Deloitte.

Together makes progress

Tackling the Cybersecurity Talent Gap in the Middle East

March 2026

Table of Contents

Abstract

The cybersecurity talent gap has emerged as one of the most pressing challenges confronting governments and organizations worldwide. As digital transformation accelerates across public services, critical infrastructure, and regulated industries, demand for cybersecurity capabilities continues to outpace the availability of skilled professionals. Despite growing investment in education, certifications, and training programs, many institutions struggle to translate these efforts into job-ready talent, resulting in persistent shortages across technical, governance, and leadership roles. This challenge is not solely a matter of supply, but a systemic issue rooted in fragmented workforce pathways, misaligned curricula, limited experiential learning, and insufficient mechanisms to measure workforce readiness and impact.

In the Middle East, these pressures are amplified by ambitious national transformation agendas, rapid adoption of emerging technologies, and increasing regulatory expectations around digital trust, data protection, and cyber resilience. Governments and organizations are simultaneously tasked with scaling cybersecurity capacity, localizing talent through workforce nationalization programs, and securing sovereign digital infrastructure, which is often within compressed timelines. These converging demands place unprecedented strain on the cyber workforce, requiring professionals who are not only technically proficient, but also capable of operating within complex regulatory, operational, and national-security contexts. Without structured pathways that translate education into deployable capability, organizations risk over-reliance on external expertise, uneven skill distribution, and limited institutional resilience.

This paper presents a system-level approach to tackling the cybersecurity talent gap in the Middle East by reframing workforce development as an integrated, outcomes-driven ecosystem rather than a collection of isolated initiatives. Drawing on regional case studies, international benchmarks, and Deloitte's delivery experience across government and regulated industries, it introduces two complementary frameworks designed to bridge the gap between talent supply and operational demand. The 6E Framework, which encompasses evaluation, education, exposure, experience, ecosystem, and environment, provides a holistic lens for assessing and strengthening national and organizational cyber workforce systems.

Building on this foundation, the **CORE Loop model** translates strategy into execution through six continuous phases:

- **Catalyze access** to talent
- **Orchestrate** learning and career pathways
- **Reinforce** skills through experience-based development
- **Evidence outcomes** through robust measurement and feedback mechanisms.
- **Academia–industry partnerships** that align education with real workforce demand
- **Policy reform** as a force multiplier that sustains scale, consistency, and long-term system impact.

Together, these frameworks emphasize skills-based workforce design, experiential learning pathways, and evidence-based measurement as critical enablers of sustainable cyber capability. The paper highlights practical mechanisms for aligning academia, industry, and government, modernizing curricula and credentialing, embedding on-the-job training and simulations, and implementing leading and lagging indicators that track workforce readiness, deployment speed, and retention.

By adopting integrated workforce strategies grounded in skills, experience, ecosystems, and measurement, governments and organizations can move beyond short-term interventions toward resilient, scalable cybersecurity talent systems. The approaches outlined in this paper provide a practical roadmap for strengthening cyber resilience, supporting economic diversification, and enabling secure digital growth across the Middle East.

Introduction

The rapid evolution of digital technologies is fundamentally reshaping economies, industries, and societies worldwide. In the Middle East, this transformation is especially pronounced as organizations accelerate their adoption of artificial intelligence (AI), cloud computing, and advanced analytics to drive innovation and competitiveness (Engage-ID, 2025). However, this digital progress is accompanied by a dramatic surge in cyber threats. The region has seen a significant increase in AI-driven attacks, geopolitical cyber risks, and the exploitation of cloud vulnerabilities, making robust cybersecurity capabilities more critical than ever (Engage-ID, 2025; SGS, 2025).

Cybersecurity is now a cornerstone of national resilience and business continuity. Yet, the demand for skilled cybersecurity professionals far outpaces supply. Recent studies show that 90% of UAE companies face a security workforce shortage, with over half reporting more than ten unfilled cybersecurity positions (MENews247, 2024). In Saudi Arabia, the shortage has surpassed 18,000 professionals, while the region as a whole is experiencing a cybersecurity workforce gap that mirrors the global shortfall of nearly 4.8 million specialists (MENews247, 2024; ISC2, 2024).

Several factors contribute to this widening gap:

- **Skills shortages**: The rapid emergence of new technologies such as AI, quantum computing, and IoT is raising the bar for required cyber skills, making continuous upskilling essential (Engage-ID, 2025).
- **Education and training gaps:** Traditional education pathways are struggling to keep pace with industry needs. Many cyber roles require specialized, hands-on training rather than just academic credentials (MENews247, 2024).
- **Burnout and retention**: The relentless pace of cyber threats is leading to high levels of stress and burnout among cybersecurity professionals. In the UAE, 69% of Chief Information Security Officers (CISOs) report burnout, and 83% of IT security staff say this has led to errors and breaches (MENews247, 2024).
- **Budget constraints**: Economic pressures and the high cost of cyber incidents—averaging $8.05 million per breach in the Middle East, nearly double the global average—are straining organizational resources (World Economic Forum, 2025).
- **Workforce diversity**: Underrepresentation of women and minority groups in the cyber workforce limits the available talent pool and hinders innovation (World Economic Forum, 2025).

To address these challenges, organizations and governments are investing in targeted education and training programs, forging partnerships with universities, and promoting continuous learning and professional certification (Engage-ID, 2025; Nucamp, 2025). There is also a growing recognition of the value of transferable skills from adjacent fields such as IT, risk management, and data analysis, which can help broaden the talent pool and accelerate workforce development (World Economic Forum, 2025).

National strategies such as the UAE's Digital Strategy 2025 and Saudi Arabia's National Cybersecurity Strategy 2.0 - emphasize the need to standardize cyber skills, align education with industry needs, and foster diversity and inclusion. These efforts are critical to closing the talent gap and ensuring that the region's digital transformation is secure, resilient, and sustainable (Engage-ID, 2025).

Ultimately, bridging the cyber talent gap in the Middle East requires a coordinated, multi-stakeholder approach that integrates education, workforce development, and policy interventions. Only by fostering a dynamic, agile, and inclusive cyber workforce can organizations and nations secure their digital futures and fully realize the benefits of ongoing digital transformation.

