Closing The Gap In The Cyber Skills Domain

WORLD GOVERNMENT SUMMIT 2023

in collaboration with Deloitte
# Table of contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>04</td>
</tr>
<tr>
<td>Section 1: The Strategic Context - A Technology- Driven World</td>
<td>06</td>
</tr>
<tr>
<td>Section 2: Cyber Capability Building - National Challenges And Solutions</td>
<td>10</td>
</tr>
<tr>
<td>Workforce Trends Influencing CISOs Today</td>
<td>18</td>
</tr>
<tr>
<td>The Changing Faces Of Cybersecurity</td>
<td>22</td>
</tr>
<tr>
<td>A Triple Helix Approach To Addressing The Cyber Human Capital Challenge</td>
<td>34</td>
</tr>
</tbody>
</table>
Executive Summary

The modern world is being shaped by extraordinary technological transitions and digital innovation. This remarkable pace of change is being fueled in part through rapid expansion and exponential growth of the digital space. These changes, according to the World Economic Forum (2016) are fueling what is being called the Fourth Industrial Revolution, where digital technology, the Internet of Things (IoT), and cyber-physical systems will come to impact every facet of life as we know it. Today, already well down the path of the Fourth Industrial Revolution, we stand at an inflection point. Artificial intelligence (AI) and machine learning (ML) coupled with developments in computing, modern digital design, and manufacturing, are propelling a new IoT which is globally and instantly interconnected through the internet, the World Wide Web, and beyond. Digital transformation has taken center stage and cannot be evaded. What has been coined as ‘the cyber world’ surrounds everything we do. It encompasses our work life, our daily living practices, and even our social activities.

However, along with its extraordinary advantages comes its anticipated perils, faults, and challenges. How can the world effectively protect its best interests in such a complicated digital/cyber domain?

Compounded with the aforementioned challenges, we have come to realize that we are neither fully equipped to culturally or technically exploit these opportunities, nor are we able to effectively defend ourselves from the threats that come along with it. It is at this point that we are obliged to emphasize the potential cyber threats of our time, and work on equipping ourselves to fight them. Cybersecurity, which in essence refers to the practice of safeguarding complex critical systems and sensitive data from digital attacks, is an area of expertise that is invaluable nowadays. So why are we still so ill-equipped in the cyber skills domain and where should the focus be placed in to close in on this impending cyber skills gap? The time has come to look towards our education system as a necessary starting point. Ironically considering everything has already gone digital, global education systems are predominately geared towards the 3 classic Rs (reading, writing, and arithmetic), rather than science, technology engineering, and mathematics (STEM).

Unfortunately, we continue to view digital skills as a specialty geared mainly to tech-savvy individuals. The skills gap has created a burgeoning industry for cybersecurity but is struggling to match expansion in vulnerabilities generated from the dynamic and well rewarded digital and software-driven growth.

If there is one certainty in this picture, it is that the use of AI and ML by adversaries will exponentially increase vulnerabilities across the digitally integrated future world, unless there is a fundamental reboot of our educational focus to align it to the world of today by going beyond simply adding courses and training. We need to witness a new shift in the inclusion of foundational skills and aptitudes that we teach to future generations. A failure to focus on, and invest in, secure digital education will create an accelerating and unmanageable risk to the prosperity and security agendas of every state and nation across the globe. Secure software and coding must become a core skill taught from early childhood through high school as a required part of the curriculum alongside
the classic subjects of reading, writing, and arithmetic. By embedding awareness, skills, and consequences of online learning, working, and socializing throughout the educational system, innovators and the workforce of the future will create a convergence, rather than a divergence, in digital opportunity and security. The clock is ticking: now is the time to take full action.

Across the full spectrum of academia, government, and the private sector, we are seeing movement towards shifting enterprise, regional, and national educational systems and awareness, yet the pace of change is well behind the technological developments needed to protect from the digital world’s most neglected threat: humans. Leadership in government needs to step up the efforts to change educational paradigms and improve long term outcomes; this will require reimagining the educational system for children, adults, and lifelong learners. Even for individuals that may not directly be involved in the development, administration, or application of advancing digital technologies, this is the only way to counter the weakest link in the system: the human being.
Section 1

The Strategic Context - A Technology-driven World
Today as the world edges towards what some are already labeling the Intelligent Age, we are still struggling to come to terms with changes that occurred in the mid-20th Century and the evolution of the information enabled society that has been commonly referred to as the Information Age. The Information Age was characterized by open and rapid data-sharing, social media-driven utilization of personal data (often for advertising), and integration of knowledge systems. Information became the new oil, according to one truism of the times. It is evident how societies are struggling to adapt and adapt to these characteristics even as they are now becoming outdated. The Intelligent Age is best characterized as one where every human works with an intelligent machine in hand during just about every activity. It merges the digital, physical, and human worlds, collaborating across the boundaries of each to improve performance, and empower smarter humans to achieve more at incredible speed. The key phrase here is incredible speed; this accelerated intelligent enhancement threatens to disrupt the adoption of Information Age thinking and derail preparations for the future. In a cybersecurity context, this provides both a business threat and an opportunity to disrupt slower-moving competitors, providing organizations the ability to explore and exploit these new technologies through a combination of agile and courageous leadership supported by an adaptive and skilled workforce.

While it would be close to arrogant to suggest that the generations in or about to enter the workplace of today are part of a transformation that transcends anything before it, the pace of technical innovation, coupled with the adoption of AI, ML, and robotics all integrated through the IoT is already driving a profound shift in how nations and states position for and will pursue their future prosperity agendas. While traditional maritime and land trade routes may still underpin the physical movement of goods, the internet is now at the heart of how populations, businesses, and governments do their business. At the heart of this global business are data and software; whether in industrial control systems (ICS), financial transactions, social media, or navigation systems, it is now impossible to function in the grid without some form of direct connection to both data and software.

