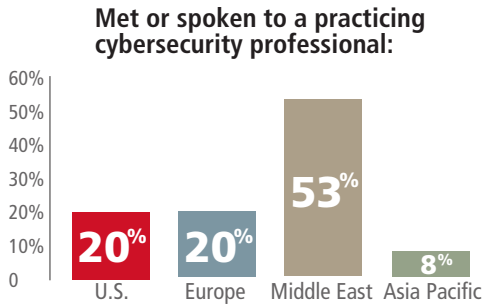
Want more classes or training to see if they would be good at a cyber career

Engaging Millennials

Taking advantage of existing cybersecurity professionals through mentoring programs or simple career conversations with millennials can make a big impact. Twenty-nine percent of young adults say they would like the opportunity to meet someone working in the field. Of the millennials who say they have met a cybersecurity professional, 60 percent said they had a conversation with them about careers. This indicates high interest among millennials who are familiar with cybersecurity careers and shows that networking is an effective tool to engage prospective professionals.

29% want the opportunity to meet a cybersecurity professional to discuss careers but only

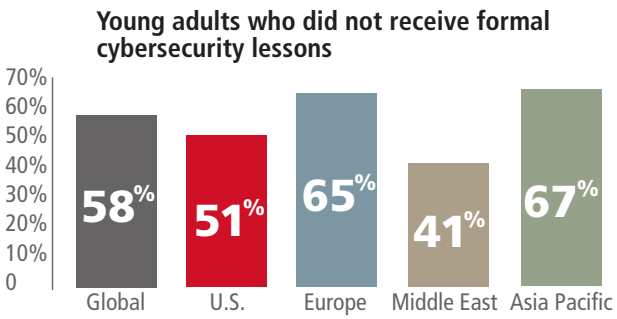
21% have met one before



Millennials also have preconceived notions regarding the downsides of cybersecurity careers, as 21 percent cite stress and 18 percent cite boring job tasks. There is a need to dispel the incorrect ideas that the field provides inadequate salaries (15 percent) and that fighting inevitable cyber attacks is a futile effort (21 percent). The identification of these real or imagined barriers that are keeping young adults from pursuing cybersecurity careers is a step toward knowing what must be overcome.

Education Isn't Addressing Cybersecurity

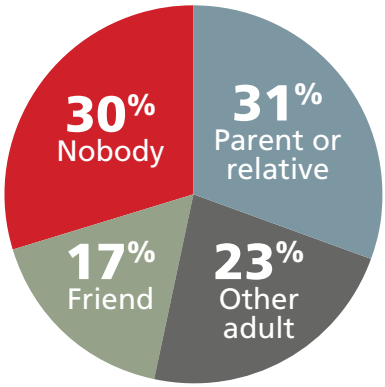
While computers and the Internet have steadily become standard tools in classrooms over the last couple of decades, the use of the technology has not directly related to training or knowledge in cybersecurity. A majority of millennials (58 percent) said they were not taught in the classroom about ways to stays safe online or were unsure whether their lessons provided that knowledge.



Education Isn't Addressing Cybersecurity

Many had families who took the time to educate them about staying safe online, as 31 percent of respondents said a parent or relative gave them their first talk about staying safe online. Unfortunately, 30 percent said said no one has given them a talk about online safety.

Who gave Millennials their first cyber talk?

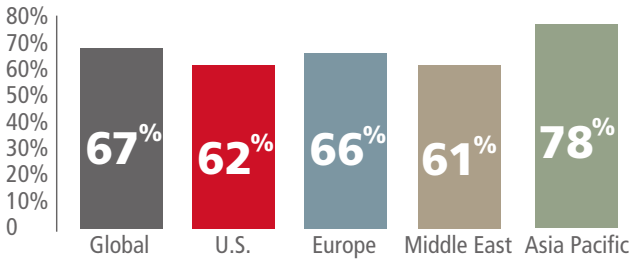


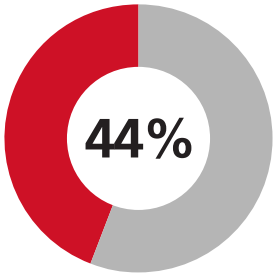
Millennials' Overconfidence in Abilities

The majority of millennials (65 percent) feel they have the ability to stay safe online, despite the lack of education, awareness and engagement of cybersecurity as a career. However, these same shortcomings that are contributing to the talent gap also contradict young adults' belief that their online actions are secure.