Section 1

Strategies to bridge the cyber talent gap

Section 1: Strategies to bridge the cyber talent gap

The cyber talent gap is no longer a looming threat; it is an evolving crisis. Organizations across all sectors face a critical shortage of skilled cybersecurity professionals, leaving them vulnerable to increasingly sophisticated cyberattacks. Numerous reports and studies from reputable sources like the $(ISC)^2$ Cybersecurity Workforce Study, Cybersecurity Ventures, and government agencies consistently demonstrate the growing cybersecurity skills gap. These reports project a significant shortfall in the number of qualified cybersecurity professionals needed to meet the growing demand. Therefore, this is not just a talking point but a reflection of a pressing global challenge. The increasing reliance on digital technologies across all industries makes a skilled cyber workforce not just desirable but essential for maintaining business operations, protecting sensitive data, and ensuring economic stability.

This section explores strategic approaches to address this challenge, moving beyond reactive measures to proactive, sustainable solutions.

Understanding the depth of the challenge:

The cyber talent gap is multifaceted. It is not simply a lack of people; it is a mismatch between the skills demanded by the evolving threat landscape and the skills possessed by the available workforce. This gap is exacerbated by:

- **Evolving threat landscape:** The constantly evolving nature of cyber threats requires professionals with advanced and up-to-date skills, which are often lacking in the current workforce. Traditional training methods struggle to keep pace.
- **Rapid technological advancements:** The constant evolution of cyber threats and technologies requires Professionals to continuously upskill and reskill, a challenge for both individuals and organizations.
- **Budget constraints:** Many organizations, particularly smaller ones, face budget constraints that limit their ability to attract and retain top cybersecurity talent.
- **Competitive talent landscape:** High demand and limited supply drive up salaries, incentives, and employment offer making it difficult for smaller organizations to compete for talent.
- **Unconventional career pathways:** Many individuals are unaware of career opportunities in cybersecurity or the pathways to enter the field. This limits the potential talent pool. Equally, pursuing a career in cybersecurity is not as straightforward as other more traditional professions. The dynamic nature of cybersecurity and changing landscape make it difficult to design a one-size-fits-all pathway.

- **Insufficient training and education:** Traditional training and education pathways often fail to keep pace with the rapid changes in the field, leaving graduates with outdated skills. Existing cybersecurity education and training programs often fail to equip individuals with the practical skills and experience needed to address real-world threats.
- **Barriers to entry:** Perceived high barriers to entry, such as the need for advanced technical skills or expensive certifications, can discourage individuals from pursuing cybersecurity careers.

Strategic approaches to bridge the gap

The fiercely competitive technology and cyber talent market demands customized strategies for attracting and retaining skilled professionals. Addressing the cyber talent gap requires a multi-faceted approach involving collaboration between industry, academia, and government.
In the ultra-competitive digital talent market, more companies are using customized strategies to attract and retain talent, with an emphasis on both offering a variety of development opportunities and rewarding in ways that appeal to this unique talent group.

A holistic talent management framework offers an integrated and strategic approach to managing an organization's talent throughout the entire employee lifecycle. It goes beyond simply filling open positions and focuses on developing, engaging, and ultimately aligning talent with long-term business goals. "Holistic" implies that it considers all aspects of the employee experience and aligns talent strategies with overall business objectives.

Key components of a holistic talent management framework typically include:

1. **Compelling employee value proposition:** Offer competitive compensation, but also emphasize challenging work, opportunities for innovation, access to cutting-edge tools, and a supportive, collaborative team environment.

2. **Employer branding for cyber:** Cultivate your reputation as an organization that values innovation, ethical hacking, continuous learning, and provides challenging, impactful cyber work. Highlight opportunities to defend critical infrastructure or develop cutting-edge security solutions.

3. **Strategic cyber talent acquisition:** Look beyond conventional Information Technology (IT) backgrounds and actively recruit from diverse fields (e.g., psychology for social engineering analysis, linguistics for threat intelligence, gaming for problem-solving aptitude). Prioritize demonstrable skills and potential over rigid academic qualifications to identify true cyber acumen.

4. **Immersive training & certifications:** Invest in hands-on-labs, simulated attack environments, and industry-recognized certifications (e.g., CISSP, OSCP, CISM).

5. **Mentorship & knowledge sharing:** Foster a culture where experienced cyber professionals mentor emerging talent, facilitating the transfer of tacit knowledge and best practices in incident response, threat hunting, and security architecture. Provide constructive, real-time feedback, particularly after incidents or security exercises, to drive continuous improvement. Implement robust knowledge transfer processes to ensure continuity and minimize risk when key cyber personnel transition.

6. **Clear career trajectories:** Define clear progression paths within cybersecurity (e.g., from security analyst to incident responder, security architect, or CISO), demonstrating opportunities for growth and specialization.

7. **Develop future leaders:** Pinpoint key cyber leadership and specialist roles that are vital for organizational security. Proactively identify and develop high-potential individuals for these critical roles, providing them with leadership training, strategic exposure, and cross-functional experience.

8. **Recognition & impact:** Acknowledge the critical, often unseen, work of cyber professionals. Highlight their contributions to protecting the organization's assets and reputation. Recognize the high-stress nature of cyber roles and implement wellbeing initiatives to prevent burnout, such as flexible working arrangements and mental health support.

Priorities for a cyber talent management framework addressing the most pressing challenges and opportunities in the cybersecurity field.

1. **Investing in education and training:**

- **Curriculum reform**: Educational institutions need to revamp cybersecurity curricula to reflect the latest technologies and threats, incorporating practical, hands-on training. This includes fostering collaboration with the industry to ensure relevance and alignment with real-world needs.
- **Providing both foundational and advanced training**: Organizations should focus on closing the experience gap by offering internships and apprenticeships to provide practical experience and simulate real-world scenarios. Additionally, they should focus on integrating AI to augment less experienced workers, as well as rethink talent acquisition strategies to prioritize human capabilities like curiosity and emotional intelligence.
- **Upskilling and reskilling initiatives**: Organizations should invest in robust upskilling and reskilling programs for existing employees, providing opportunities to learn new skills and adapt to evolving threats. This can involve apprenticeships, online courses, and mentorship programs.
- **Promoting STEM education**: encouraging young people to pursue careers in Science, Technology, Engineering, and Mathematics (STEM) is crucial for building a future pipeline of cybersecurity talent. This requires engaging initiatives at the primary and secondary school levels.