Against this background, it is only natural for a specialist industry, such as that of cybersecurity to emphasize its own sector specific concerns and suggest mitigations regarding such dependencies for the public good and for business growth. However, such an evident claim misses a profound truth underlying the circumstances the global community faces today. The ability to develop and exploit data and software is now at the heart of any nation’s future prosperity agenda; expertise in these skills will fuel a nation’s prosperity as well as create dependencies and vulnerabilities for others to exploit. Faced with similar needs in the First Industrial Revolution, nations introduced subjects such as mathematics, reading, and writing because without these skills, the opportunities that were emerging could not be exploited. Without a baseline of foundational skills delivered through an established and managed educational system, the ability to generate the necessary workforce capacity and capability required to realize the potential and demands of the new workplace would have been a chimera.

These days, the world faces a similar tipping point; without digital literacy or deep expertise in securing the digital transformation of our nations, societies will be dislocated from the very essence of their future security and prosperity agendas. Currently the World Economic Forum points to a global cybersecurity workforce gap of nearly three million. At the same time, there is mounting concern in terms of the talent gaps that exist in industries across AI, data science, and a range of other critical technology sectors. It is important to emphasis how the key here is that the gap is not purely a numbers game, but rather more of a reflection of an increasingly constraining mismatch between...
the skills and aptitudes required by industries. While the world of cybersecurity might focus on the three million gap, the worlds of AI, computing, and communications are being impacted by proportionately similar scales of shortage - all are victims to the demands of a fundamental workplace shift towards data and software.

The acceleration in technological innovation and value realization through adaptive combinations of technology AI, human teaming, and software development, is also often driven by speed to market factors, which are accelerating the lag in security awareness and governance. This will exacerbate a growing divide between innovation and cybersecurity. Similar to the phrase that “it is better to treat the source of an injury rather than the symptoms,” societies should recognize that in order to create a manageable cybersecurity landscape, secure by design coding and software awareness must become part of the cradle to grave school curricula, and therefore, children should be introduced to digital literacy and its secure and safe usage at a very young age.

"Without digital literacy or deep expertise in securing the digital transformation of our nations, societies will be dislocated from the very essence of their future security and prosperity agendas"
Section 2

Cyber Capability Building - National Challenges And Solutions
World governments have been actively trying to address the shortages of skilled cybersecurity workers through various programs and initiatives. In many cases, countries have even created specific residency visa programs to attract such skilled professionals in a very limited labor market. Further a number of government entities have been adapting cybersecurity skills and workforce frameworks to try to create learning pathways, and support and promote adult students in seeking cybersecurity careers.

The United States, for example, introduced the National Initiative for Cybersecurity Education (NICE) Framework, which outlines seven categories of cybersecurity functions, 33 specialty areas, and 52 distinct work roles. The NICE Framework was the first attempt at scale to help shape the cybersecurity workforce by defining the knowledge, skills, and abilities needed across the multitude of roles.4

The European Union Agency for Cybersecurity’s (ENISA) European Cybersecurity Skills Framework (ECSF)4 was established to define the relevant roles, competencies, skills, and knowledge in the cybersecurity field across 12 profiles, which outline the general responsibilities, skills, synergies, and interdependencies.5 The framework was designed for employers, education providers, and government entities to understand the specific skills, training, and technical competencies needed across their workforce.

Other examples of cybersecurity skills frameworks can be found in the Australian Signals Directorate (ASD), a joint effort in Singapore with the SkillsFuture Singapore (SSG), Workforce Singapore (WSG), and the Ministry of Home Affairs (MHA), plus additional national efforts underway such as with the United Kingdom Cyber Security Council (UKCSC). Each of these national efforts are focused on adult and continuous learning models that will help build a skilled cyber workforce and reduce the number of vacancies. Such models are designed to identify the required cyber workforce skills and roles, and guide individuals and organizations in educational, training, and experiential development.

There are a number of disjointed efforts that are driving science, technology, engineering, and mathematics within populations around the world. Within these are also a number of programs to include the US Cyber Challenge (USCC), which aims to serve as a “premiere program to identify attract, train, recruit, and place the next generation of cybersecurity professionals into the workforce.”6 The USCC originated out of a contract with the Department of Homeland Security (DHS) through the Center for Internet Security (CIS), but now operates as a non-profit organization that sponsors a number of Cyber Quests and Camps. However, like most adult learning programs, it only targets a limited set of individuals rather than being embedded within a standardized educational paradigm.

Another collaboration under the designation K12CS (the K-12 Computer Science Framework) has brought together a number of teaching and computer science associations to design and draft curriculum to embed concepts of computer and data science, cybersecurity network engineering, algorithms, and programming into the K-12 curriculum.7 Again, another noble effort, but one that is not scaled to a national level that looks to make these concepts a core component of the overall curriculum for all students.

"The UK has developed guidance, resources, and opportunities for schools and students that are interested in cybersecurity, and a couple of programs that support the next generation of students to build their cyber capabilities"
The UK and the US, particularly, are forming guidelines to embed cybersecurity within their education system. The National Cyber Security Centre (NCSC) in the UK, for example, has developed guidance, resources, and opportunities for schools and students that are interested in cybersecurity and a couple of programs that support the next generation of students to build their cyber capabilities. In the US, the Cybersecurity Education and Training Assistance Program (CETAP) was formed, which aims to improve the cybersecurity workforce and literacy by providing educational content to every K-12 student within the US. Moreover in 2018, Deloitte Romania and EC-Council collaborated to create cyber content to be added to the educational curriculum that fit the needs of securing the usage of digital devices and identity to prepare graduates for the job market and bridge the gap between the educational system and workplace requirements, several businesses are setting up apprenticeship programs and on-the-job trainings. In the Middle East, Deloitte’s BrightStart program, for example, offers a unique opportunity for growth and enrolls graduate students to launch their training and professional careers in cybersecurity at the firm.

