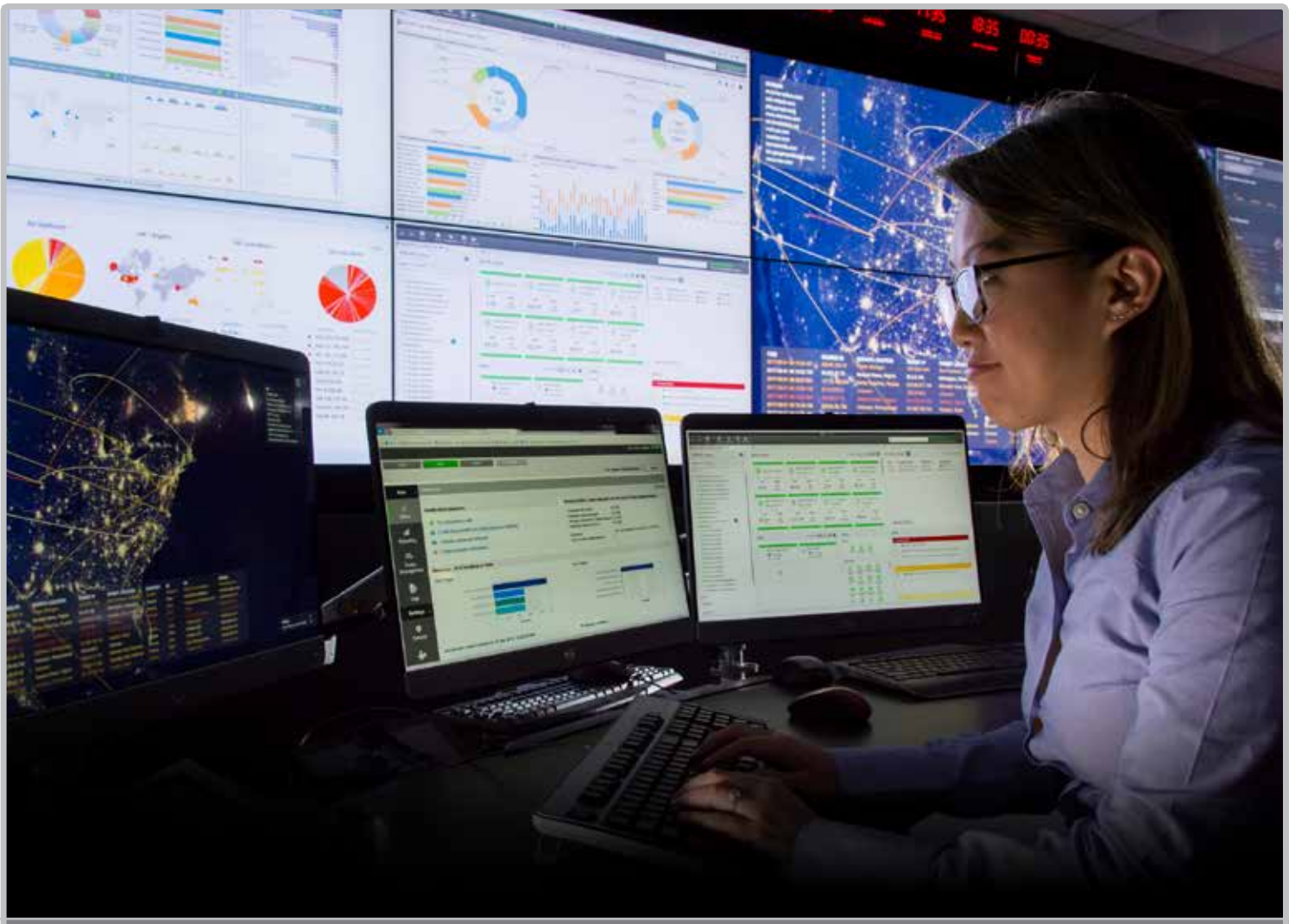


Securing Our Future:
Cybersecurity and the Millennial Workforce

A study commissioned by Raytheon, Forcepoint and the National Cyber Security Alliance about security practices in the new workforce and preparedness for cybersecurity careers among young adults in nine countries.

FORCEPOINT
POWERED BY Raytheon

NATIONAL CYBERSECURITY ALLIANCE

Raytheon

OVERVIEW

The ever-evolving era of internet-connected technology has provided the world with unprecedented ways to make our lives easier and more productive. Unfortunately, when everything is connected, everything is potentially vulnerable to cyber threats.

The resulting rise in cyber risks has created a worldwide need for cybersecurity employees, one that is as real as the attacks that are occurring all too often these days. In the next five years, it's estimated 1.8 million cybersecurity jobs will go unfilled across the globe.[1]

For the fifth consecutive year, Raytheon, Forcepoint and the National Cyber Security Alliance conducted the *Securing Our Future: Cybersecurity and the Millennial Workforce* survey of more than 3,000 millennials in nine countries to better understand the issues and improve the current state.

The themes of this report were based on the answers of these young adults. They provide an interesting look into the cybersecurity career field as it relates to millennials:

- Millennials believe cybersecurity is important; however, they generally practice cyber behavior that could put their employer at risk.
- There is an increased level of awareness about cybersecurity career options, but that hasn't translated to a higher interest in the field.
- Various types of role models are key to inspiring young people to choose cybersecurity careers.