2. **Fostering diversity and inclusion:** Building a diverse and inclusive cyber workforce is essential for bringing diverse perspectives and experiences to the table. Organizations should actively promote diversity and inclusion in their recruitment and retention efforts. This includes targeting underrepresented groups, creating inclusive work environments, and providing opportunities for professional development and advancement for all employees:

- **Targeted recruitment**: Organizations should actively seek out and recruit individuals from diverse backgrounds, including women, minorities, and individuals with disabilities. This requires addressing unconscious bias in recruitment processes and creating inclusive work environments.
- **Mentorship and sponsorship programs**: Mentorship and sponsorship programs can help support and advance the careers of underrepresented groups within the cybersecurity industry.
- **Promoting flexible work arrangements**: Offering flexible work arrangements can attract and retain talent, particularly those with caregiving responsibilities or other commitments.

3. **Collaboration and partnerships:**

- **Public-private partnerships**: Collaboration between government, industry, and academia is essential for developing effective strategies to address the cyber talent gap. This includes sharing best practices, developing training programs, and funding research.
- **Industry consortiums**: Industry consortiums can pool resources and expertise to develop training programs, share knowledge, and advocate for policies that support the cybersecurity workforce.

- **Cybersecurity awareness campaigns**: Raising public awareness about cybersecurity threats and the importance of cybersecurity professionals can help attract more individuals to the field.

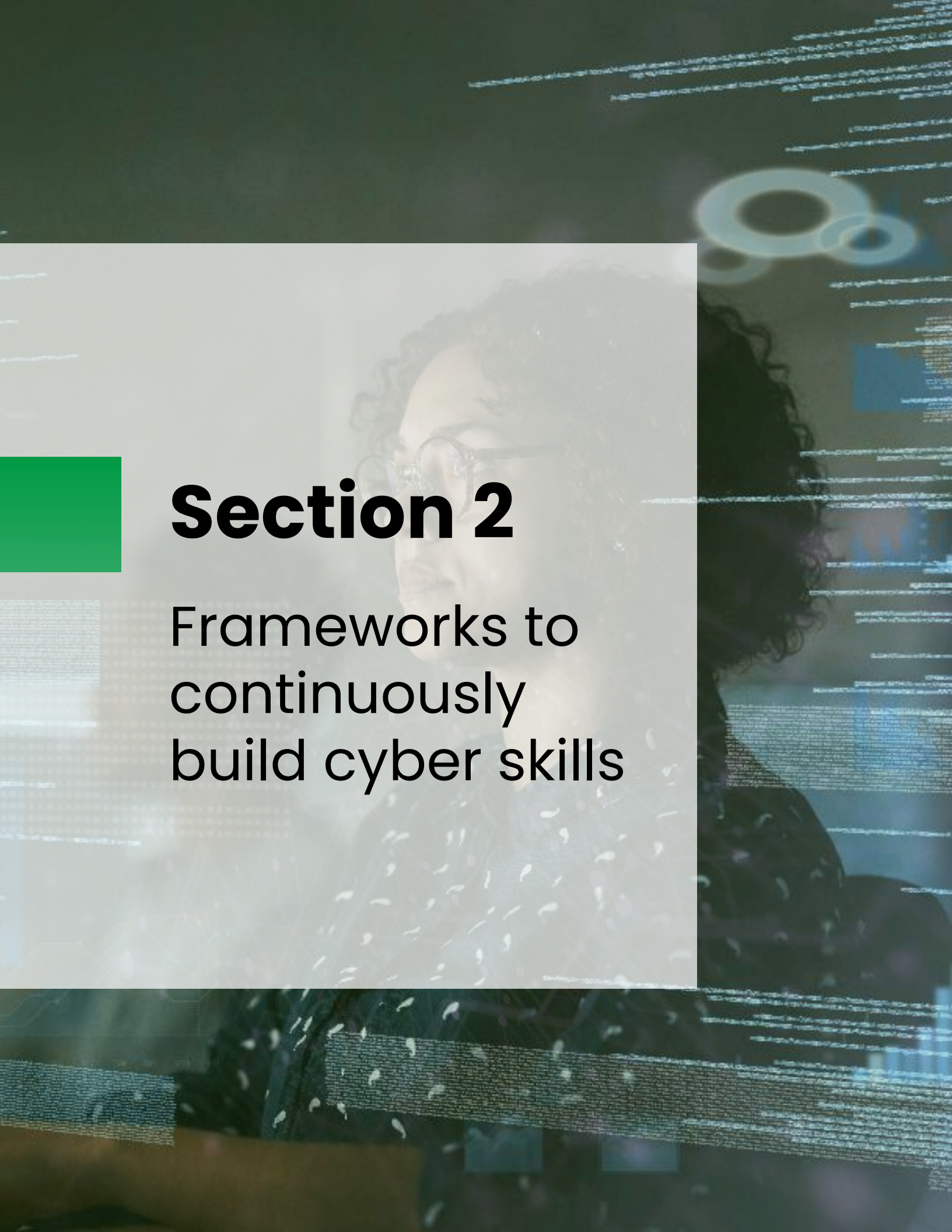
4. Skills based organization: The cybersecurity landscape is constantly evolving, with new threats and technologies emerging regularly. In response, organizations are shifting from organizing work and the workforce around traditional jobs to skills-based work that taps into the full range of workers' capabilities, interests and motivations. Skills based organizations match people and skills to the work, developing and engaging workers based on their individual needs, talents, skills, and preferences. By focusing on individual capabilities rather than fixed roles, organizations can better match specific cybersecurity skills (e.g., incident response, threat intelligence, cloud security, secure coding) to projects and tasks where they are most needed.

