Bridging the Cyber Skills Gap

World Economic Forum

Centre for Cybersecurity

In today's hyperconnected digital landscape, the cybersecurity industry faces a global shortage of over 4 million professionals

With a consistent year-on-year increase in demand for qualified practitioners, the deficit shows no sign of abating. Some of the underlying factors contributing to the shortage include:

A lack of understanding of what cybersecurity professionals do, coupled with insufficient awareness of how to enter the cybersecurity sector, discourages individuals from pursuing a career in cybersecurity.

What measures could be taken to attract cybersecurity talent?

Educational programs on cybersecurity face challenges, including outdated and misaligned curricula, a shortage of qualified instructors and a lack of structured mentorship programs.

How can cybersecurity education be improved to equip learners effectively with essential skills?

While many cyber skills are transferable, employers' demand for formal cybersecurity education creates a barrier to entry.

How can organizations rethink recruitment and talent-sourcing practices?

Continued stress, fatigue and pressure experienced by cyber professionals result in high employee attrition rates.

How can organizations create incentives for talent and retain their staff?

Recognizing that a single actor alone cannot effectively tackle the cybersecurity workforce shortage, the World Economic Forum established the “Bridging the Cyber Skills Gap” initiative to…

Raise awareness and share knowledge

Raise awareness and share knowledge amongst C-suite executives and decision-makers about the cybersecurity skills and talent deficit and its economic and security implications.

Define actionable approaches on cyber talent

Define actionable approaches and processes that will help build sustainable cyber talent pipelines within organizations across sectors and geographies.

Showcase success stories and scale opportunities

Showcases successes and best practices from partner organizations on cybersecurity workforce development and explore opportunities to scale.

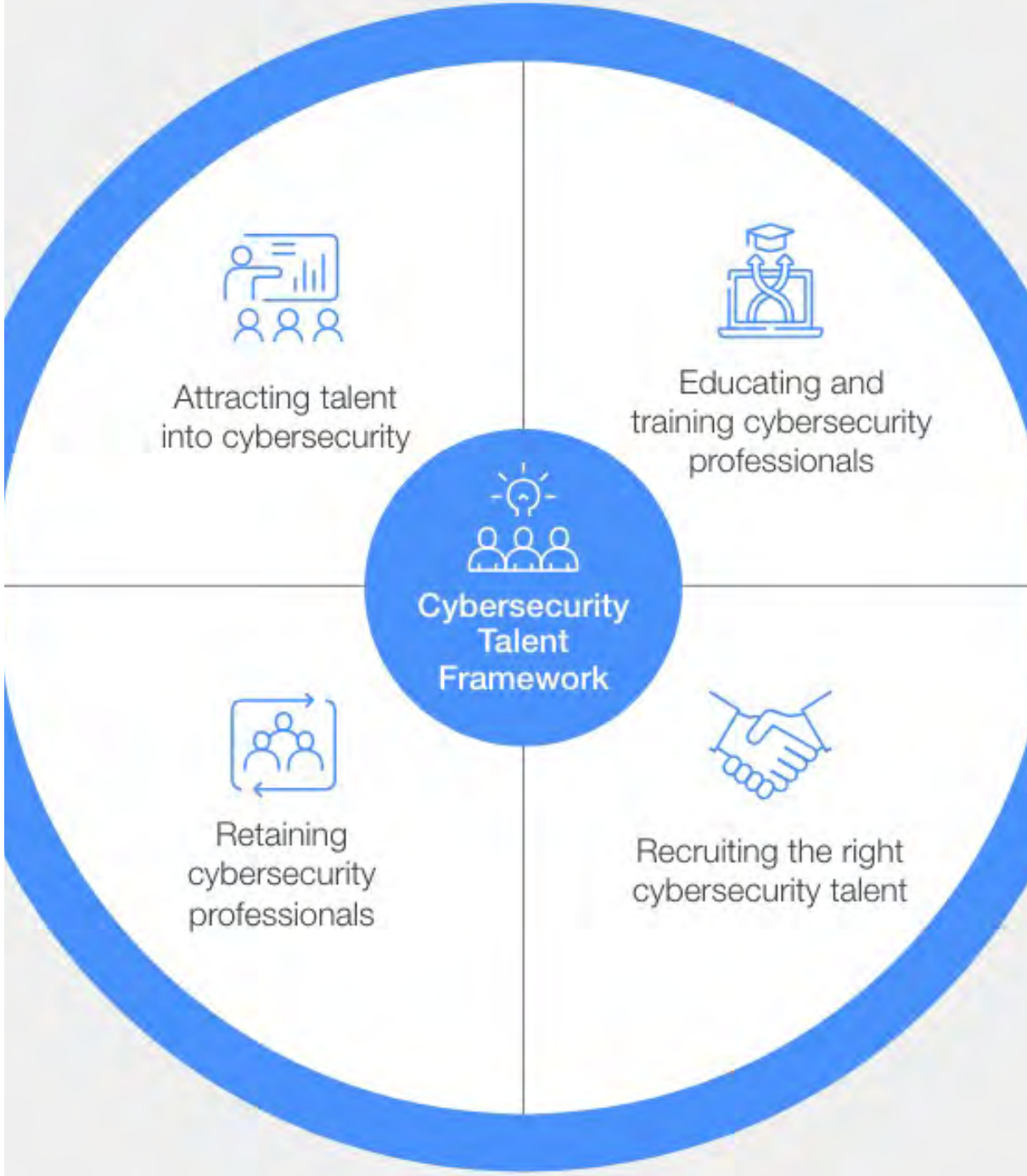
The initiative developed a **Strategic Cybersecurity Talent Framework (CTF)** featuring actionable approaches to help organizations build sustainable talent pipelines. The Framework was launched during the World Economic Forum`s Special Meeting in Saudi Arabia.

