Viewpoint

ENGAGING MENA MILLENNIALS IN CYBERSECURITY CAREERS

NOVEMBER 2019

Authors:
Souheil Moukaddem
Ziad Antoine Nasrallah
Rosemary Mosquea
Casey O’Conor
Dr. Jamie Lopez
INTRODUCTION

The digital environment has created opportunities and driven progress for societies globally but has also opened a new frontier for malicious cyber activity. The cybersecurity workforce continues to face difficulties in keeping pace—there is a current gap of 2.9 million cybersecurity workers around the globe. Attention turns to the millennial generation, which comprises more than 50 percent of the labor force and will be responsible for securing our networked nations over the coming decades. This is especially true within the Middle East and North Africa (MENA), a region with one of the world’s youngest populations, highest youth unemployment rates, and ongoing cybersecurity threats. Millennial participation in the cybersecurity sector in MENA will be required to address the challenge of securing cyberspace; an increasingly vital component of the stability of infrastructure, businesses, governments, and economies. Against this backdrop, this Viewpoint considers factors known to influence the career choices of MENA millennials and outlines potential solutions for government, employers, and academia to attract potential millennial talent to the cybersecurity profession.

The cyber landscape increasingly influences many aspects of our lives as technology and the internet penetrate the way we socialize, purchase goods, maintain our health, and much more. In 2018, the United Nations (UN) estimated that internet usage would reach 3.9 billion global users by the end of that year, which is over half of the world's population. This reality is particularly salient in MENA, a region that boasts one of the world's highest internet penetration rates and youngest populations. Perhaps most notably, Kuwait, Bahrain, the United Arab Emirates (UAE), and Qatar report internet usage in more than 90 percent of households, as shown in Figure 1. These internet usage rates rank in the top 5 percent of developing countries.

As the internet expands and connectivity speeds increase, there are a growing number of commercial and consumer uses for digital technology. We no longer require static hardwired desktops but now have on-demand access to mobile smartphones and a range of internet-enabled and interconnected devices, the ecosystem that we call the internet of things (IoT). This will only be magnified further as nations move from third- and fourth-generation networks to new fifth-generation service (i.e., 5G).

The societal shift toward an increased use of digital technology and greater connectivity is evidenced in Abu Dhabi’s Vision 2021, Saudi Arabia’s Vision 2030, and Kuwait’s Vision 2035. These transformation strategies envision a rapidly growing digital infrastructure enabling economic development at a national level. Ambitious plans have been set for technology to play a crucial role in these transformations, helping to support nation building, diversified economies, and a sustained culture of innovation. As a recent example, the UAE became the first nation to appoint a Minister of State for Artificial Intelligence after releasing its Strategy for Artificial Intelligence, a document that dictates a fast adoption of such technologies. Leading technology companies are also taking note of the digital growth in MENA and the opportunities that it brings. Recently in 2019, Microsoft announced new data centers in Abu Dhabi and Dubai. Shortly thereafter, Amazon Web Services (AWS) launched three new data centers in Bahrain that will connect MENA to its global network.

The Gulf States have also seen an increased usage of e-government services through digital platforms, especially in Saudi Arabia and the UAE. According to the UN e-Government Development Index, each of these aforementioned Gulf States ranks in the upper quartiles globally and continues to trend upward. Saudi Arabia, for instance, moved from a global ranking of 50 in 2004 to 32 in 2018, while the UAE ranked 21st overall in 2018. This expansion of the cyber landscape brings opportunity but also a new open system of data and information that may have downstream impacts that must be monitored.

Figure 1. Percentage of Individuals Using the Internet
The continued expansion of technology and interconnected systems, as seen in examples such as digital banking, smart homes, and supervisory control and data acquisition (SCADA) systems, create an expanding attack surface vulnerable to exploitation by threat actors. This expanding attack surface is already difficult to secure and will, following Moore’s Law, continue to become exponentially challenging as quantum-powered computing becomes more prevalent. Furthermore, unlike many traditional threats, cyber-attacks are often agnostic to the geography of the threat source—the ecosystem is so interconnected that threat actors can be distanced and hidden and still infiltrate a system while remaining undetected for extended periods of time.