[1] *Eighth Global Information Security Workforce Study, (ISC)², 2017*

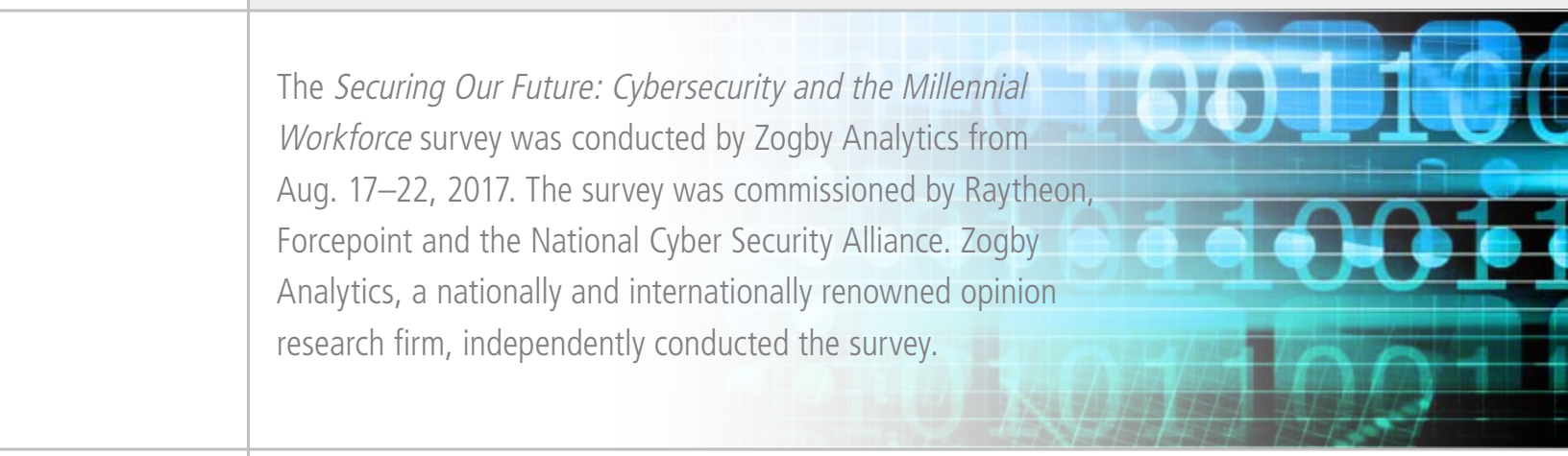
OVERVIEW

- Women continue to say they run into more hardships and have fewer opportunities than their male counterparts.
- Improvements in education have raised cybersecurity awareness.
- Millennials believe, often incorrectly, that they are unqualified for cyber careers.
- Young adults want to feel personally connected to the goals of their employers.
- Millennials in the U.S. blame cyberattacks for their loss of trust in the electoral system.

With a shortage of cyber professionals and the need for employers to adapt to a changing, younger workforce, this survey report provides insights into the root causes of these findings, suggests courses of action to develop a strong cybersecurity talent pool and provides employers an understanding of the pool's security practices.

Raytheon and Forcepoint's collaboration with the National Cyber Security Alliance underscores their shared mission to improve cybersecurity postures at all levels of security, including individual, organizational, national and global. This survey is one of numerous ways all three organizations work to fulfill this important commitment to the world's citizens, businesses and governments.

METHODOLOGY AND SAMPLE CHARACTERISTICS

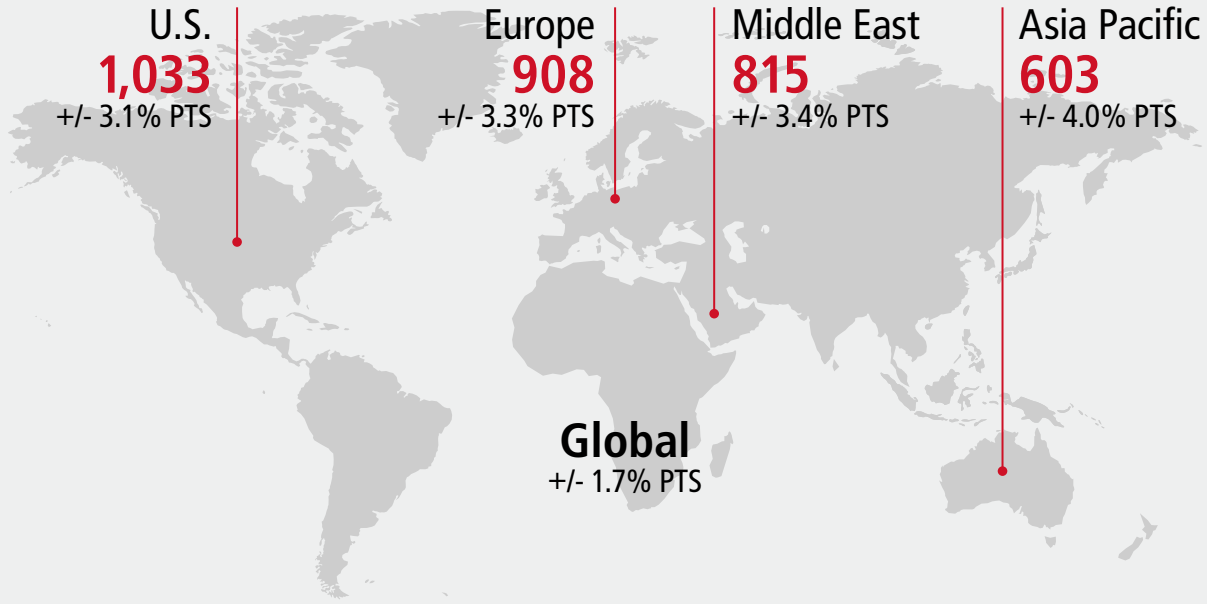


The *Securing Our Future: Cybersecurity and the Millennial Workforce* survey was conducted by Zogby Analytics from Aug. 17–22, 2017. The survey was commissioned by Raytheon, Forcepoint and the National Cyber Security Alliance. Zogby Analytics, a nationally and internationally renowned opinion research firm, independently conducted the survey.