More alarming is the lack of awareness of current threats among millennials, and not changing their behaviors despite experiencing security breaches firsthand. Despite more publicized threats and hacks in the news, 67 percent of millennials say they didn't hear about a cyber attack in the last year, and 84 percent said they have not read any articles about the topic in the past month. Also troubling: of those young adults who experienced credit card fraud, identity theft, a malware-infected device or other personal online violation within the last year, nearly half (44 percent) said they did not change their behavior as a response.

Young adults who didn't hear about cyber attacks in the news last year:



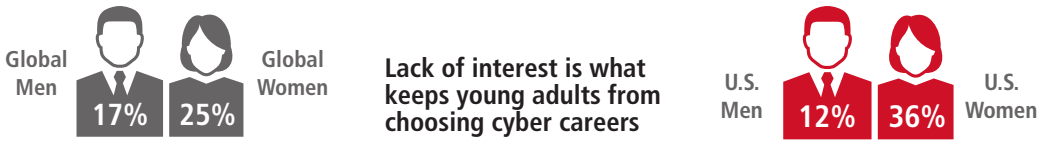


Upon having a credit card number stolen, identity theft, a device infected with malware or other personal online violation happen within the last year, nearly half of young adults did not change their behavior as a response

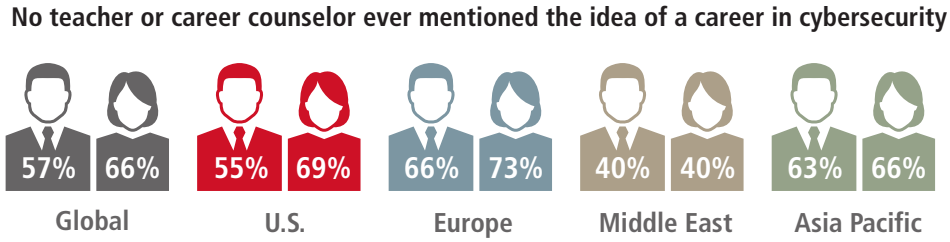
The Gap Within the Gap

The last major finding in this year's survey results is a noticeable gender gap between men and women and their feelings or history with cybersecurity-related issues. While the gender gap is global, it is slightly larger in the U.S. When working on solutions to close the talent gap, extra steps should be taken to ensure these solutions and answers to the problem reach all millennials, regardless of gender.

Globally, for those young adults who said they are less likely now than a year ago to choose a career to make the Internet more secure, 25 percent of females and only 17 percent of males gave lack of interest in that kind of work as the reason. In the U.S., the gap is even wider. When it comes to awareness of what a cybersecurity career entails, the gap is even larger with 51 percent of U.S. men and only one third of U.S. women having such knowledge.



So, what are the causes of this gender gap in a career field already desperate for skilled workers? As shown, millennials aren't receiving information about the cybersecurity profession, but the problem is even worse for females. Compared with men, 9 percent more females reported that no high school or secondary teacher or counselor had discussed cybersecurity careers as an option with them.



Meanwhile, 62 percent of men and three quarters of women globally said no high school or secondary school computer classes offered the skills necessary or prepared them to pursue a career in cybersecurity or a related degree like computer science.

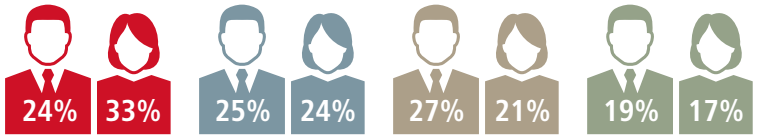
Young men are more likely than young women to consider cybersecurity careers. Globally, men are more likely (33 percent) than women (24 percent) than they were a year ago to consider a career where they could make the Internet safer and more secure. In the U.S. the gap is wider with 40 percent of men and only 23 percent of women more likely now to choose such careers.

Globally, nearly an equal amount of women (25 percent) and men (23 percent) said they haven't sought out cybersecurity programs because they did not think they were qualified.

The Gap Within the Gap

The consistently worse gender gap in the U.S. showed again in the numbers, with a nine-percentage-point disadvantage for women saying they didn't think they were qualified compared with men. In contrast, the difference between genders is less in Europe (1 percent), Middle East (5 percent) and Asia Pacific (2 percent).

More U.S. women felt they were not qualified for cybersecurity programs and activities than men.



Conclusion

While each country surveyed has its own small differences, the survey results show common themes among millennials globally when it comes to cybersecurity as a career option. Between not being aware of the field, not receiving an education that prepares them for computer science, being overconfident in their online behavior or the gender gap within the talent gap, there are many reasons cybersecurity jobs are going unfilled. The good news, however, is that by identifying these problems, we can put solutions in place that address the issues millennials face when it comes to pursuing careers in cybersecurity.