MENA nations have experienced significant targeting due to the rising threat of state-sponsored actors looking to assert or expand regional influence and power. Many of these attacks continue to be carried out by large nation-states targeting government, military, and critical national infrastructure assets. Some of these attacks have persisted for multiple years, seeking to obtain sensitive information, monitor specific individuals, or continue influence operations in targeted countries to promote unrest. Such attacks usually have larger strategic objectives impacting economic, geo-political, or national defense structures. For instance, when cyber-attacks compromise actual weapons platforms or command and control systems (e.g., C4ISR), a nation’s ability to defend its citizenry in a kinetic conflict is called into question. Despite an increased number of cyber and physical security measures implemented across government systems, the threat remains real. Several organizations in Saudi Arabia, including the Ministry of Labor, reported they had been attacked by a recurrence of the same sophisticated malware virus that crippled two-thirds of Saudi Aramco’s computer network several years ago.1 In this more recent attack, Saudi Arabia’s Computer Emergency Response Team (SA-CERT) became publicly involved in the incident response and remediation efforts and acknowledged the severity of the threat. Commercial companies in MENA have also been a priority target as evidenced by the recent cyber-attacks against Saipem and Petrofac, two leaders in the oil and gas industry, as shown in Figure 2. Likewise, the financial services sector remains a priority focus for cyber-attacks because of the potential for compromising sensitive financial data and systems, which would ultimately call the integrity of the financial system itself into question. Attacks like these can, and are often intended to, have dire consequences for a nation’s economy.


Figure 2. Consequences of Recent Cyber Attacks in MENA
Cybersecurity Talent Shortage Impacts MENA’s Ability to Address the Cyber Threat

Cyber-attacks are complex and evolving, and as such, programs require cutting-edge solutions and highly skilled people to protect assets, information, and services across the entire cyber ecosystem. There are several efforts globally, and in MENA more specifically, to advance cybersecurity technology and stay one step ahead of the adversary. Unfortunately, it is the people dimension of cybersecurity that remains a consistent challenge. The availability of professionals with the cybersecurity acumen required to protect critical assets is not keeping pace with rising threats. This trend has been known for some time; however, the gap continues to widen. The latest estimate is a global shortage of 2.9 million cybersecurity professionals.7

In a similar study conducted by Frost & Sullivan in partnership with (ISC)² and Booz Allen Hamilton, it was reported that approximately two out of every three professionals claim to have too few cybersecurity workers in their department. In MENA this gap is noted to be more pronounced for three reasons—leadership lacks understanding of cybersecurity requirements; business cannot support new staff; and qualified talent is hard to find.8

Research also revealed a startling mismatch between what hiring managers are looking for and what potential employees are prioritizing for a successful career. Specifically, workers were reported to have placed higher emphasis on technical skills (e.g., cloud security, incident response) when in fact hiring managers prioritized competencies such as communication and analytical skills as the most critical. The difference in expectations is making it more difficult for the labor force to respond to the current demands of employers; and in turn, this requires solutions to improve the alignment of the supply and demand. These underlying issues, without immediate intervention, will continue to persist and likely grow. These challenges are compounded by the fact that workforce vacancies in MENA, especially in the Gulf, are often filed by an expatriate labor pool, third-party vendors, or even overseas partners (off-premises). Where sensitive data and systems are concerned, such offshoring may result in additional risk being inserted into the cybersecurity ecosystem. As such, governments and enterprises must continue to address the cybersecurity workforce shortages with local, innovative, and comprehensive solutions.

AN OPPORTUNITY FOR THE MILLENNIAL GENERATION WORKFORCE

Given the persistent cybersecurity talent shortage, this Viewpoint will address the potential for MENA millennials, a generation that continues to dominate the labor force, to address this shortage. To better understand the potential for MENA millennials to help remediate the cybersecurity supply gap, Booz Allen has examined the foundational demographics, motivators, and preparedness of this group.