5. Attracting and recruiting top talent: Competition for skilled cybersecurity professionals is fierce. Organizations need to develop proactive recruitment strategies to attract top talent. This includes building a strong employer brand, offering competitive compensation and benefits, and leveraging diverse recruitment channels. They should also target non-traditional talent pools, such as veterans or career changers, and offer internships and apprenticeships to develop future talent.

6. Retention and engagement: Retaining skilled cybersecurity professionals is crucial. Organizations need to create a positive and supportive work environment that fosters employee engagement and loyalty. This includes providing opportunities for career growth, recognizing and rewarding performance, offering flexible work arrangements, and promoting a culture of learning and development. Mentorship programs and clear career paths can significantly improve retention.

7. Performance measurement and metrics: Establishing clear performance metrics and regularly evaluating the effectiveness of the cyber talent management framework is crucial for continuous improvement. This means tracking key metrics such as employee retention rates, time-to-fill open positions, employee satisfaction, and the number of security incidents. This data can be used to identify areas for improvement and adjust the framework accordingly. Regularly assessing the return on investment (ROI) of talent management initiatives is also a very important step.

Addressing the cyber talent gap is a critical imperative for organizations and nations alike. By adopting a comprehensive approach that encompasses education, diversity, technology, and collaboration, building a more resilient and secure digital future becomes a great significance. The investment in these strategies is not merely a cost; it is an investment in the future security and prosperity of our interconnected world. Ignoring this challenge will leave organizations increasingly vulnerable to the ever-growing threat of cybercrime.



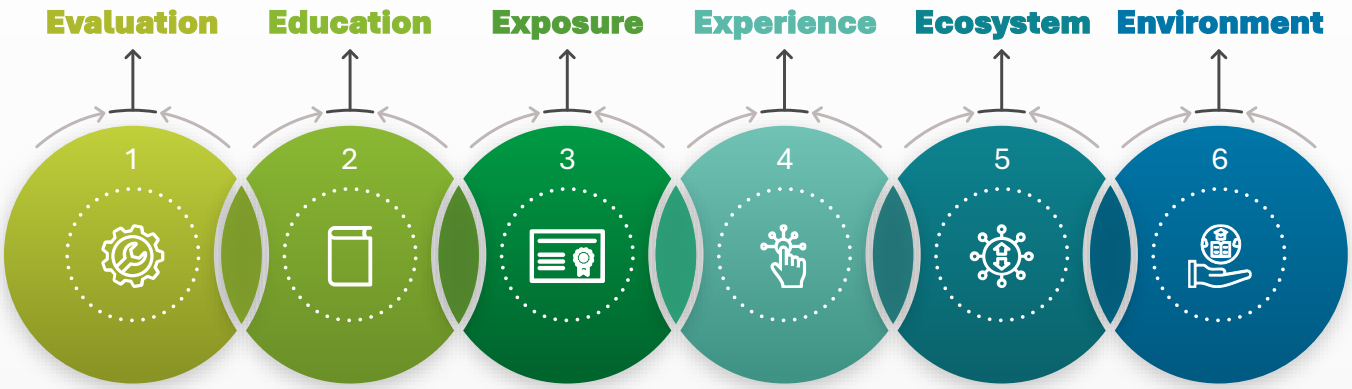
Section 2

Frameworks to continuously build cyber skills

Section 2: Frameworks to Continuously Build Cyber Skills

The rapidly evolving threat landscape is creating a critical need for organizations to strengthen their security posture through a skilled and adaptable workforce. A comprehensive approach to continuous development is required for building resilient organizations.

Our **6E Framework*** focuses on core aspects of continuous learning to ensure effective and sustained workforce development.



6E FRAMEWORK

1. ***Evaluation:*** This element involves a thorough analysis of the current skill levels of learners, identifying gaps and areas for improvement. It also includes evaluating the effectiveness of training programs to ensure they meet the desired outcomes and contribute to the overall development goals.
2. ***Education:*** Education is focused on creating customized curriculums that can adapt swiftly to changing needs. It leverages various learning modalities to cater to different learning preferences ensuring comprehensive capability development.
3. ***Exposure:*** This element emphasizes the importance of hands-on practice and continuous reinforcement of learned skills. It involves providing learners with opportunities to apply their knowledge in real-world scenarios, thereby solidifying their understanding and enhancing their proficiency.
4. ***Experience:*** This element puts learners at the center and focuses on designing interactive, engaging and personalized learning experiences that are memorable and high-impact.
5. ***Ecosystem:*** The ecosystem element highlights the importance of collaboration and partnerships in the learning process. It involves engaging with a network of external and internal partners, such as industry experts, educational institutions, and technology providers, to enrich the learning experience and provide diverse perspectives.
6. ***Environment:*** Environment refers to creating a supportive and accessible learning space. Whether physical, digital, or hybrid, it ensures that learners always have the necessary resources and tools available to facilitate continuous learning. This includes access to learning platforms, materials, and a conducive atmosphere that promotes a learning culture.

*Adapted from Deloitte's Continuous Learning Model [Get to know our Continuous Learning Model]

1. ***Evaluation:*** There are two types of evaluations included in this element. **The first** is pertaining to workforce capability assessment and the second is related to training effectiveness evaluation. To assess workforce capability, various evaluation methods can be used:

    i. **Technical and behavioral interviews:** assessors use a structured evidence-based approach to evaluate technical and behavioral skills.

    ii. **Knowledge based assessment:** these assessments focus on testing knowledge or principles, concepts, standards through multiple choice or qualitative questionnaires.

    iii. **Cognitive ability tests:** logical, numerical, and verbal reasoning tests can help assess problem-solving, analytical thinking, and learning agility.

    iv. **Capture the flag:** red/blue team challenges can be used to assess practical skills and teamwork.

    v. **Scenario-based assessment:** hypothetical scenarios are used to assess skills as candidates are asked to provide solutions, strategies or decisions.

    vi. **Practical assessment:** Simulations, hands-on-labs, coding challenges or practical real-world scenarios are designed to test candidates' skills, abilities, and application of knowledge.

    vii. **Psychometric assessment:** Personality or ability tests are structured assessments used to measure a variety of psychological attributes, including personality traits and behavioral styles.