The challenges of starting future generations on a pathway for success cannot be understated. Collectively government bodies focus on education needs to reassess their entire curriculum requirements and design, with the stated goals of adopting systemic changes that will better prepare future generations of children for the challenges the world faces in cybersecurity. The Organization for Economic Co-operation (OECD) has investigated the challenges in producing technically competent students, while also addressing global inequities though the embodiment of agency in students to help drive future generations as part of the learning system. According the OCED 2018 Learning Framework 2030 report, the OCED finds that the “rapid advance of science and technology may widen inequities, exacerbate social fragmentation, and accelerate resource depletion”. Building on the knowledge, skills, abilities, and values that will be needed during and beyond the Fourth Industrial Revolution and

“in the cyber domain demand equitable access to education to ensure the future security in technology and a sustainable future."
The European Union Institute for Security Studies (EUISS) recently examined the role that coordination and international cooperation plays in the development of cybersecurity and technology skills. Their findings found a world that is highly siloed across cyber capacity building (CCB) projects, where individual countries and their respective government bodies, private companies, and not-for-profit entities are working on primarily self-interested objectives. Solving a global concern will take a global coordinated effort. While there have been a few international agreements on coordination in developing cybersecurity capacity, in practice, the level of coordination remains fragmented at best. There is competition for limited funds, lack of equity in projects, lack of focus all around; in many cases, there is simply an absence of such initiatives, particularly in least developed countries. The EUISS study also noted that what started out as an international effort to reduce cybercrime, has now expanded its remit to include incident response, protecting critical national infrastructure, strategic planning, public awareness, skills for the workforce, diplomacy, and even more broadly complex digital issues and manipulation of political outcomes across digital platforms.

One of the notable perspectives of the EUISS study was the need to have a greater level of responsibility and global engagement through the Global Forum for Cyber Expertise (GFCE). As one of the recommendations made by the authors, it was noted that the GFCE should continue to expand their role in cyber capacity building and coordination through the various exchanges, such as their annual conference with the World Bank, the World Economic Forum, and the Cyber Peace Institute. Furthermore, they felt the GFCE should continue supporting coordination and sharing knowledge amongst CCB practitioners as a high priority.

There is a strong growing focus on the development of cybersecurity curriculum within the global collegiate and university systems to include two-year trade schools, bachelor’s, graduate, postgraduate, and certificate programs. The National Security Agency (NSA) of the United States has established a program called the National Centers of Academic Excellence in Cybersecurity (NCAE-C), which is managed by NSA’s National Cryptologic School. The NSA collaborated with a number of federal partners including the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), the National Institute of Standards and Technology (NIST)/National Initiative on Cybersecurity Education (NICE), the National Science Foundation (NSF), the Department of Defense Office of the Chief Information Officer (DoD-CIO), and the U.S. Cyber Command (USCYBERCOM), to aide in the development of a joint cybersecurity focused educational program for the nations, community colleges, colleges, and universities.

The NCAE-C program uses a three-category certification program, starting with Cyber Defense (CAE-CD); designation is awarded to regionally accredited academic institutions offering cybersecurity degrees and/or certificates at the associate, bachelor’s, and graduate levels. The second certification is designed to foster academic research; the Cyber Research (CAE-R) designation is awarded to Department of Defense (DoD) schools, PhD producing military academies, or regionally accredited degree granting four-year institutions rated by the Carnegie Foundation Basic Classification system as either a Doctoral University - Highest Research Activity Doctoral University - Higher Research Activity or Doctoral University - Moderate Research Activity. The third designation is focused on development of Cybersecurity Operations (CAE-CO); the CAE-CO program is designed around computer science, engineering, and technical applications for hands-on learning in laboratories or through cybersecurity exercise programs.
The CAE programs are focused on providing a uniform set of standards for cybersecurity curriculum and are built around specified competencies aimed at development for both students and faculty. The CAE program further builds on a concept of community outreach and leadership in professional development, and fully integrates cybersecurity practice within the institution across academic disciplines from computer science to engineering, and even business degrees. Further, the CAE program seeks to actively foster and develop solutions to growing challenges in the educational domain and the growing cyber threat landscape. These CAE-designated institutions must demonstrate leadership at the NSA by validation of their individual programs of study. The programs must provide designated study pathways, courses, degrees, and certificates that foster growth and development for learners through experience in obtaining their degrees and certificates in the cybersecurity disciplines. The CAE program is an example of national level coordination on development of cyber talent through the traditional college and university system.

In the European Union, the Cybersecurity Higher Education Database (CyberHEAD) provides a listing of 136 programs of study across 26 countries within the EU. CyberHEAD provides a single point of reference for students and citizens seeking to develop knowledge, skills, and abilities in the cybersecurity domain. The database aims to enable universities to attract high-quality students, and to connect with young talents seeking to understand the potential careers and higher education opportunities in cybersecurity. Colleges and universities can submit their individual programs of study for ENISA validation, which is based on a number of different requirements. Clearly, the program must be recognized or accredited by the EU Member State or an EFA Member State. From there, the level of specified modules within each program must include 25% of a bachelor’s degree in cybersecurity, 40% of a master’s degree focused on cybersecurity topics, and for postgraduate specialization programs, at least 40% of the taught modules must be in cybersecurity topics and have a minimum of 30 credits. Additionally, any programs that feature sufficient courses in cybersecurity might be eligible to be listed. The EU Joint Task Force on Cybersecurity Education defined the cybersecurity curricula in 2017, and the topics that might fall within the remit of the knowledge areas need to be listed in the database.