The population in MENA has increased significantly over the past several decades and stood at roughly 450 million in 2018. The millennial generation in MENA comprises approximately one-third of the total population and more than 50 percent of the labor force. They were born between the years of 1982 and 2000, making the current age range 19–37. Still, many challenges remain in harnessing their yet untapped full talent potential—millennial unemployment in MENA countries continues to be the highest in the world, at more than 25 percent in 2018.1 While there have been several efforts aimed at resolving unemployment over the past decade, the challenge persists because of inconsistent implementation of labor initiatives, further compounded by the financial crisis, the fall in oil prices, and ongoing geo-political conflicts in the region. Nevertheless, there is opportunity to better target this population of the labor force, many of whom are looking for work, and attract them to the cybersecurity profession in need of talent.

DEMOGRAPHICS

Although there is some variation across the Middle East (e.g., Gulf states compared to North Africa), this group of MENA millennials has expectations that influence the education and careers they pursue, which ultimately impacts the way they work, collaborate, and communicate. The top priorities for millennials in MENA include the ability to continuously learn, to have a successful career, and to have a long and healthy life. These preferences also directly influence the jobs and careers millennials pursue. The top motivators that encourage loyalty to an organization include good work-life balance, training opportunities, fairness in salary/remuneration, and work that is engaging/interesting (refer to Figure 3).10 Those factors that are most concerning include lack of career development; a job that does not match personality, work style, or preferences; and inability to realize career goals.

The cybersecurity profession aligns well with many of the common motivators for MENA millennials. For instance, the profession is often known for prioritizing continued professional development for valued industry certifications (e.g., CISSP, GCIA, CISA), offering engaging work that evolves to keep pace with an ever-changing threat landscape, career progression opportunities, and highly commanded salaries. This suggests that there is an opportunity to match the shared traits of MENA millennial work motivators and attributes of the cybersecurity profession to develop attractive cybersecurity recruitment plans and career paths.

MOTIVATORS

PREPAREDNESS

While we have noted that cybersecurity jobs are available and that the cybersecurity profession may align with MENA millennial career motivators, a fundamental question still remains—is this group of millennials prepared for the job responsibilities required of the cybersecurity profession? General evidence shows that talent in MENA continues to face uphill challenges in entering the workforce. While general school enrollment and literacy rates have increased in recent years, graduates still tend to demonstrate a lower level of preparedness for the skill demands of employers.11 In turn, employers often turn to on-the-job upskilling and training to ensure that employees meet the required performance standards.

Upskilling workers is a common approach in the global cybersecurity profession. In fact, on a scale of most important factors for employment, a cybersecurity-related degree was ranked much lower in value than relevant experience or cybersecurity certifications often earned in parallel with job training. The implication being that cybersecurity degrees alone are not sufficient evidence of cybersecurity skill acquisition. Data also shows that 80 percent of cybersecurity workers in MENA started in a non-cybersecurity career before switching into a cybersecurity role. This suggests that although most MENA millennials may not be immediately ready for a cybersecurity career from a skills acquisition standpoint, this should not preclude them from such a career because it has been shown that they can learn the field through experience. Furthermore, given the age range of millennials, many have been immersed in technology since birth. As digital natives, many are tech-savvy enough to quickly acclimate and evolve into a cybersecurity occupation with the appropriate formal and on-the-job training.

5. Booz Allen Hamilton proprietary information.

Figure 3. Top Motivators Which Encourage Loyalty to an Organization
Effective cybersecurity workforce programs require the coordination of multiple stakeholders, including government, employers, and academia (refer to Figure 4). In theory, the cycle is simple: government provides the workforce framework, policy, and incentives; employers drive cybersecurity capability development and job requirements; and academia cultivates the skilled and qualified talent the market requires. In isolation, each of these stakeholders has an essential part to play within the cybersecurity ecosystem, but it is in combination that their impact is most powerful.

Stakeholders should take into consideration the previously described factors that influence the career decisions of millennials. These factors can be used as the catalyst for driving the talent pool toward the profession. Based on our analysis, we put forth recommendations, shown in Figure 5, to engage MENA millennials in cybersecurity careers with a focused employee value proposition.