We recommend aligning the assessment framework and tools to the organization's competency framework. Customized cybersecurity assessments can help organizations make better decisions on cyber and non-cyber talent management.

The second type of evaluation focuses on measuring the impact of learning. The Kirkpatrick Model is the most widely used for examining and evaluating training outcomes. It considers all types of training, both informal and formal, to establish aptitude using four tiers of criteria. It was introduced for the first time in 1959 by Donald Kirkpatrick.

Level 1: Reaction

What was the reaction of participants to the training?

Level 2: Learning

How much did the participants learn from the training?

Level 3: Behavior

Is there noticeable change in the behavior of the participants?

Level 4: Results

Have targeted outcomes been achieved?

2. ***Education:*** Education focuses on the development of comprehensive curriculums for education and training. Given below are critical components of curriculum development:

    i. **Competency framework:** Competencies are defined through knowledge, skills, abilities, and tasks that are required for different roles. This framework serves as the backbone of education and training.

    ii. **Training needs assessment:** A comprehensive analysis of needs based on surveys, assessments, analysis of demand, etc. is done to inform the curriculum.

    iii. **Training strategy:** A comprehensive strategy is developed with clear objectives, outline of training curriculum, description of delivery methods, resources, budget and timelines.

    iv. **Curriculum development:** Learning objectives are defined, and a robust curriculum is developed to cover the competencies and training needs holistically.

    v. **Content development:** Organizations can make a decision to build or buy content. Content should complement the learning pedagogy described in the training strategy.

    vi. **Pilot testing:** Once programs and courses have been developed, they need to be tested with a small group of learners to be updated or refined as needed.

3. ***Exposure:*** Exposure is about creating opportunities for learners to deepen learning. Exposure could be provided through:
    i. **Job shadowing:** Extend shadowing experiences to learners through which they can learn about tasks, application of knowledge and skills, workflows, etc. from experienced employees.
    ii. **Mentoring and coaching:** Assign cybersecurity experts as mentors and/or coaches to share experiences, advice, best practices and provide guidance to learners.
    iii. **Meetings & presentations:** Invite learners to attend team meetings, business presentations, strategy sessions to learn how concepts are applied.
    iv. **Cybersecurity conferences and events:** Provide opportunities for learners to connect and interact with experts, leaders, peers and others to gain insights.
    v. **Job rotation:** Offer rotation into different roles or functions to gather wider understanding about diverse roles and functions.
    vi. **Cyber incident case studies:** Provide real-world examples or case studies to learners to expose them to practical applications.
    vii. **Special projects:** Assign special or stretch projects to learners allowing them to stretch their abilities, learn new skills or apply existing skills in new ways.
    viii. **Hackathons and competitions:** Host hackathons and capture the flag competitions to provide learners the exposure to new tools, techniques and approaches.
    ix. **Cybersecurity communities and forums:** Provide opportunities to engage with cybersecurity communities and forums. Provides learners with new knowledge, information and practices that can be applied to their organization or role.
    x. **Cybersecurity simulations:** Use cyber range platforms or virtual labs where learners can practice defending networks, responding to attacks, or conducting penetration tests in a safe and controlled environment.
    xi. **Red/blue team exercises:** Create exercises where one group attacks (Red Team) and another defends (Blue Team), fostering practical skills in both offensive and defensive cybersecurity.

4. ***Experience:*** Learner experience includes the overall journey and interaction a learner has. This includes:
    i. **Content:** Relevance and quality of learning content that is tailored to learner needs.
    ii. **Learning delivery:** Instructional design approach, format of delivery and level of interactivity and engagement.
    iii. **User interface and accessibility:** Ease of navigation through learning platforms and materials including varied devices and inclusivity of different types of learners.
    iv. **Personalization:** Customization of learning paths based on learner types/ preferences, skill levels, functions and roles.
    v. **Support:** Availability of support in the form of helpdesk, cybersecurity experts as coaches/ mentors, materials, feedback on tasks/ assignments, etc.
    vi. **Engagement:** Continuous learner motivation and engagement through leaderboards, rewards, badges, etc.

5. ***Ecosystem:*** The learning ecosystem for cybersecurity training and education would consist of various partnerships, alliances, relationships, etc. that the entity has established:
    i. **Training and education partnerships:** Partnerships with universities/ academic institutions and/or with training providers for the development of training programs and content.
    ii. **Technology providers:** Relationship with companies/platforms supplying LMS, virtual labs, cyber ranges, and cybersecurity tools.
    iii. **Certification providers:** Relationship with organizations offering recognized cybersecurity certifications (e.g., CISSP, CEH).
    iv. **Industry partners:** Cybersecurity firms and organizations reputed for cybersecurity expertise.
    v. **Subject matter experts (SMEs) and trainers:** Experienced professionals, academicians and experts in cybersecurity.
    vi. **Alliances:** Strategic, formalized collaborations with vendors, government agencies, consortia, and institutions.
    vii. **Market relationships:** Network of interactions with employers, recruiters, industry bodies, and customers.

6. ***Environment:*** The learning environment consists of the physical, digital, or hybrid spaces that are critical for effective learning and development:
    i. **Physical:** The physical environment is constituted of the physical space including classrooms, collaboration spaces, labs, facilities and amenities that augment learning and development.
    ii. **Digital:** The digital environment refers to platforms and systems, connectivity and network, virtual labs and ranges for practical exercises which come together through a seamless learner experience.
    iii. **Hybrid:** The integration of physical and digital learning modes including tools for live streaming, interactive sessions providing learners with flexibility to use the modes for effective learning and development.

The **6E Framework** ties the crucial components for cyber workforce capability development together. It considers the principles for adult learning as well as the preferences of the modern learner in the era of diverse digital change and transformation.