Across the Middle East and Gulf region, governments have established nationwide talent accelerators and cyber academies to empower the next generation capabilities in the field of advanced technologies, such as preparing cyber graduates for professional careers by offering them different learning channel programs, such as bug bounties, boot camps, and hackathons. Saudi Arabia’s National Cyber Authority (NCA) has created the Saudi Cybersecurity Workforce Framework (ScWF) to define the knowledge, skills, and abilities needed to build the cyber workforce and safeguard its national critical infrastructure in collaboration with high-priority sectors, government entities, and training providers. Several events and conferences focusing on innovation and research and development (R&D) are being delivered to connect cyber professionals with academia and industry as they work together in advancing knowledge and solutions around reducing the digital risk and human capital challenge in cyber. The United Arab Emirates has launched yearly events (e.g., cyber month and cyber week) to engage various stakeholders in celebrating cybersecurity highlighting the importance of cyber not only as a matter of national security but also to promote business resilience and community safety.

Despite the aforementioned focused attention on the cyber workforce skills gap on the national and international level, it is still unlikely that the world’s governments are going to be able to close the workforce gap or build a pipeline of talent capable of improving the situation. The reason for this stems partly from trying to bolt on skills to adults and college/university students.
“Across the Middle East and Gulf region, governments have established nationwide talent accelerators and cyber academies to empower the next generation capabilities in the field of advanced technologies”

as the primary solution; however, it is also related to the aforementioned speed and pace of technological change. Clearly, a revisioning of our fundamental educational system is urgently required.

In addition to the need to retool the educational system, regional and international coordination is much needed to effectively help drive cyber capacity building (CCB) on a much broader scale beyond these typical forums and institutions. World leaders need to look at a much broader spectrum including not only adult learning and CCB projects, but also cyber workforce development frameworks and learning pathways for cyber professionals. The need to open the aperture and initiate discussions about changes to global educational models needs to be addressed, incorporating the building of cybersecurity capacity and intellectual understanding at the beginning of the educational cycle, rather than only focusing on mature students. CCB coordination should include national and international educational regulatory bodies, academia, not-for-profit educational foundations and organizations, and international coordination bodies and organizations through the United Nations, EU, GFCE, OCED, and others. For example, the GFCE strengthens international cooperation on CCB by linking resources, expertise, and needs, and by offering practical knowledge to the global community. Working cooperatively is clearly the only way to tackle the growing global challenge.
Section 3

Workforce Trends Influencing CISOs Today
The shortage in cybersecurity talent is indisputable and estimated to be around 4.7 million according to the ICS2 study. The challenge is having a ripple effect within all sectors. Both public and private sector employers required more highly qualified employees, as cyber threats and complex attacks have become a significant risk for most organizations worldwide.

According to the Information Systems Audit and Control Association’s (ISACAs) State of Cybersecurity 2022 report, 73% of those surveyed are significantly understaffed and cybersecurity teams say their organizations have had difficulty retaining qualified cybersecurity professionals. This is an eight-point increase from last year which could be attributed to burnout from the pandemic.

Current cybersecurity workforce challenges include:

- Attracting graduates into the field of cybersecurity;
- Recruiting cybersecurity experts;
- Providing a culture that retains cyber employees (particularly with the new remote job demands post-pandemic); and
- Providing constant training.

The report also found that cyberattacks, staff retention, and staffing levels are somehow interconnected. 69% of respondents whose organizations were subjected to more cyberattacks in the last year reported being moderately or significantly understaffed. As a result, 70% of respondents, whose organizations experienced more attacks, were unable to retain qualified cybersecurity professionals.

Comparably based on research conducted by Deloitte Insights and National Association of State Chief Information Officers (NASCIO) in 2022, where a survey was shared with CISOs to provide insight on the current state of cybersecurity barriers, and taking into consideration that the same study was assessed two years prior in 2020, the lack of cybersecurity professionals and staff remained among the top five barriers with a substantial increase from 28% to 50% in two years.

![Figure 1: Inadequate Availability Of Cybersecurity Professionals Is Among The Top Five Barriers That CISOs Cite](source: 2022 Deloitte-NASCIO Cybersecurity Study and 2020 Deloitte-NASCIO Cybersecurity Study.)

<table>
<thead>
<tr>
<th>2020</th>
<th>2022</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lack of sufficient cybersecurity budget</td>
<td>Legacy infrastructure and solutions to support emerging threats</td>
</tr>
<tr>
<td>46%</td>
<td>52%</td>
</tr>
<tr>
<td>Inadequate cybersecurity staffing</td>
<td>Inadequate availability of cybersecurity professionals</td>
</tr>
<tr>
<td>42%</td>
<td>50%</td>
</tr>
<tr>
<td>Legacy infrastructure and solutions to support emerging threats</td>
<td>Inadequate cybersecurity staffing</td>
</tr>
<tr>
<td>34%</td>
<td>46%</td>
</tr>
<tr>
<td>Inadequate availability of cybersecurity professionals</td>
<td>Decentralized IT and security infrastructure and operations</td>
</tr>
<tr>
<td>28%</td>
<td>38%</td>
</tr>
<tr>
<td>Lack of dedicated cybersecurity budget</td>
<td>Increasing sophistication of threats</td>
</tr>
<tr>
<td>28%</td>
<td>29%</td>
</tr>
</tbody>
</table>
According to the CISOs responses, the top five identified barriers to cybersecurity that most organizations face as of 2022 are:

- Legacy infrastructure and solutions to support emerging threats;
- Inadequate availability of cybersecurity professionals;
- Inadequate cybersecurity staffing;
- Decentralized IT and security infrastructure and operations; and
- Increasing sophistication of threats.