**Figure 4. Stakeholder Collaboration Model**

**Figure 5. Recommendations for Engaging Millennials in Cybersecurity Careers**
Using these recommendations, it follows that cyber workforce initiatives should be specifically crafted for millennials. In Figure 6, we have put forth nine initiatives that will chart a way forward for stakeholders, working together, to harness millennial talent and engage them in cybersecurity careers.

**PROPOSED INITIATIVES FOR ATTRACTING AND DEVELOPING MILLENNIALS FOR THE CYBERSECURITY PROFESSION**

**GOVERNMENT**
- Develop a national cybersecurity career framework
- Design interdisciplinary cybersecurity curriculums

**EMPLOYERS**
- Identify risk-based and adaptive workforce needs
- Tailor the employee value proposition
- Offer experiential cybersecurity learning

**ACADEMIA**
- Foster connections between students and employers
- Adopt ‘Hire-the-Train’ strategy

**I. PROFESSIONALIZED CYBERSECURITY CAREER MODEL**

**GOVERNMENT**
**DEVELOP A NATIONAL CYBERSECURITY CAREER FRAMEWORK**
Government should develop a National Cybersecurity Career Framework to establish a consistent taxonomy that defines cybersecurity workers across sectors and cybersecurity functional areas. The framework should also include guidelines for how to identify, recruit, develop, reward, and retain a cybersecurity workforce. For success, the framework should be built to reflect the learning styles and career preferences of millennials because they constitute a large percentage of the cyber talent pool. Similar frameworks exist globally, such as the U.S. National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. In addition, the framework can provide transparency in career advancement opportunities to attract millennials who desire clear direction and defined ways forward to advance their careers.

**EMPLOYERS**
**IDENTIFY RISK-BASED AND ADAPTIVE WORKFORCE NEEDS**
Leading cybersecurity programs often adopt a risk-based and adaptive approach that is informed by the degree to which their most valued assets are vulnerable to potential threats. Advances in artificial intelligence and integrated data analytics are making adaptive cybersecurity models, which can respond to new threats in real time and correlate valuable information about attackers, more feasible than ever before. In turn, dynamic cybersecurity controls and resources are put in place to mitigate against the identified non-static risk. Employers must use this risk-based and adaptive understanding of their cybersecurity requirements to inform what is needed of their cybersecurity workforce. Specifically, risk reports can be translated into mapping the types of capabilities (e.g., incident response), teams (e.g., multifunctional), competencies (e.g., analytical thinking), and positions (e.g., forensic analyst) that are in most demand.

**ACADEMIA**
**DESIGN INTERDISCIPLINARY CYBERSECURITY CURRICULUMS**
The cyber domain is complex. The most dangerous threats are often multifaceted, taking different vectors to achieve malicious objectives. This complexity typically includes a technical dimension that exploits interconnected systems, devices, and networks and is compounded by the risk of human threat actors exploiting known human behavior (e.g., phishing attacks via email). To establish a workforce capable of responding to such multidimensional requirements, academic cybersecurity curriculums should be interdisciplinary. Curriculums should seek to develop the technical skills and technology familiarity required of a cybersecurity analyst; teach the non-technical concepts of ethics, law, regulation, policy, and governance; and expand the broader social skills that are uniquely critical for understanding the human behavior that drives threat actors and malicious intentions.

---

**Figure 6. Initiatives to Address Cybersecurity Workforce Gap**
II. MOTIVATION-BASED RECRUITMENT

GOVERNMENT
DEVELOP CYBER AWARENESS AND RECRUITMENT CAMPAIGNS
Although millennials may compose half of the MENA labor force, the cybersecurity community has not adequately tapped into this supply of available resources. Government should improve its understanding of, and outreach to, this future supply pool of talent. National workforce mapping of MENA millennials could provide visibility into which locations have the highest density of future cybersecurity workers and the level of competition for hiring talent in that region. For example, the National Institute of Standards and Technology (NIST) developed a software tool called CyberSeek that provides detailed actionable data to employers, defining how large the cybersecurity workforce is in a particular region, the average cost of such workers in the region, and the level of difficulty to source particular cybersecurity positions. Subsequently, tailored cybersecurity career awareness campaigns should be focused on these talent centers with higher numbers of millennials. Recruitment messaging should seek to generate interest in cybersecurity careers by highlighting the career options and career benefits of joining the cybersecurity field.