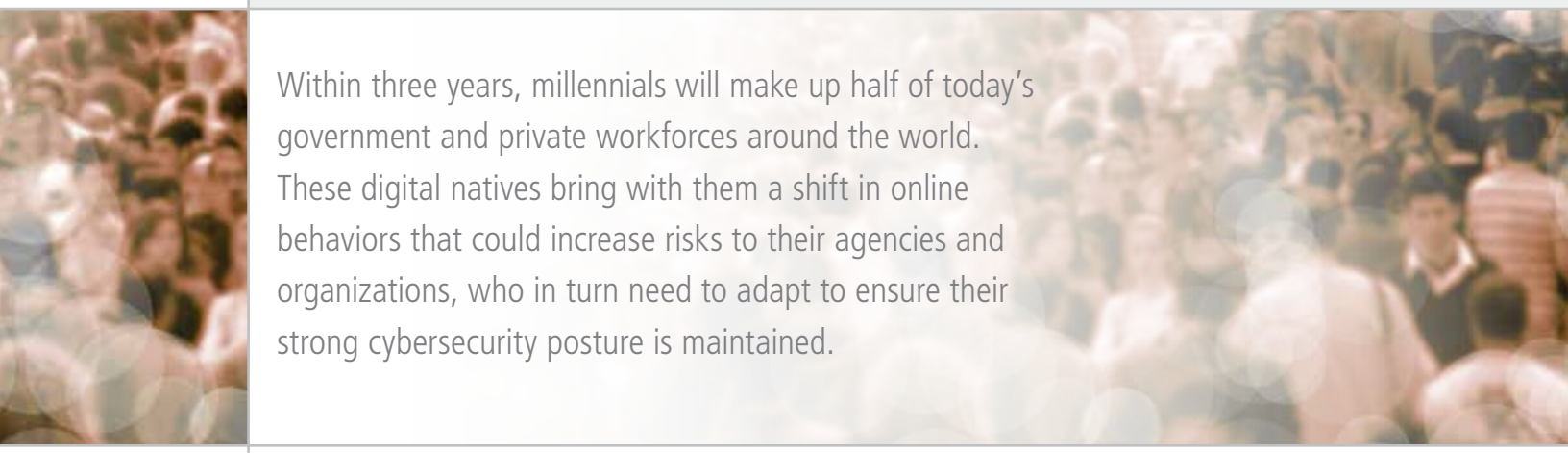
The global study polled 3,359 young adults ages 18–26 in nine countries: Australia, Germany, Jordan, Poland, Qatar, Saudi Arabia, United Arab Emirates, United Kingdom and United States. Using trusted interactive partner resources, thousands of adults were invited to participate in this interactive survey. Each invitation was password coded and secure to ensure each respondent could only access the survey one time. Using information based on census data, voter registration figures, CIA fact books and exit polls, Zogby used complex weighting techniques to best represent the demographics of the surveyed population. 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.

RESPONDENTS AND MARGIN OF ERROR IN SURVEY SHOWN BY COUNTRY



WORKFORCE PRACTICES



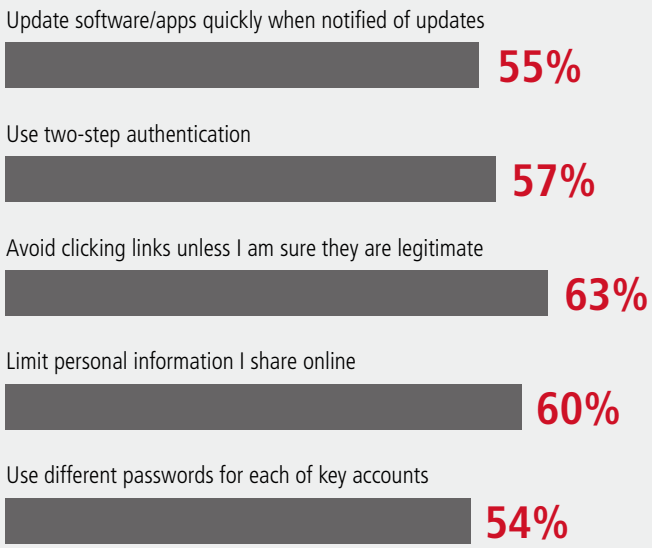
Within three years, millennials will make up half of today's government and private workforces around the world. These digital natives bring with them a shift in online behaviors that could increase risks to their agencies and organizations, who in turn need to adapt to ensure their strong cybersecurity posture is maintained.

The good news on this issue is that most millennials believe that cybersecurity is important, with 83 percent surveyed saying it's "important, very important or extremely important" to increase cybersecurity awareness programs in the workforce and formal education programs. Most also reported an increase in such programs, with 70 percent somewhat or strongly agreeing that their high school or secondary education prepared them to use technology safely, securely, ethically and productively in the workplace, up from 55 percent in 2013.

The bad news is that this belief has not translated to most young adults using proper cybersecurity practices.

> "...most millennials believe that cybersecurity is important..."

ACTIONS MILLENNIALS DON'T TAKE BUT THINK THEY SHOULD



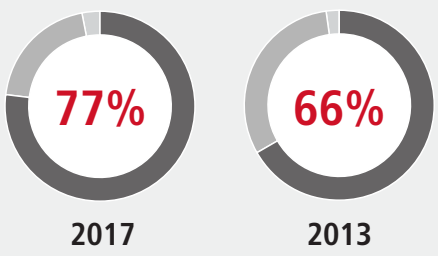
WORKFORCE PRACTICES (CONTINUED)

Millennials said they are good about protecting their smartphones (87 percent) and computers (83 percent) with a password or PIN. But they're also often overlooking the importance of protecting other connected devices with passwords, with just 46 percent doing so for their tablets and 25 percent for their game consoles.

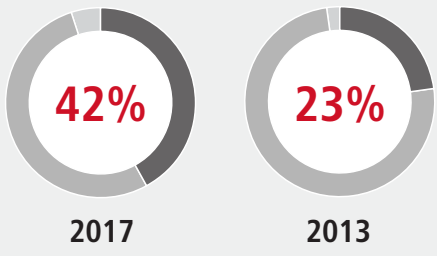
Other behaviors young adults admitted to could spell danger for employers if used in the workplace, with survey results showing a step backward as compared with 2013's survey.

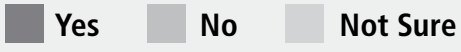
> "Behaviors young adults admitted to could spell danger for employers if used in the workplace."