As a result, the CISOs were taking into consideration the following to mitigate the risk:

- Transforming state employment practices to attract the next-generation workers; and
- Turning to external resources to fill the gaps.

To illustrate, 52% of the CISOs relied on outsourcing the security operation center core function, and thereafter came the forensics and legal support. Moreover, the majority of the CISOs responded that they were more confident in getting cyber services from a third party contractors, service providers, and business partners. One key barrier indicated by the CISOs was the hiring timespan, as it could take 3 to 6 months to hire a mid-level cybersecurity professional and more than 6 months to hire one at a director-level.

Lastly, one of the recurring issues in cyber that the CISOs have highlighted is the limited awareness of organizations around diversity equity, and inclusion (DEI) in the cyber function and the need to address this area to attract more women and individuals from diverse nationalities and backgrounds. According to Cybersecurity Ventures, only 25% of the cyber workforce are women and the number is much lower when it comes to senior leadership levels. Based on an article published by the World Economic Forum, women generally find the cyber field as a male centric space and a field that may prevent them to achieve work-life balance. Interestingly 22% of women did not have sufficient information about the cyber field and may be willing to join the workforce if they learn more about the profession and hence change their perceptions.

“52% of the CISOs relied on outsourcing the security operation center core function, and thereafter came the forensics and legal support”
Section 4

The Changing Faces Of Cybersecurity
Digital transformation is certainly unleashing the potential for growth and productivity. It is also giving rise to new and rapidly evolving digital risks that are accentuating the need for effective cybersecurity and increasing the demand for cybersecurity professionals. The convergence of unprecedented pace of change, automation, and emerging technologies is moving faster than what current cybersecurity teams can handle (refer to Figure 2).

"Digital transformation is certainly unleashing the potential for growth and productivity"

![Figure 2: The Growing Cyber Risk Gap](image)

"It is also giving rise to new and rapidly evolving digital risks that are accentuating the need for effective cybersecurity"

The changing faces of cybersecurity report, published by Deloitte in collaboration with Toronto Financial Services Alliance in 2018, addresses how Canada can bridge the cyber skills gap and stay ahead of these increasingly complex cybersecurity challenges. The report analyzes findings from a large-scale survey of leaders across governments, educational institutions, and businesses, and reveals both a qualitative and quantitative shift in demand for cyber expertise. The report asserts that countries need to take a bold and different action to address this global problem and calls for humanizing the faces of cyber personas. As such, a new talent framework is proposed and includes seven key personas with diverse skills and competencies (refer to Figure 3).
The framework brings together key drivers from key economic sectors, as well as global and leading competency frameworks (e.g., NICE and MITRE). By taking a human-centric framework, the report introduces a new way of thinking around a holistic approach to solving the talent gap. Deloitte’s cyber talent framework proposes seven cybersecurity personas: Strategist, Advisor, Defender, Firefighter, Hacker, Scientist, and Sleuth. These personas humanize the complex and multi-layered sets of capabilities required for effective cybersecurity. The cyber talent framework also: (1) expands the current narrow view of technical skills associated with cyber roles and functions; (2) leverages neurodiversity as a main ingredient to forming high performing teams; and (3) creates a more stable dictionary of skills relevant to the rapid pace of change in cybersecurity.

The report also stresses examining the critical actions that affect every stage of the human capital life cycle from recruitment of the right people, to onboarding graduates, continuously developing a pool of talent and retaining and advancing the top talent and high potentials all the way to exiting people to protect an organization’s talent brand in such a tight, yet global cyber industry (refer to figure 4). In regards to the female presence in the pool, organizations are encouraged to promote cyber and their brand as employers to women, highlighting the benefits of joining the cyber field through learning sessions, demonstrations, and orientations. Employers can also work with schools, universities, and recruiters to motivate women to join the cyber realm, expanding the reach to non-STEM programs and offering them opportunities to connect and network with mentors.

"Organizations are encouraged to promote cyber and their brand as employers to women, highlighting the benefits of joining the cyber field through learning sessions, demonstrations, and orientations"
Figure 4: The Talent Life Cycle Model

Case Study From NEOM, Saudi Arabia's Cognitive City Capitalization and WGS favors "Saudi Arabia" over "KSA"

Mesfer Almesfer, NEOM Group Chief Information Security Officer (CISO)
Mesfer Almesfer is an experienced cybersecurity leader who has delivered innovative security programs to safeguard billion-dollar enterprises. He is focused on maximizing security program efficiency and minimizing costs. A true collaborator, he champions new ideas to gain buy-in and build consensus.

01. What major challenge is your organization facing when it comes to bridging the talent gap in cyber (technical and awareness)?

The cybersecurity talent crisis has been making headlines in current mainstream media. While reports discuss how as many as 3.5 million job opportunities remain unfilled, I think employers may have a very different perspective on the topic. One can certainly discuss a gap, which for a number of organizations can be a concern; however, I think we are yet to reach the crisis stage.

The shortage of cybersecurity professionals represents an opportunity as it means that there is a new skillset to be mastered. If we play with the supply and demand formula, the impact on salaries, and the overall effects of market opportunities, this popular cybersecurity shortage suddenly appears to be an exciting opportunity for professionals, employers, and the system as a whole.

Let's go back to the 1990s for a moment, when the role of a database administrator was one of the hottest and most complicated roles to fill in the market, especially Oracle database administrators; fast forward to the second decade of the 2000s, and we see big initiatives and deployments globally requiring technically skilled cloud security professionals.