Section 3

Design, implementation & measurement

Section 3: Design, implement, and measure

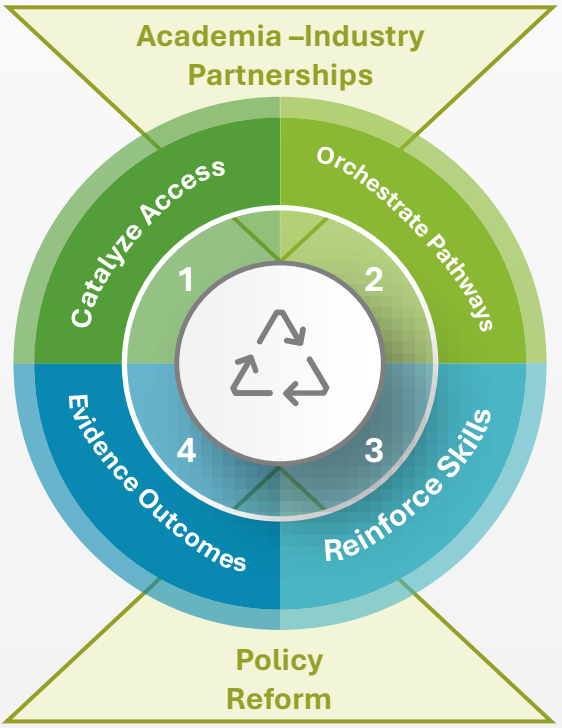
Strategies for designing and implementing effective cyber workforce transformation programs

The cybersecurity workforce gap isn't a problem we can solve with a single program. It is a system design challenge. When we fund scholarships without creating clear paths to employment, the result is frustrated graduates. When we run training programs without employer input or *real* buy-in, we create misalignment. Industry partnerships that lack policy support stay small and localized. And when we only measure participation instead of outcomes, we generate a lot of activity but not much actual **capability**.

What it needs, is a cohesive, scalable approach that treats talent development as an ecosystem. We need to deliberately engineer the feedback loops that make the system self-reinforcing over time. This section introduces a model that can help design programs, align stakeholders, and measure what *actually* matters when it comes to cybersecurity workforce capability development.

The CORE Loop Model

CORE Loop is a workforce development framework designed to build capability and capacity that compounds over time. Think of it as four interconnected phases brought together through two deeply binding needs:



1. ***Catalyze access:*** Remove barriers through scholarships, funding, and early exposure to widen entry into the field.
2. ***Orchestrate pathways:*** Build clear, stackable pathways that connect education, training, experience, and employment.
3. ***Reinforce skills:*** Support continuous upskilling through competency-based learning, modern curricula, and practice-rich environments.
4. ***Evidence outcomes:*** Create measurement and feedback systems that improve the model with each cycle.
5. ***Academia-industry partnerships:*** Develop education deeply aligned to industry needs.
6. ***Policy reform:*** The force multiplier across the entire framework, which reinforces the flywheel and reduces fragmentation.

Picture CORE as a flywheel. When you increase access, you get more participation. Clear pathways reduce drop-off. Skills reinforcement increase readiness. Evidence of outcomes builds trust and attracts investment, which then funds more access. Each element strengthens the others rather than operating in isolation.

1. Catalyze access: Scholarships and early talent activation

Scholarships as strategic investment, not just financial aid

We often think of scholarships as a financial aid mechanism. In the CORE model, they're a strategic capability investment with specific design requirements. The key is to target the real barriers, not just tuition. The most common obstacles include exam fees, devices, internet access, transportation, opportunity cost, childcare, and time. A scholarship that only covers tuition won't meaningfully expand the pipeline if these other barriers remain.

Instead of a single lump-sum award, design staged disbursement is tied to achievements like completing foundation skills, earning a first credential, or securing an internship placement. This improves persistence and transforms scholarships into a pathway tool rather than a one-time grant. And crucially, combine money with support structures. Mentorship, cohort-based learning, tutoring, career coaching, and mental health support reduce attrition and increase completion rates. Financial access alone is like trying to fill a leaky bucket.

Building the youth pipeline early

Developing young talent isn't about watering down the content or making cybersecurity easy. It's about introducing the right concepts at the right time. This means following a natural progression: cyber awareness leads to cyber literacy, which then leads to cyber practice. Awareness teaches safe behaviors. Literacy introduces concepts like identity, privacy, data integrity, and adversarial thinking. Practice involves labs, competitions, and real scenarios.

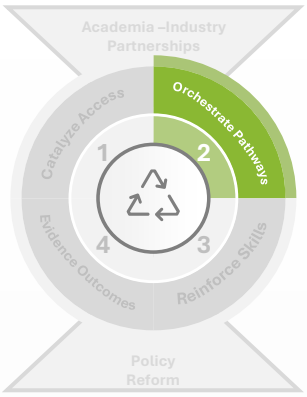
Just as importantly, we need to make career paths visible. Many students think 'cybersecurity = hacking.' Early programs should showcase the full range of roles—governance, risk, compliance, security operations, digital forensics, cloud security, application security, privacy engineering, and operational technology security—so students can self-select based on their strengths and interests.

Equity and inclusion as performance engineering

Cybersecurity desperately needs diverse problem-solving perspectives. But inclusion must be designed as a performance feature, not an afterthought. This means providing bridge programs for foundational skills in math and IT, offering flexible scheduling for working learners, creating multiple entry points (not everyone comes from a computer science background), and using bias-aware selection that values aptitude and motivation rather than just prior access. When done well, Catalyze Access expands the talent pool while maintaining standards. The rigor comes through competency demonstration and evidence in the later CORE phases.

2. Orchestrate pathways: Routes that actually lead somewhere

A major workforce challenge isn't just shortages—it's pathway confusion. People don't know what to learn, in what order, to qualify for which roles. Employers don't trust the signals they're seeing. Education providers aren't sure which outcomes to optimize for. CORE addresses this through deliberate pathway orchestration.



Pathway architecture: Stackable, role-aligned, experience-integrated

A functioning pathway needs four explicit layers working together. First, role profiles and competencies that define what 'job-ready' means in observable behaviors are needed.

Second, curriculum must be mapped to those competencies, specifying what gets taught and practiced. Third, work-based learning allows learners to prove capability in real conditions. Finally, hiring signals and placement agreements convert training into actual jobs. This architecture bridges the gap between 'learning' and 'employability.'