MILLENNIALS WHO CONNECTED TO NO-PASSWORD WI-FI IN THE LAST MONTH



YOUNG ADULTS WHO SHARED A PASSWORD WITH A NON-FAMILY MEMBER IN THE LAST YEAR





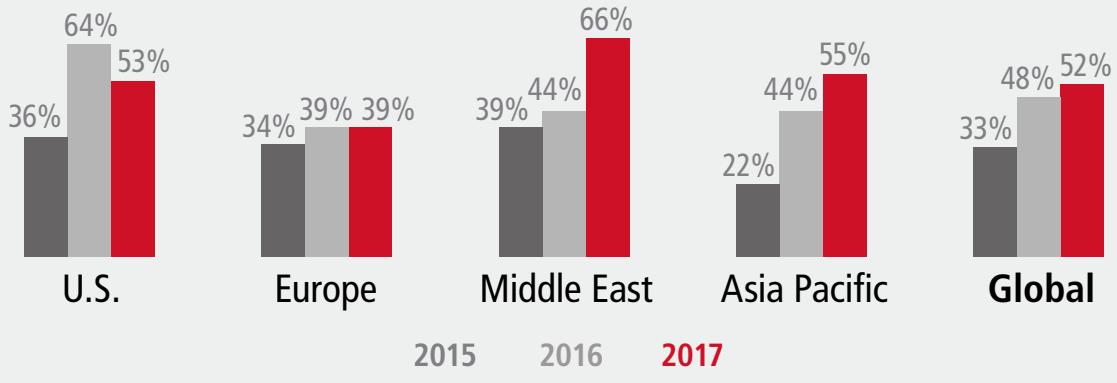
AWARENESS OF CYBERSECURITY ISSUES AND CAREERS

The rise of knowledge among young adults about the importance of cybersecurity has also translated into an increased level of awareness about cybersecurity career options. However, many millennials aren't aware of recent cyberattack news and their interest in cyber positions seems to be stagnant.

Over the last few years, a divide has existed between the skill sets applicable to a cybersecurity career and the skills that young adults believe the job requires. However, the 2017 survey showed improvement in this area with 52 percent of respondents saying they know the typical range of responsibilities and job tasks involved in the cyber profession, an increase of 15 percent since 2014. Yet, there is a gender gap behind those numbers, with nearly two-thirds of men aware of cyber job responsibilities compared to 41 percent of women.

Thirty-nine percent of respondents said they were more likely than a year ago to consider a career where

YOUNG ADULTS WHO HEARD ABOUT CYBERATTACKS IN THE NEWS LAST YEAR



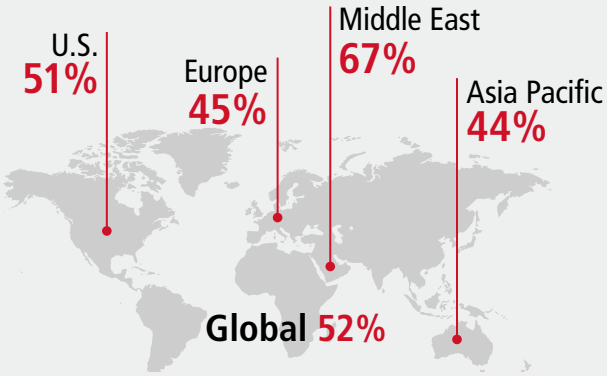
AWARENESS OF CYBERSECURITY ISSUES AND CAREERS (CONTINUED)

they could make the internet safer and more secure. This figure has fluctuated but on average has remained flat since 2014. However, a closer look at the survey results since then reveals a growing gender gap.

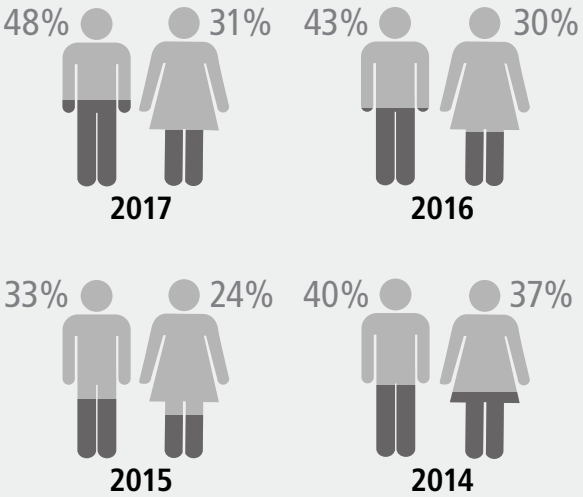
Among those who said they were more likely to choose such a career, the top reason cited (52 percent) was a belief that a secure internet is "important." This opens the potential for millennials to see cyber jobs as a valid option, considering that a whopping 89 percent of those surveyed said a personal connection to their employer's goals was of "average, very or extreme importance" to them.

On a related note, a high number of millennials say they want a career that requires problem-solving, management, data analysis, communication or software programming, but they aren't aware that the cybersecurity field calls for those skills.

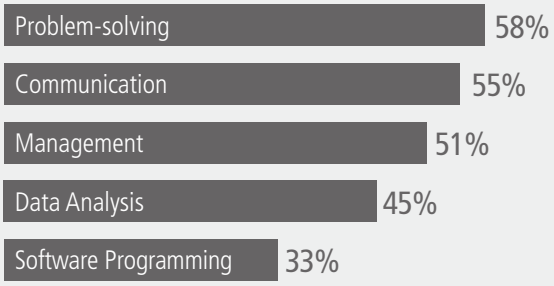
YOUNG ADULTS WHO KNOW WHAT CYBERSECURITY PROFESSIONALS DO



MILLENNIALS MORE LIKELY THAN A YEAR BEFORE TO CHOOSE A CAREER TO MAKE THE INTERNET SAFER



MILLENNIALS WHO WANT A JOB REQUIRING THESE SKILLS, ALL OF WHICH ARE AVAILABLE IN CYBER



WHY ARE YOU MORE INTERESTED NOW IN A CAREER TO KEP THE INTERNET SAFE THAN A YEAR AGO?

Includes only respondents more interested now than a year ago

INFLUENCE OF ROLE MODELS

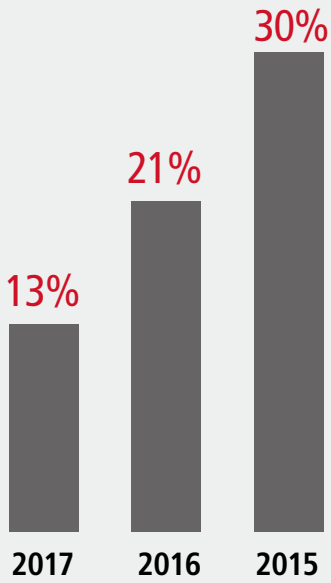
The increasing pervasiveness of cybersecurity issues in the world today underscores the need for cyber professionals, parents and peers to influence young adults' career decisions.