EMPLOYERS
TAILOR THE EMPLOYEE VALUE PROPOSITION
The career motivators for millennials are highly compatible with the realities of the cybersecurity profession. Organizations should use this information to formulate their employee value proposition cognizant of millennial career motivators. For example, millennials have demonstrated a tendency to switch employers instead of remaining with one employer for life. This can be capitalized on by cybersecurity employers by emphasizing opportunities to learn about various parts of the cybersecurity industry through job rotations and offering a transparent career advancement plan with multiple paths forward. Employers should also emphasize the workplace benefits that would most pique the interest of MENA millennials, such as employer-sponsored training, exposure to leadership at their organizations, and opportunities to participate in interesting, meaningful, and rewarding projects.

ACADEMIA
FOSTER CONNECTIONS BETWEEN STUDENTS AND EMPLOYERS
Universities and primary schools should provide students with greater levels of access and opportunities to the cybersecurity industry that translate to future cybersecurity employment. Students will benefit from increased understanding of the expectations of a cybersecurity career and job opportunities. Such understanding and insight can come from career counselors who are well-versed in the cybersecurity job market; employer career fairs; and student participation in cybersecurity industry events, trade shows, surveys, studies, and research programs.
III. CYBERSECURITY WORKFORCE CAPACITY BUILDING

GOVERNMENT
CREATE A LOCAL CYBERSECURITY CORPS WITH SCHOLARSHIP PROGRAM
While off-premises cybersecurity solutions may be common and expedient, they do come with risk. MENA organizations are rightfully concerned about the confidentiality of their data when it leaves their network and is accessed by foreign companies. To alleviate this risk, MENA governments must build a robust Government Cybersecurity Corps of local nationals that can be more readily trusted with sensitive data. This corps should be recruited early in school to be given the proper exposure to such opportunities at an early age, and then incentivized with education scholarships and selective government cybersecurity opportunities when they become of age. Government scholarship programs can be effective at attracting skilled cybersecurity talent for a broad range of cybersecurity roles. As an example, the Cyber Security Agency of Singapore (CSA), Government Technology Agency (GovTech), and Infocomm Media Development Authority (IMDA) sponsor the Smart Nation Scholarship for Singapore citizens or permanent residents with the intention of taking on citizenship. These scholarships encourage the development and nurturing of technology talents, and future leaders in public service, by providing comprehensive tuition and living allowances for awardees with 4–6 years of required government service.14

EMPLOYERS
ADOPT A “HIRE-THEN-TRAIN” STRATEGY
While millennials are often thought of as tech-savvy, very few report receiving adequate technical skills or cybersecurity knowledge (e.g., security architecture, incident triage) in formal education programs. Consequently, organizations should adopt a “hire-then-train” strategy as opposed to a “hire-for-certs” approach. They should offer benefits for employees to obtain advanced technical certifications after they have been hired. These training programs should also reflect the need for cybersecurity functions to be fulfilled by teams with diverse skill sets and should be coupled with efforts to grow junior employees through apprenticeships, formal on-the-job shadowing, and monitored performance that provides real-time feedback as they carry out their job duties.

ACADEMIA
OFFER EXPERIENTIAL CYBERSECURITY LEARNING
Schools must not only embed cybersecurity into the classroom but also offer students experiential cybersecurity learning programs. This can be offered through lab simulations, cyber ranges to exercise red/blue team scenarios, or cybersecurity competitions. Such an example is the UK CyberFirst Girls Competition, which provides a fun but challenging environment to inspire the next generation of women to consider a career in cybersecurity. In 2019, more than 3,000 teams from nearly 850 schools participated. Each team is guided by a mentor, often a teacher, through a set of competitive activities across the areas of cybersecurity, coding, and computer networking.15 There should also be opportunities to practice applying skills with cybersecurity employers. One such program would integrate co-op internships into a school’s cybersecurity curriculum. In a program like this, students would alternate semesters of academic study with semesters of employment with a cybersecurity employer. This process would include guided instruction and mentorship from both an academic advisor at the school and a mentor or manager in the workplace.