The CTF should guide public- and private sector actors in building a skilled cybersecurity workforce

The CTF sought to identify and address the underlying reasons contributing to the broader cybersecurity workforce gap. Challenges and recommended solutions cover 4 priority areas including:

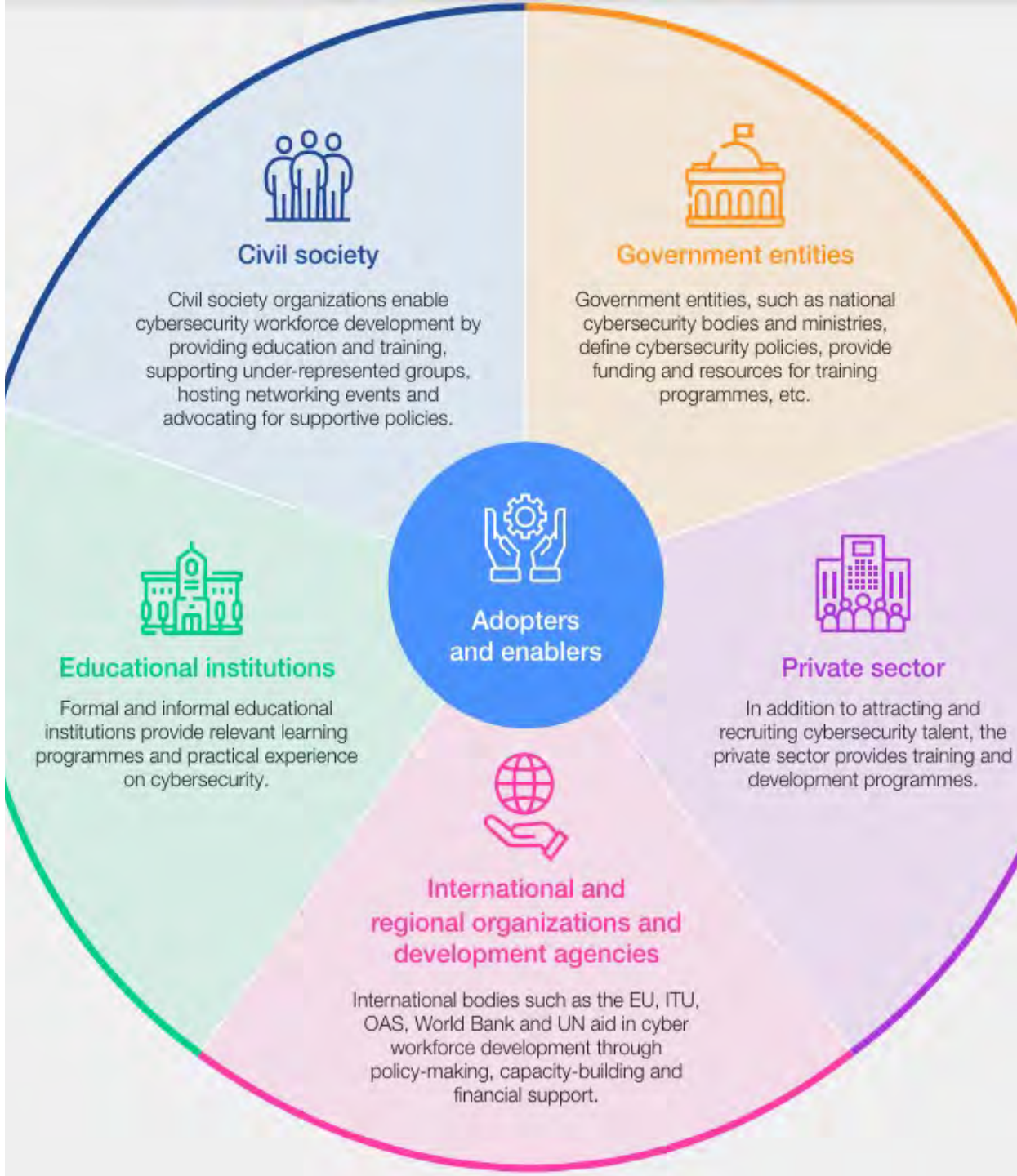
- Attracting talent into cybersecurity
- Educating and training cybersecurity professionals
- Recruiting the right cybersecurity talent
- Retaining cybersecurity professionals

The four priority areas should not be viewed in isolation, but as interconnected components of a comprehensive cybersecurity talent-management approach.



The cybersecurity workforce landscape is multifaceted involving an array of actors dedicated to securing an increasingly digitalized world

- Government entities responsible for defining and setting policies and regulations on cybersecurity workforce development, and providing funding, grants and resources for cybersecurity training programs and initiatives.
- The private sector supports and promotes training programs and offers avenues for practical development of competencies.
- International/regional organizations and development agencies that help build a cyber-savvy workforce by shaping policies, facilitating capacity-building programs and providing technical and financial assistance, etc.
- Educational institutions that provide formal education on cybersecurity which occurs in a systematic, structured environment and non-formal training which consists of programs and courses designed to provide learners with cybersecurity skills, knowledge and competencies outside the formal education system.
- Civil society organizations that provide affordable and accessible education and training, support under-represented groups, host networking events and advocate for supportive policies.



It is imperative that decision-makers in public and private organizations collaborate in efforts to inspire the next generation of cyber defenders and remove entry barriers for individuals aspiring to pursue a career in the field.

The CTF provides over 50 recommendations on how to action the 4 priority areas, including the following:

Marketing cybersecurity as value-based work, emphasizing its profound impact on society and multidisciplinary nature.

Incorporating cybersecurity education in primary/secondary schools and ensuring curricula are flexible and adaptable to the changing cyber landscape.

Providing individual development plans rather than predefined career paths to address the different needs and aspirations of employees.

Ensuring that talent retention is not the sole responsibility of HR, but is an effort of various stakeholders, including employees, managers and executive leadership.

The needs and possibilities of different stakeholders vis-à-vis the CTF may vary across geographies and industries.

Thank you

For more information about this initiative, please contact:

Tal Goldstein, Head of Strategy and Policy, Centre for Cybersecurity –tal.goldstein@weforum.org

Natasa Perucica, Research and Analysis Specialist, Centre for Cybersecurity – natasa.perucica@weforum.org