The number of those surveyed who reported having met or spoken to these potential cyber role models has steadily increased to 32 percent, up slightly from previous years. Of those who said they had met one, 72 percent said the professional discussed cyber as a career field with them. More than one-third of young adults (36 percent) also reported knowing a classmate in high school or college who was studying to enter the field, and that connection can help young adults gauge their interest and aptitude for their own careers.

The proportion of millennials reporting that a parent was the first to talk to them about cybersecurity importance remained steady from 2016 to 2017 at 43 percent. This is by far the highest of any type of person in a young adult's life, including other relatives, friends, teachers and other adults.

Parents also held the top rank (40 percent) as influential figures in regard to career advice, the same percentage as 2016, and are savvier than a year ago in their ability to guide young adults

MILLENNIALS REPORTING NOBODY HAS TALKED TO THEM ABOUT STAYING SAFER ONLINE

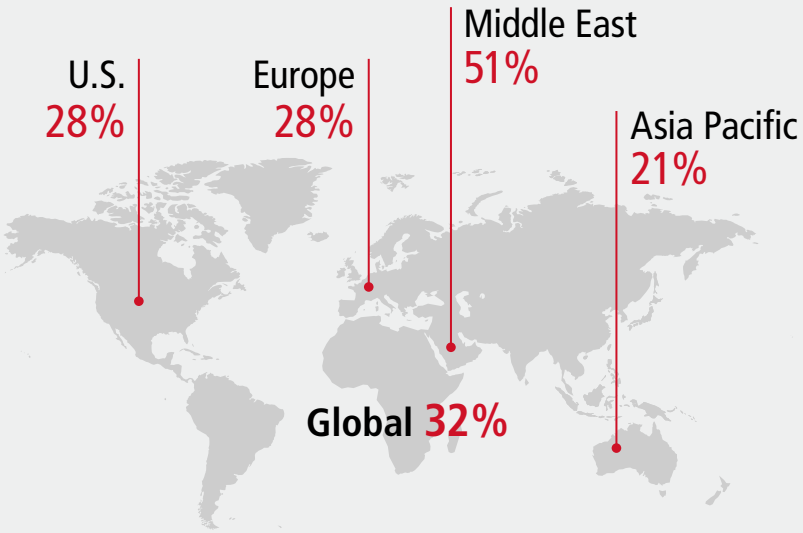


INFLUENCE OF ROLE MODELS (CONTINUED)

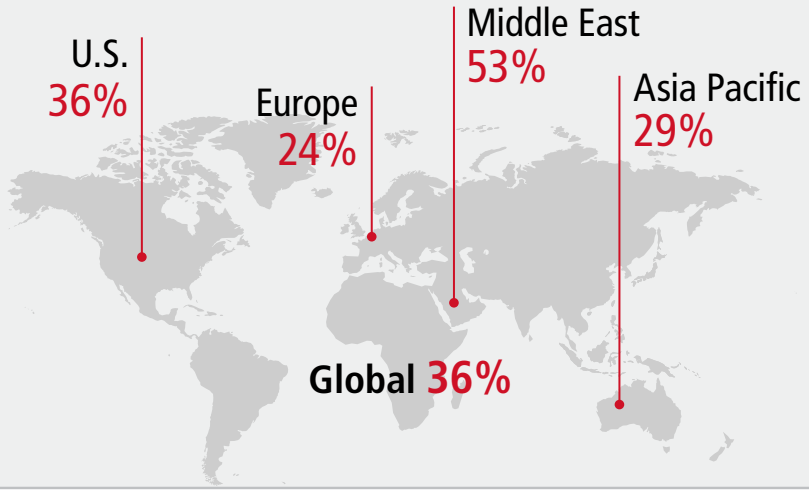
to pursue cybersecurity careers. However, gender gap issues appear here, with 65 percent of men and 48 percent of women saying they had confidence their parents could guide them to pursue a cyber career, up from 51 percent (men) and 38 percent (women) last year. This could mean parents favor sons when it comes to cyber, or that young women are projecting their lack of confidence in a cyber career onto their parents.

Still, 57 percent of millennials are "confident" or "very confident" in their parents' ability to guide them in pursuing a cybersecurity career, a significant boost from 45 percent in 2016.

MILLENNIALS WHO HAVE MET A CYBER PROFESSIONAL



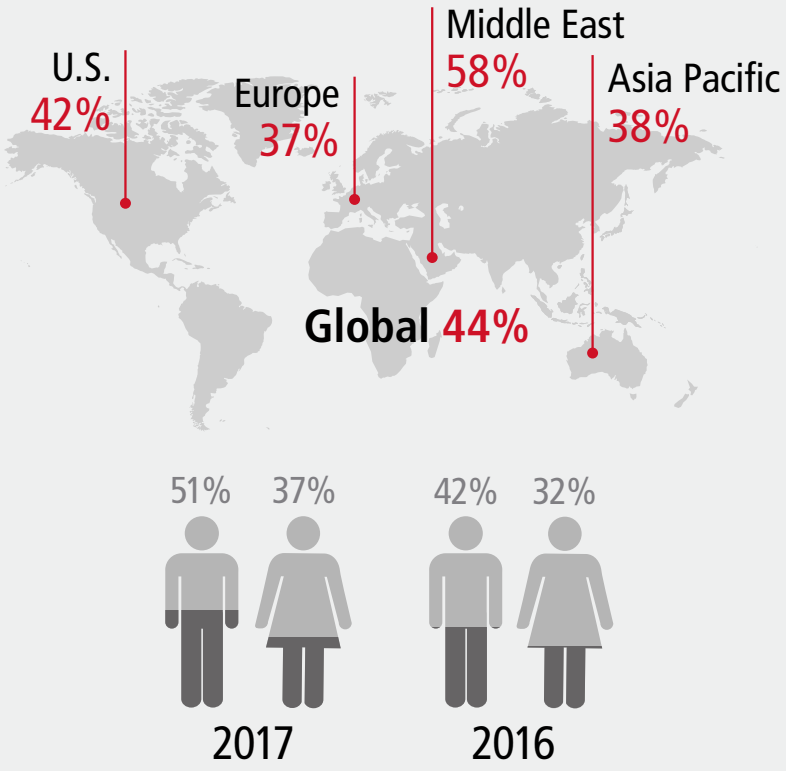
YOUNG ADULTS WHO HAVE KNOWN SOMEONE STUDYING CYBERSECURITY



EDUCATION IMPROVEMENTS

Global efforts to improve education about cyber seem to be paying off, and are also likely contributing to the positive results seen in other areas of the survey results. Sixty-two percent of young adults said they were taught about staying safe online in a formal classroom setting, up from 55 percent in 2016.