While this is an exciting skillset to master, there are two intrinsic challenges that I see and that I think we do not discuss enough as a cybersecurity community:

If there is a big surge in demand for cloud security professionals, you will see the demand for cloud certifications increasing and, as cybersecurity professionals, we know that obtaining such certifications requires a substantial investment. Some of these talents, who do not have the budget, will not be able to master the desired skillsets. Access to resources to develop and nurture talent is extremely important and often a topic that remains undiscussed; for this reason, here in NEOM, we allocate our budget to learning and development, ensuring that our resources have access to professional qualifications, either because they are in high demand, or because they are sought after by our talents.

Another associated challenge with the talent gap that is often not spoken about is motivation. Let me unpack this further; when the gap is filled by compensation-seekers, as an employer you look at a talent pool that is substantially different to your ideal
scenario, and that is because remuneration drives a professional up, to an extent. More than any other professions, cybersecurity talents need to have passion, patience, and ability to learn, and this is because they need to face cybercriminals who have two key characteristics: patience and ability to learn. Hackers are relentless when it comes to searching for an open door in your

infrastructure, and when they cannot find an open door they are eager to learn techniques to forcefully open one. Pace of sophistication in techniques and strategies is considerably higher than other professions, so as cyber heroes, we need to master other drivers, mainly patience and the ability to learn.

02. What solutions and initiatives have you adopted so far to successfully address those challenges?

I think there are a number of solutions and initiatives that one can take and that I certainly look at to ensure those challenges are adequately addressed in NEOM.

To start, I think mapping your current human capability helps in identifying not only what you have, but also what is available to you and that you did not consider because it does not fall squarely under the category of cybersecurity professionals.

For instance, we tightly collaborate with our colleagues in IT and often times, what you see is a desire to expand their skills into those overlapping areas between the two professions. Therefore, to enhance their needs, we provide the required learning and development opportunities so that they can broaden their skillsets and inject cybersecurity into their original domain.

This example feeds into the broader initiative that we adopt around promoting our people to enhance our existing human capital. Similarly, we have established a Cyber Risk Champion Program; the network covers departments, sectors, and corporate functions and its ultimate objective is to promote a cybersecurity culture within their domain, as well as provide real-time view over challenges and opportunities across NEOM.

NEOM is a complex environment due to its dynamic nature; the program allows us to enhance our understanding of the business, the needs, and challenges, while also leveraging the Champions’ expertise.

A second key initiative is staying close to management and leadership in order to have the adequate buy-in and support. Having a seat at the table and direct lines of communications means we obtain all necessary support, whether in the form of allocated budgets or operational capabilities. On this, I think another element to point out is how cybersecurity professionals also need to be able to discuss cyber risk in a business-friendly way. What I call the storytelling of cybersecurity is a key skill for CISOs to have, and one that we need to keep enhancing, particularly as we continue to talk about educating our management on cybersecurity. Similarly, we should be able to educate ourselves on how we can indeed become business accelerators and enablers.
03. What worked well and what would you do differently in implementing such initiatives at the strategic and operational levels?

Based on my humble experience in NEOM and before NEOM, people want to understand more context; by this I mean to fully know why you are implementing a certain control... why you may be pushing for a certain risk management change. We, as cybersecurity professionals, fall back too easily into the risk and compliance argument. In my previous answer I discussed how we should be educating ourselves to speak to the business using that language; I put myself in the shoes of other members of the leadership group and I can see how basing every control or initiative on compliance does not aid the building of a long-term sustainable relationship.

For this reason, looking back, I think this is one area of improvement I’m focusing on. I think a key component of the storytelling of cybersecurity is precisely to take the leadership into the journey providing them with the right level of context and explanation that is tailored to their expectations. It is extremely important to know and analyze your audience, understand their interests, their set of beliefs, backgrounds, and priorities.

“I think a key component of the storytelling of cybersecurity is precisely to take the leadership into the journey, providing them with the right level of context and explanation that is tailored to their expectations”

04. What recommendations and advice would you put forward and share with other entities that would like to adopt the same approach?

To start, I cannot stress enough the point that one size does not fit all. In NEOM, we know this particularly well as we set ourselves to be the very first cognitive region that the world has ever seen, so as you can imagine, there is nothing quite comparable to the ambitious mission we are striving for. But the same is applicable for other entities as well, as each entity has its own micro-cosmos. For this reason, I recommend beginning by understanding your environment, your needs, and your applicable threat landscape. Accordingly ensure to have a fit-for-purpose cybersecurity program and strategy.

Secondly ensure that your cybersecurity
strategy and program is in the radar of your top management; if it is not captured by your decision-makers, you are bound to struggle and face challenges with a variety of things, including budget allocation, human capital availability, and stakeholder management.

Thirdly, I believe the golden triangle of people, processes, and technology drives feed into the approach we are adopting. Understand your people, and make sure to have the best talent in your organization; and not just having it, but also retaining your talent as a long sustainable investment. Establish processes and document them through your policies and activate these across your organization in a way that is known within your environment; this will certainly expedite your operations and will create a structure to fall back to. Lastly, technology is the key to help you by automating the way you protect your accounts and streamline those processes and operations that are particularly relevant to you.

"Understand your people, and make sure to have the best talent in your organization; and not just having it, but also retaining your talent as a long sustainable investment"

05. What are your organization’s next steps or future plans as you continue to build your people capabilities in cyber?

More collaboration and partnerships with academic centers to ensure they see cybersecurity as a viable academic path. Having more graduates specializing in cybersecurity will enable us to have a bigger pool to choose from. This is definitely one of the next steps here in NEOM.