Graduate and early-career pathways

The common failure mode for graduates is academic learning that's conceptually strong but operationally thin. CORE closes this gap by building in capstone work that mirrors actual job deliverables: incident reports, risk assessments, threat models, cloud security baselines, identity and access management designs, and secure code reviews. Students also need live-fire practice environments like Security Operations Center (SOC) simulations, phishing response drills, vulnerability management cycles, and tabletop exercises. Even short work placements through guaranteed internships or rotations with partner organizations dramatically increase conversion to employment.

Apprenticeships and 'earned experience'

When entry-level roles require experience, apprenticeships solve the paradox by creating structured experience. These should be paid placements with defined competency checklists, dual mentorship from both academic and industry supervisors, and rotations across different functions like SOC, Governance, Risk, Compliance (GRC), cloud security, and Identity and Access Management (IAM). The key is assessment based on demonstrated tasks rather than just attendance. Experience is earned, and not just through logged hours.

Mid-career conversion pathways

One of the fastest ways to close the gap is converting people from adjacent roles: IT support staff, network administrators, developers, auditors, analysts, and engineers. CORE treats these as high-velocity lanes with diagnostic assessments to place learners efficiently, modular learning targeting specific gaps, and immediate job alignment; for example, converting developers to application security roles or auditors to governance and risk positions. Orchestrating pathways also reduces wasted training investment. When the pathway is clear, learners invest with confidence and employers invest because outcomes become predictable.

3. Reinforce skills: Training systems that keep pace with change

Cybersecurity changes too quickly for static curricula. Reinforcement is about building learning systems that update as threats, platforms, and practices evolve.

Competency-based education as the backbone

Time-based learning—measuring progress in seat hours—is a weak proxy for actual ability. CORE emphasizes competency-based design where you define competencies as observable actions, follow a cycle of teach → practice → assess → remediate, and let students progress based on mastery rather than time spent. This is how scholarships, pathways, and credentials become coherent;
everyone aligns to the same definition of 'ready.'

Curriculum modernization: From content-heavy to practice-rich

Reform doesn't mean abandoning theory. It means integrating theory with repeated practice. Teach security as a process, not just topics. Have learners repeatedly execute full cycles: asset inventory → risk assessment → control implementation → monitoring → incident response → post-incident improvement. Build tool fluency with conceptual grounding; tools change, but concepts persist. Teach the concepts first, then apply them with current tools so graduates can adapt when the tooling landscape shifts.

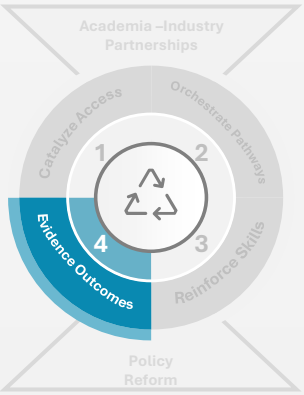
Just as importantly, emphasize communication skills. Cybersecurity work is inherently cross-functional. Learners must be able to write clearly, brief effectively, document thoroughly, and influence others. Technical excellence without communication skills is a career limiter.

Continuous Professional Development Infrastructure

To keep skills current, organizations and governments can institutionalize continuous professional development through annual learning minimums tied to role requirements, micro-credentials aligned to emerging needs like cloud security, AI security, operational technology, privacy engineering, practice communities and mentoring networks, and shared training resources across public and private sectors. Reinforcing skills also supports retention; professionals stay where growth is structured and visible.

4. Evidence outcomes: Measuring what matters

Workforce programs often measure what's easy: enrollment numbers, completion rates, and satisfaction scores. CORE measures what's useful: capability development, job conversion, and sustained performance.



The CORE measurement stack

A strong measurement system tracks five layers. It starts with inputs like funding, scholarships, instructors, lab capacity, and partner commitments.

It examines process quality through learner engagement, practice hours, mentorship access, and curriculum alignment. It captures outputs including credentials earned, projects completed, and competency assessments passed. It measures outcomes such as job placement rate, time-to-hire, role alignment, and internship-to-job conversion. Finally, it tracks impact: retention at 12 and 24 months, promotion velocity, skills currency, reduced vacancy duration, and improved organizational cyber posture.

Leading and lagging indicators

Both types of indicators are necessary. Leading indicators predict success early—practice completion rates, assessment mastery, and mentorship utilization enable rapid course correction. Lagging indicators confirm system value—retention rates, performance ratings, and promotions justify sustained investment. Together, they create a complete picture of system performance.

Feedback loops: Turning data into redesign

Measurement only matters if it changes decisions. CORE requires an explicit improvement cadence: quarterly employer feedback on graduate performance, curriculum refresh every 6–12 months, scholarship criteria adjusted based on persistence and outcomes, and pathways updated based on labor market shifts. This is how the system improves each cycle rather than repeating the same mistakes.

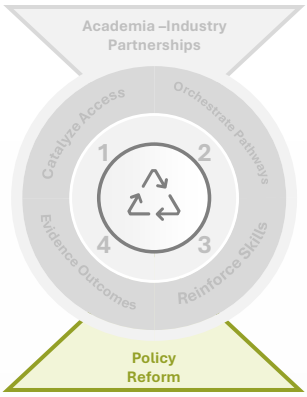
5. Academia–industry partnerships: The transmission belt

What makes partnerships operational

Partnerships often exist as memoranda of understanding with limited operational impact. In CORE, partnerships are engineered to produce three concrete outputs: shared competency frameworks and role profiles, co-designed learning experiences including projects, labs, and capstones, and conversion mechanisms like internships, apprenticeships, and hiring pipelines.

Operational partnerships require joint governance through a shared steering committee with actual decision-making authority. They involve shared assets like cyber ranges, datasets, case libraries, and lab environments. They include shared people—adjunct practitioners, visiting faculty, and co-supervised capstones. Most critically, they create shared incentives: employers get talent pipeline, academia gets placement outcomes, and governments get capability and resilience. Partnerships also enhance measurement—employers can validate whether graduates perform on the job and feed that evidence back into curriculum redesign.