MILLENNIALS WHOSE HIGH SCHOOL CLASSES PREPARED THEM TO PURSUE A CYBERSECURITY DEGREE



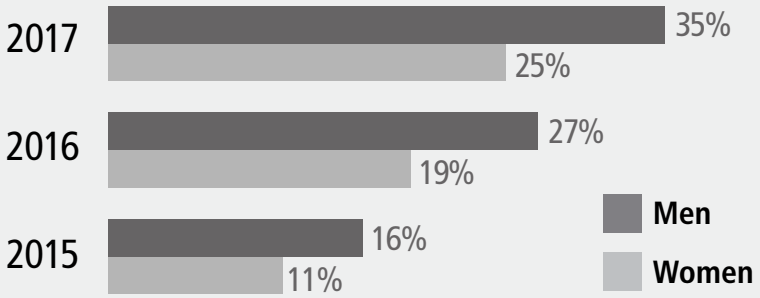
One of the biggest gains in cyber education at the classroom level is from teachers, as 37 percent of survey respondents said a teacher discussed cyber with them as a career choice. This has tripled since 2013, but also means nearly two-thirds of students are still not hearing about the opportunity to work in cybersecurity while in the classroom.

Only one-fourth of women compared to one-third of men also agreed that their high school education prepared them to use technology safely in the workplace. While teachers seem to be reaching more boys than girls, the average upward trend shows progress among educators.

EDUCATION IMPROVEMENTS (CONTINUED)

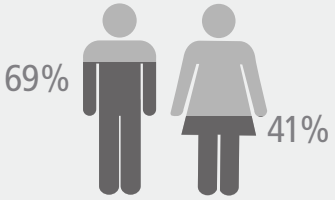
The use of enrichment activities for students to gauge interest or aptitude for cybersecurity as a career has also increased. In this year's survey, 26 percent of millennials said no cybersecurity programs or activities were available to them. While this may sound disappointing, progress is being made as the figures were 32 percent last year and 46 percent in 2015. The Middle East is outpacing the rest of the world by leaps and bounds in this arena, with just 2 percent of the region's respondents saying no such programs were available to them.

STRONGLY AGREE HIGH SCHOOL ENABLED SAFE USE OF TECHNOLOGY AT WORK

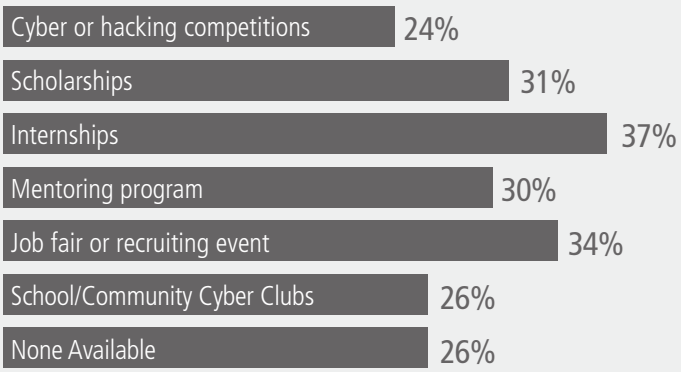


NO CYBERSECURITY PROGRAMS ARE AVAILABLE

SOUGHT OUT CYBERSECURITY PROGRAMS



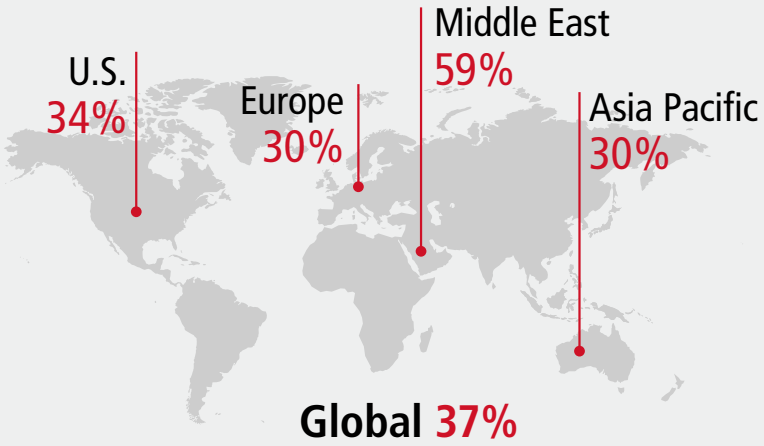
PERCENTAGE OF MILLENNIALS WHO SAID EACH ACTIVITY WAS AVAILABLE TO THEM



EDUCATION IMPROVEMENTS (CONTINUED)

A bright spot in the findings is that 55 percent of respondents have participated in at least one of these activities, up from 45 percent last year and 37 percent two years ago. This time spent on related activities could be an indication that these students might be on the road toward choosing cybersecurity as their occupation.

YOUNG ADULTS APPROACHED BY A TEACHER ABOUT CYBERSECURITY CAREERS

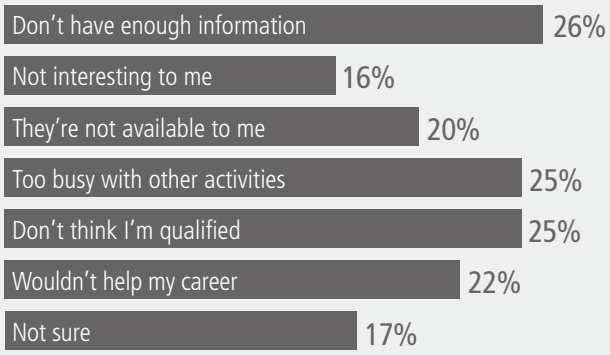


> "The number of U.S. teachers who talked to students about cybersecurity careers tripled from 2013 to 2017."