In addition to this, we are actively promoting the cybersecurity industry by having more small and medium companies involved. We believe in the amazing and innovative work that some start-ups are making, creating undeniable value to their customers and service providers, as well as to human capital capabilities.

Lastly over the last couple of years in particular, we have seen how radically and drastically the landscape can change; for this reason, looking into global trends, whether these are geopolitical or supply chain, are extremely relevant to monitor and analyze as they can have an impact on the business, as well as direct and indirect cybersecurity ramifications. Ultimately this type of analysis supports us in maintaining a cyber posture.
A Global Perspective - A Multi-Disciplinary Approach

Part of the solution to bridging the skills gap also includes moving away from stereotypes and preconceptions of the cybersecurity professional image and moving towards the objective of embracing a diverse neuro, socio, cultural, and academic discipline pool of individuals instead. The first step in doing so is accepting the definition of cybersecurity as a “meta-discipline” (Allen Parrish, 2018) composed of an aggregate spectrum of disciplinary variants, and thus requiring vertical technical knowledge, as well as horizontal renaissance-like competency abilities generally found in non-STEM social sciences. Companies such as Google and Microsoft and government organizations such as the UK’s Government Communications Headquarters (GCHQ) and National Crime Agency (NCA) are at the forefront of such an approach and are meeting the challenge of tackling the cyber skills gap through harnessing neurodiversity and multi-disciplinarity within their cybersecurity teams. This has brought a series of benefits including: (1) promoting non-linear thinking; (2) providing a holistic capability able to meet the enhanced risk exposure stemming from an increased attack surface as a result of the accelerated digitalization due to the advent of COVID-19; and (3) an increased pool of candidates from which to recruit.

“Companies such as Google and Microsoft and government organizations such as the UK’s Government Communications Headquarters (GCHQ) and National Crime Agency (NCA) are at the forefront of such an approach and are meeting the challenge of tackling the cyber skills gap through harnessing neurodiversity and multi-disciplinarity within their cybersecurity teams"
Section 5

A Triple Helix Approach To Addressing The Cyber Human Capital Challenge
International Coordination To Join Forces

As a starting point, governments need to join forces with academia and the private sector to tear down individual country level silos in learning and development around the digital and cyber domains. This naturally begins with assessing how cyber aware student populations are in relationship to the current headwinds in order to build a true baseline for development and target private and public investment to where it is needed most, while considering economic and digital access disparities and ecological concerns in the immediate and near future. As such, it is critical to start early and embed cyber hygiene principles geared to young students in order to familiarize them and their parents with the cyber domain and build their foundational understanding around what is a cyber-attack and how to secure their digital life.

In parallel, greater international coordination on global development programs are needed and should start providing bootcamps, hackathons, and bug bounty programs that will sharpen skills and enhance students’ cyber capabilities, while simultaneously growing interest in the field and identifying candidates earlier in the educational spectrum. Global governments and academia need to work to establish exchange education or training programs related to cybersecurity between countries, with the private sector sponsoring these exchange programs by providing internships and/or materials that prepare students for their careers.

Retooling The Education Sector

The education sector is under pressure to address skills shortages in the cybersecurity industry as well. Educators are faced with the challenge of teaching current and future generations of students about cybersecurity and privacy, fields that are relatively new and difficult to learn for most. Furthermore, getting students to consider careers in cybersecurity is another obstacle to overcome, as well as encouraging more female students to consider embarking on a cyber career. Nevertheless, there are many ways to encourage students to consider the cybersecurity field.

One way is to begin by conversing with students and introducing them to the world of cybersecurity, an area that many of them have most likely never heard much about. The Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency (CISA) has issued a set of guidelines and tips aimed specifically at younger students.25 Such tips will assist educators in facilitating discussions with students about exciting new jobs in the cybersecurity field and help create interest at a younger age and across a more diverse range of students that may have not considered the field as an option.

Governments and the private sector should develop cyber or digital secure awareness programs based on gamification for students to capture the information in a fun yet educational way. Game theory and gamification have demonstrated how the format is able to reach broader audiences and increase the uptake of information around most subjects, making it an ideal medium for students seeking to play a role in the future of cybersecurity.
Schools should offer digital training or coding camps during holidays and summer seasons, when students have additional free time. The goal of such training camps is to teach students how to think like a hacker in order to stay ahead of them, while simultaneously improving their digital and cyber knowledge, skills, and abilities. Such camps, when made available to diverse student populations, could immerse students in the worlds of computer programming, network administration, and system design so that they can gain a solid understanding of the core components of cybersecurity. This type of camp teaches a variety of extremely valuable computer science skills and concepts, such as algorithm creation, encryption, network security, cryptography, and the fundamentals of various programming languages such as Java, C#, Swift, and Python. For instance, Digital Media Academy Tech Camps offer one or two-week summer sessions for children ages 7 to 19. They provide technology education curriculum and learning experiences for global science, technology, engineering, art, and mathematics (STEAM) education leaders. These bootcamps are supported by Stanford educators, researchers, and industry experts, and have impacted the lives of more than 500,000+ students in 125+ countries.

Schools can offer a free digital platform that engages teens and lifelong learners in games and interactive software that foster authentic scientific exploration. A content-rich platform built around the gamification concept could allow for international competition at the individual and group levels, with the ability to attain prizes and potential scholarship funding as a means of supporting diverse global future talents that can uplift and fill out the growing gaps across the cybersecurity labor market.

Schools and educators should organize field trips to various cybersecurity companies so students can observe what professionals do firsthand. Students might even have the chance to participate in real-world security exercises, such as patching an outdated operating system, which is an easy task that can be done at home.