The increased usage of interconnected digital technologies, the rising number of cybersecurity threats, and the insufficient local workforce to address those threats constitute growing challenges in the MENA region. Governments and enterprises must be able to respond to such threats with a workforce equipped to prevent, identify, and respond to cyber-attacks.

This can be done by attracting MENA millennials to join the future cybersecurity workforce and can be bolstered through better engagement and preparation of this generation. This includes examining the generational preferences, designing targeted cyber-awareness campaigns, improving the cybersecurity employee value proposition, adopting hire-then-train strategies, and better engaging this generation through government, employer, and academia collaboration.

Establishing a well-equipped and skilled cybersecurity workforce comprising highly engaged millennials is a direct means to protect national security, business operations, information, brands, and finances. As such, all stakeholders must make sure they are contributing to efforts that are engaging millennials in the cybersecurity profession as a means to close this critical workforce gap.

CONCLUSION
Souheil Moukaddem is an Executive Vice President at Booz Allen Hamilton, leading the firm’s work and organizational growth in the MENA region. In his position, Souheil plays a pivotal role in driving the firm’s strategic decision-making in the region. A Booz Allen stalwart for over a decade, Souheil has solid experience in Organizational Design and Implementation, having worked with both commercial and government clients to provide best-in-class processes and procedures, reduce their business risk and allow them to better compete in the global marketplace. Steering the firm’s operations in the MENA, Souheil brings extensive expertise in a variety of other areas, including vision and mission, strategy, governance, process improvement, human capital, and change management.

Ziad Antoine Nasrallah is a Principal at Booz Allen Hamilton and a leader within the firm’s international cybersecurity practice. He draws on more than 17 years of strategy and business experience, gained through numerous consulting engagements across North America, the Middle East, and Africa.

Casey O’Conor is a Senior Associate with Booz Allen Hamilton and a capability leader focused on building and deploying management consulting teams to solve complex challenges facing clients across the globe. He has served over a dozen major client projects as a consultant in the U.S. and international markets, including significant work in the Middle East and North Africa (MENA) region.

Dr. Jamie Lopez is a Senior Associate at Booz Allen Hamilton and leads the U.S. Based International Strategy Consulting Team as well as the International Cyber Human Capital Portfolio. He brings over 17 years of management consulting experience across the commercial and government sectors. Dr. Jamie has led enterprise and national level cybersecurity talent strategy, framework development, skills assessment and workforce planning engagements as well as large scale cybersecurity baselining and benchmarking studies. Jamie’s functional specialization is in human capital strategy, organizational development, change management, talent assessment and workforce planning.

Authors:
Souheil Moukaddem
Executive Vice-President
moukaddem_souheil@bah.com

Ziad Antoine Nasrallah
Principal
naarallah_stad@bah.com

Rosemary Mosqua
Principal
mosqua_rosemary@bah.com

Casey O’Conor
Senior Associate
casey_casey@bah.com

Dr. Jamie Lopez
Senior Associate
lopez_jamie@bah.com
About Booz Allen

For more than 100 years, military, government, and business leaders have turned to Booz Allen Hamilton to solve their most complex problems. As a consulting firm with experts in analytics, digital, engineering, and cyber, we help organizations transform. We are a key partner on some of the most innovative programs for governments worldwide and trusted by their most sensitive agencies. We work shoulder to shoulder with clients, using a mission-first approach to choose the right strategy and technology to help them realize their vision. With global headquarters in McLean, Virginia and more than 80 offices worldwide, our firm employs more than 26,400 people and had revenue of $6.7 billion for the 12 months ending March 31, 2019. To learn more, visit BoozAllen.com. (NYSE: BAH)