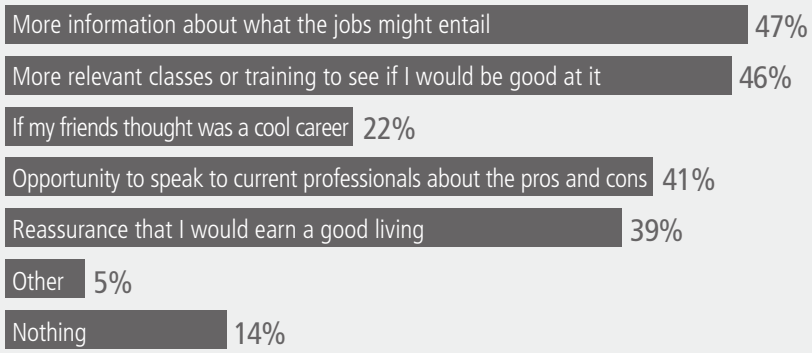
CAREER CHOICE FACTORS AND CONFIDENCE

Several factors come into play when young adults are choosing a career field, ranging from feelings of being qualified to wanting the profession to align with what is personally important to them.

WHY HAVEN'T YOU PARTICIPATED IN OR SOUGHT OUT ANY CYBERSECURITY PROGRAMS OR ACTIVITIES?



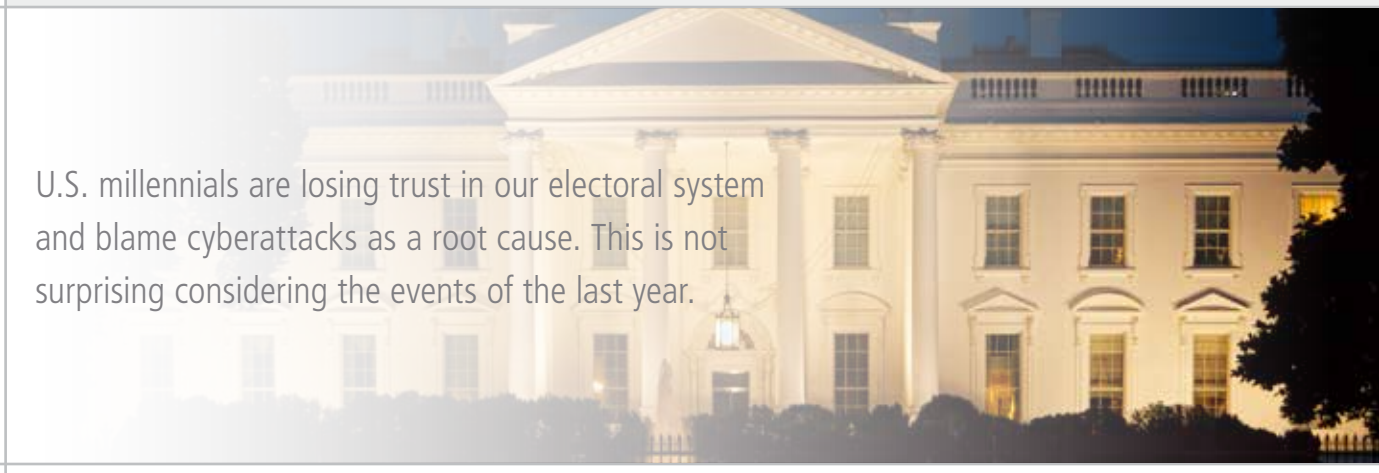
WHAT WOULD INCREASE YOUR INTEREST IN A CAREER IN CYBERSECURITY?



Of respondents who have never sought out a cybersecurity program, a leading reason young adults cite is that they do not think they are qualified, while lack of interest is the least cited reason. This finding represents a call to action among influential people in millennials' lives to instill confidence, encouragement and the right skills needed to get started.

Young adults show an overwhelming desire to feel personally connected to the goals of their employer, as a combined 89 percent said this was either "important, very important or extremely important" to them. When asked what type of organization they would want to protect, millennials reported government (41 percent) to technology companies (55 percent) to banks (50 percent), health care (45 percent), military (32 percent) and more.

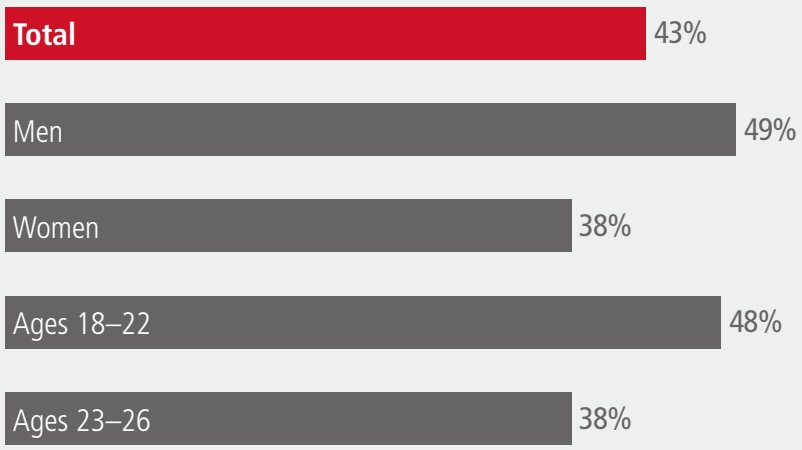
2016 U.S. PRESIDENTIAL ELECTION (U.S. RESPONDENTS ONLY)