Governments, ministries of education, and cybersecurity professionals need to work together. This will ensure that cyber culture is taught to children early on in order to develop basic and fundamental cybersecurity habits that can protect their lives and digital presence, potentially paving the way for a career in the cyber domain while helping to build a more secure world.

All of these initiatives will help students gain knowledge of cybersecurity exposure from an early stage, increasing the possibility of having more university students interested in securing the world and thereby increasing the number of cybersecurity professionals.
Governments Making An Impact

Over the next five years, governments need to take the initiative and lead the development, creation, and integration of cyber content within the school base digital and/or technology classes taught. At the same time, governments need to assess the current cyber maturity of students, educators, and the technologies used for remote schooling to determine whether they are cyber aware or secure. Furthermore, the cyber digital and technology content taught at schools should be reviewed and updated on a regular basis.

Considering a long-term journey, governments must collaborate to develop regulations that incorporate cybersecurity into the schooling curriculum. A global standard requirement that introduces cybersecurity education should be developed for high-school students as a compulsory subject and as an optional education opportunity for younger students. There should also be more in-depth knowledge and skills training similar to the teaching of trades in schools.

Governments, in collaboration with the private sector, need to create additional internship initiatives that support graduates during and after completing their degree by providing some benefits, such as the governmental paid internships for students enrolled in technology related fields. Additionally, governments should be working to enhance and innovate new ways to attract cybersecurity professionals and students, for example, optional practical training (OPT) programs that allow students to study, train, and work in a foreign country under the condition of joining a cybersecurity-related degree.

The opportunities that the current wave of innovation and digital development is creating to advance our collective society are unparalleled in human history as are the threats to that advancement through a growing cadre of global cyber threat actors. Without immediate action from global governments, academia, and private industries working in collaboration across borders and siloed development efforts, our future generations will be more at risk of societal instability and potential collapse than ever before. The ability for cyber threat actors to manipulate societal outcomes through digital means presents a current and growing threat to humanity. Effectively countering this will require a top to bottom evaluation and rethinking of how we approach digital and thereby cybersecurity education and development. It will require global coordination, versus competition, to foster a collaborative spirit and build a secure future.

“The ability for cyber threat actors to manipulate societal outcomes through digital means presents a current and growing threat to humanity. Effectively countering this will require a top to bottom evaluation and rethinking of how we approach digital and thereby cybersecurity education and development"
Abbreviations:

AI: Artificial Intelligence
ASD: Australian Signals Directorate
CAE-CD: Center of Academic Excellence in Cyber Defense
CAE-CO: Center of Academic Excellence in Cybersecurity Operations
CAE-R: Center of Academic Excellence in Cyber Research
CCB: Cyber Capacity Building
CETAP: Cybersecurity Education and Training Assistance Program
CIS: Center for Internet Security
CISA: Cybersecurity and Infrastructure Security Agency
CyberHEAD: Cybersecurity Higher Education Database
DHS: Department of Homeland Security
DoD: Department of Defense
DoD-CIO: Department of Defense Office of the Chief Information Officer
ECSF: European Cybersecurity Skills Framework
EFTA: European Free Trade Association
ENISA: European Union Agency for Cybersecurity
EUISS: European Union Institute for Security Studies
FBI: Federal Bureau of Investigation
GCHQ: Government Communications Headquarters (UK)
GFCE: Global Forum for Cyber Expertise
ICS: industrial control systems
IoT: Internet of Things
ISACA: Information Systems Audit and Control Association
MHA: Ministry of Home Affairs
ML: Machine Learning
NCA: National Crime Agency (UK)
NCA: National Cyber Authority
NCAE-C: National Centers of Academic Excellence in Cybersecurity
NCSC: National Cyber Security Centre
NICE: National Initiative for Cybersecurity Education
NIST: National Institute of Standards and Technology
NSA: National Security Agency
NSF: National Science Foundation
OECD: Organization for Economic Co-operation
OPT: Optional Practical Training
SCyWF: Saudi Cybersecurity Workforce Framework

SSG: SkillsFuture Singapore

STEAM: Science, Technology, Engineering, Art, and Mathematics

STEM: Science, Technology, Engineering, and Mathematics

UKCSC: United Kingdom Cyber Security Council

USCC: US Cyber Challenge

USCYBERCOM: U.S. Cyber Command

WSG: Workforce Singapore
Bibliography:


Footnotes:


20 Srini Subramaniam and Meredith Ward, NASCIO Cybersecurity Study (United States: Deloitte, 2022).


Contact the authors

Dr. Amira Khattab
Partner
Amira is a Partner and the ME Leader for Cyber Talent & Education practice at Deloitte with over 20 years of experience in the digital, cyber, and education domains. akhatab@deloitte.com

Alan James Mears
Senior Advisor
Alan is a Senior Advisor in the Cyber practice at Deloitte with 20+ years of experience in cyber strategy and awareness. almears@deloitte.com

Wayne Loveless
Senior Advisor
Wayne is a Senior Advisor in the Cyber practice at Deloitte with 25+ years of experience in cyber defense and strategy. wloveless@deloitte.com

Edoardo Giglio
Partner
Edoardo is a Partner, GPS Lead, Cyber & Strategic Risk at Deloitte Italy with 22 years of experience in high-tech crime, crisis management, defense technologies, and government strategies. egiglio@deloitte.it

Alhanouf Albelewi
Manager
Alhanouf is a Manager in the Cyber practice at Deloitte with 8+ years of experience in cyber governance, risk, and compliance (GRC) and cyber awareness. aalbelewi@deloitte.com

Mohamad Baydoun
Manager
Mohamad is a Manager in the Cyber practice at Deloitte with 8 years of experience in cyber strategy, awareness, and technical assessments. mbaydoun@deloitte.com