We cannot underestimate the importance of solving this problem. According to the U.S. Department of Homeland Security, "As information technology becomes increasingly integrated with physical infrastructure operations, there is increased risk for wide scale or high-consequence events that could cause harm or disrupt services upon which our economy and the daily lives of millions of Americans depend. In light of the risk and potential consequences of cyber events, strengthening the security and resilience of cyberspace has become an important homeland security mission."[2] Developing a strong cybersecurity workforce is critical to ensure global economic and security stability.

With online breaches and attacks trending in today's headlines, there is a golden opportunity for industry and educators to mention cybersecurity careers and generate more interest with millennials and younger generations. Educators and current cybersecurity professionals need to collaborate to develop courses, provide information about cybersecurity job responsibilities, ensure both genders are being informed, and offer mentoring and job shadowing. Millennials and the future generations would be more interested in cybersecurity professions if they had information about the many career paths and the required training.

The private sector, government and educational institutions also need to work together to help inspire our next generation of innovators and cybersecurity defenders. We'll need millennials' talent to protect data and devices as the world becomes increasingly connected.

[2] U.S. Department of Homeland Security (2015). Cybersecurity Overview. Retrieved from http://www.dhs.gov/cybersecurity-overview

About Raytheon

Raytheon Company, with 2014 sales of $23 billion and 61,000 employees worldwide, is a technology and innovation leader specializing in defense, security and civil markets throughout the world. With a history of innovation spanning 93 years, Raytheon provides state-of-the-art electronics, mission systems integration and other capabilities in the areas of sensing; effects; and command, control, communications and intelligence systems, as well as cybersecurity and a broad range of mission support services. Raytheon is headquartered in Waltham, Massachusetts.

Raytheon became the three-year sponsor of the National Collegiate Cyber Defense Competition in 2014 and also provides technical resources and employee volunteers to the event. The tournament-style competition sees student-only teams from 180 U.S. colleges and universities competing to protect computer networks against real-world cyberthreats.

The company has several executives currently serving on the advisory boards of different colleges and universities, and runs internship programs that brings college students into the business to learn firsthand. Other Raytheon initiatives include MathMovesU®, an ever-expanding family of unique initiatives and key partnerships that connects with students from elementary school through college to address the STEM education crisis; the Raytheon MATHCOUNTS National Competition; and Teachers in Industry, a program through the University of Arizona that gives teachers summer internships so they can bring knowledge back into the classroom.

For more about Raytheon, visit us at www.RaytheonCyber.com and follow us on Twitter @ RaytheonCyber.

About Zogby Analytics

Zogby Analytics is respected nationally and internationally for its opinion research capabilities. Since 1984, Zogby has empowered clients with powerful information and knowledge critical for making informed strategic decisions.

The firm conducts multi-phased opinion research engagements for banking and financial services institutions, insurance companies, hospitals and medical centers, retailers and developers, religious institutions, cultural organizations, colleges and universities, IT companies and Federal agencies. Zogby's dedication and commitment to excellence and accuracy are reflected in its state-of-the-art opinion research capabilities and objective analysis and consultation.

About The National Cyber Security Alliance

The National Cyber Security Alliance (NCSA) is the nation's leading nonprofit public-private partnership promoting the safe and secure use of the Internet and digital privacy. Working with the Department of Homeland Security (DHS), private sector sponsors and nonprofit collaborators to promote cybersecurity awareness, NCSA board members include representatives from ADP, AT&T, Bank of America, BlackBerry, Comcast Corporation, ESET, Facebook, Google, Intel, Logical Operations, Microsoft, PayPal, PKWARE, RSA - the Security Division of EMC, Raytheon, Symantec, Verizon and Visa. Through collaboration with the government, corporate, nonprofit and academic sectors, NCSA's mission is to educate and empower digital citizens to use the Internet securely and safely, protect themselves and the technology they use, and safeguard the digital assets we all share. NCSA leads initiatives for STOP.THINK.CONNECT., a global cybersecurity awareness campaign to help all digital citizens stay safer and more secure online; Data Privacy Day, celebrated annually on January 28 and National Cyber Security Awareness Month, launched every October.

For more information on NCSA, please visit staysafeonline.org/about-us/overview/.

Raytheon
Intelligence, Information
and Services
22260 Pacific Blvd
Sterling, VA
20166 USA

www.RaytheonCyber.com/TalentGap

Raytheon

Customer Success Is Our Mission