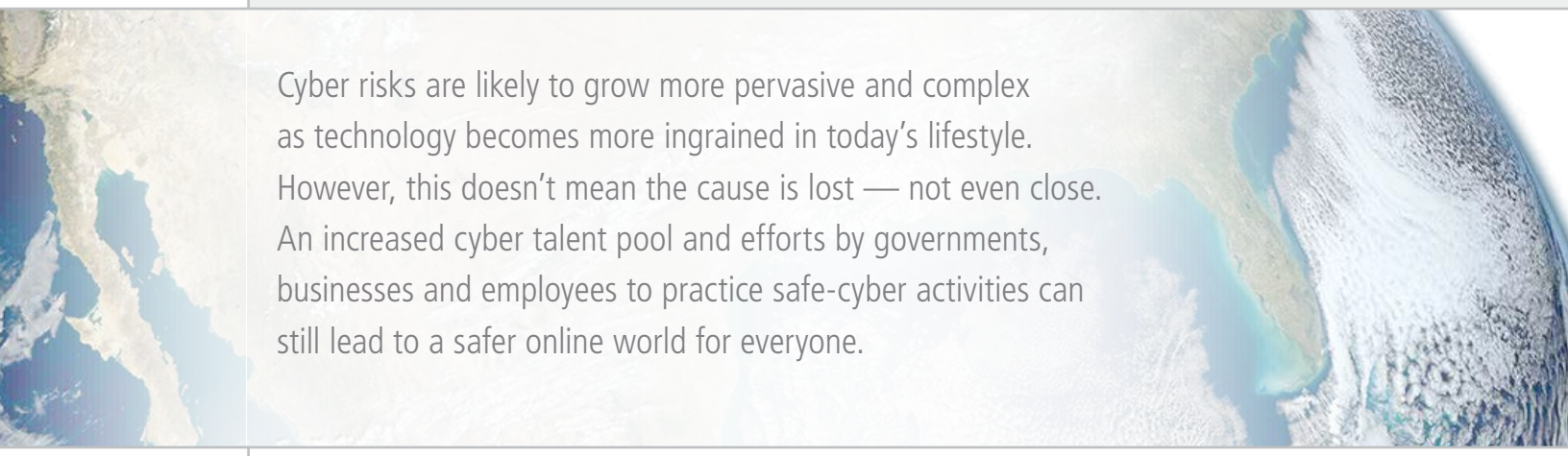
U.S. millennials are losing trust in our electoral system and blame cyberattacks as a root cause. This is not surprising considering the events of the last year.

As cybersecurity issues play an increasingly pervasive role in modern society, the electoral system has shown it can no longer escape scrutiny. A variety of sentiments has been represented in news headlines leading up to and following the 2016 U.S. presidential election. Regardless of what may or may not have occurred, 43 percent of U.S. young adults, the dominant share, believe cyberattacks influenced the election results. Just as a new generation is growing old enough to vote, many young Americans are already losing trust in a pillar of democracy and national security.

U.S. YOUNG ADULTS WHO THINK CYBERATTACKS INFLUENCED THE 2016 ELECTION



CONCLUSION



Cyber risks are likely to grow more pervasive and complex as technology becomes more ingrained in today's lifestyle. However, this doesn't mean the cause is lost — not even close. An increased cyber talent pool and efforts by governments, businesses and employees to practice safe-cyber activities can still lead to a safer online world for everyone.

Raytheon, Forcepoint and the National Cyber Security Alliance believe that millennials have a large hand to play in this effort because they will be in the workforce for decades to come, and they have grown up as natives to the digital landscape. Conducting the annual survey is an important piece of the puzzle for governments and businesses to understand their youngest and future employees and what might draw them to the cyber career field.

It's important to know that these young adults believe cybersecurity is important, just as it is to know they conduct cyber practices that might put businesses at risk. By understanding that millennials often feel that they aren't qualified for cyber jobs, and that they want a personal connection to their company's goals, schools and businesses are able to better appeal to them. Data showing that women face more difficulties or may be unconsciously overlooked can also help businesses to counter the problem with new approaches and opportunities.

There have been improvement in education systems regarding cybersecurity and there is an increased level of awareness among young adults about cyber careers. But that hasn't necessarily translated into more interest in the field. Role models such as teachers, parents and cyber professionals could play a larger role in countering this issue. The fact that many U.S. millennials also blame cyberattacks for their lost confidence in the electoral system might be turned into a positive because a cybersecurity career gives them a chance to do something about this set of issues.

There are multiple steps that can be — and are being — taken to secure the world's important information. While many factors can counteract these risks, such as policies, standards, technology and management, a strong, informed and ready talent pool of young adults could potentially take the lead for decades to come.

"Blue Marble" image of Earth (photo courtesy of NASA) captured by the Raytheon-built Visible Infrared Imaging Radiometer Suite (VIIRS).

ABOUT RAYTHEON

Raytheon Company, with 2016 sales of $24 billion and 63,000 employees worldwide, is a technology and innovation leader specializing in defense, civil government and cybersecurity solutions. Raytheon is headquartered in Waltham, Massachusetts.

With decades of experience in protecting information across any domain, Raytheon builds the most advanced cyber defenses into operational systems to safeguard what matters most. From hardening defense systems against intruders to protecting critical infrastructure and data, we offer the most effective shields against cyber threats.

Raytheon will continue our title sponsorship of the National Collegiate Cyber Defense Competition through 2019 and also provide technical resources and employee volunteers to the event. The tournament-style competition features student-only teams from 230 U.S. colleges and universities competing to protect computer networks against real-world cyberthreats. These contests are preparing students to take on threats in technology careers following graduation.

The company is also leading several cyber education initiatives.

Raytheon has also partnered with the Center for Cyber Safety and Education to establish the Raytheon Women's Cybersecurity Scholarship, a program that has provided more than $100,000 in scholarships and paid internships since 2016 to encourage women to pursue degrees in cybersecurity.

Raytheon's Cyber Academy, a global cyber education program, was launched in 2016 in the United Arab Emirates with a vision for expansion to additional countries.

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

ABOUT FORCEPOINT

Forcepoint works to transform cybersecurity by focusing on what matters most: understanding people's intent as they interact with critical data and intellectual property wherever it resides. The company's uncompromising systems enable companies to empower employees with unobstructed access to confidential data while protecting intellectual property and simplifying compliance. Based in Austin, Texas, Forcepoint protects the human point for thousands of enterprise and government customers in more than 150 countries. Forcepoint is an independent Raytheon company. For more about Forcepoint, visit www.Forcepoint.com and follow us on Twitter at @ForcepointSec.

ABOUT ZOGBY ANALYTICS

Zogby Analytics provides custom research and insight to individuals and leaders of businesses and communities and 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.

Zogby delivers data worldwide 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 numerous well-known and global companies. NCSA collaborates with the government, corporate, nonprofit and academic sectors. Its mission is to build strong public/private partnerships to create and implement broad-reaching education and awareness efforts to empower users at home, work and school with information to keep themselves, their organizations, their systems and their sensitive information safe and secure online and encourage a culture of cybersecurity. NCSA believes that securing our online lives is a shared responsibility.

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 Jan. 28; and National Cyber Security Awareness Month, launched every October. For more information on NCSA, visit staysafeonline.org/about.

EVERY SIDE OF
CYBER

Raytheon