6. Policy reform: The multiplier across CORE



Policy isn't a separate pillar. It's a force multiplier across all four CORE elements. When designed thoughtfully, policy reinforces the flywheel and reduces fragmentation.

Policy levers that strengthen the system

To strengthen access, policy can provide scholarship funds and tax incentives for employers who sponsor learners, targeted support for underrepresented groups and high-need regions, and funding for K–12 cyber literacy and teacher training.

To strengthen pathways, policy can establish standards for apprenticeships and paid work-based learning, create public procurement requirements that encourage training-to-hire partnerships, and streamline recognition of non-traditional credentials where competency can be validated.

To strengthen skills reinforcement, policy can provide incentives for institutions to adopt competency-based models, fund cyber ranges, labs, and simulation environments, and require curriculum refresh cycles and industry advisory boards.

To strengthen evidence and outcomes, policy can create data sharing frameworks that respect privacy while enabling outcome tracking, establish common reporting standards for workforce programs, and tie performance-based funding to placement, retention, and progression metrics.

Implementation blueprint: Putting CORE in motion

A practical rollout can follow these six steps. First, define priority roles and competency profiles: Start narrow, then expand as you learn what works. Second, map existing programs to competencies to identify gaps and redundancies in your current system. Third, design scholarships as progression instruments with staged support and mentoring rather than one-time funding. Fourth, build pathways with conversion agreements by creating internships, apprenticeships, and hiring commitments with partner organizations. Fifth, modernize learning delivery to make it practice-rich, competency-based, and modular. Finally, stand up a measurement dashboard with shared metrics, governance structures, and regular review cadence. Success depends on governance—you need a cross-sector body that owns role definitions, quality standards, funding alignment, and reporting.

Emerging trends & future directions

Emerging trends & future directions

Around the world, the cybersecurity workforce is undergoing a profound transformation driven by the accelerating adoption of AI, automation, and other emerging technologies. These advancements are reshaping the nature of cybersecurity work, disrupting traditional job roles, and redefining the competencies required for future professionals. As security operations become more technology-driven, organizations are rethinking how to build, train, and sustain cyber talent.

Globally, AI-enabled platforms are already performing complex functions once reserved for human analysts such as threat detection, log correlation, anomaly identification, and automated incident response. According to a 2024 Deloitte survey of global CISOs, **39% are using AI capabilities** in their cybersecurity programs to a large extent. This is contributing to the rise of new hybrid roles such as AI threat analysts, cyber data scientists, and cloud security architects that blend cybersecurity expertise with data science, automation, and systems thinking. These roles are increasingly central to future workforce planning, yet many traditional cybersecurity education pathways still lag in addressing these interdisciplinary demands.

The shift toward automation is also **reshaping human value** within security functions. Routine tasks such as patch management, log analysis, vulnerability scanning are increasingly handled by intelligent systems, shifting human focus to higher-order skills such as adversarial thinking, contextual risk assessment, digital ethics, and strategic decision-making.

Globally, upskilling and reskilling have become strategic priorities, with the World Economic Forum estimating that half of the workforce will require significant reskilling by 2030. Cybersecurity is one of the sectors most affected.

In this global context, the Middle East faces both a challenge and an opportunity. As regional governments and industries drive ambitious digital transformation agendas, the adoption of AI and automation in cybersecurity is accelerating. National visions, particularly in the Gulf Cooperation Council (GCC) increasingly position **AI as a cornerstone of digital resilience**, with several countries integrating intelligent systems into national security strategies.

However, the **regional talent landscape remains under strain**. Many local workforces are still building foundational cybersecurity capacity, and education systems often lack the agility to incorporate fast-evolving skill demands. The rise of AI-driven security operations necessitates an urgent pivot toward more flexible, modular, and interdisciplinary training models. Institutions must foster capabilities in areas like algorithmic transparency, cyber governance, data privacy, and machine learning, disciplines that are currently underrepresented in many regional curricula.

For Middle Eastern organizations, this means **redefining cybersecurity** not just as a technical function, but as a strategic, cross-cutting capability. Career pathways must evolve to reflect new realities, with employers leading efforts to design role-based training, support continuous learning, and embed cyber thinking across business units. Moreover, **ethical and regulatory** concerns around AI such as decision accountability, data governance, and model explainability are no longer optional knowledge areas. They are becoming essential to building **digital trust**, particularly in sectors like finance, energy, and government.

Ultimately, AI and automation are not eliminating cybersecurity roles; they are **transforming them**. A future-ready cyber workforce in the Middle East, and globally, will be one that is adaptive, ethically grounded, and equipped to work alongside intelligent systems. Those who act early to **align workforce strategies** **with these emerging realities** will be best positioned to **lead in a rapidly evolving digital world.**

Regional case studies

Regional case studies

There are numerous real-world examples of successful initiatives focused on transforming the workforce by developing cyber skills throughout the citizen's lifecycle. These case studies offer valuable insights into effective strategies for cultivating a proficient cyber workforce. By analyzing these examples, we can identify best practices and lessons learned that can be adapted to address the current challenges faced both in the Middle East and globally.

Case Study 1: National Cybersecurity Workforce Enablement Program (NCWEP)

The NCWEP is a national initiative designed to close the cybersecurity talent gap by developing a more **diverse, inclusive, and capable cyber workforce**. It is structured around two distinct workstreams tailored to different talent segments. The Cyber Women Workstream empowers women through targeted mentoring, coaching sessions, exchange and rotation programs, international women's celebration events and cybersecurity competitions. Simultaneously, the Job Seekers Workstream connects emerging talent with industry needs via employment fairs, awareness campaigns, apprenticeships, and success stories.

This 18-month-long initiative has driven measurable impact, including a 26% increase in women's participation in the cyber workforce and a 29% increase in certified cybersecurity professionals.

Key lessons learned include the importance of persona-based programming**, industry collaboration,** and storytelling to boost visibility and motivation. Tailored engagement strategies and alignment with labor market demand are also critical to attracting and retaining diverse talent.

Case Study 2: Cybersecurity Workforce Capability Development (CWCD)

The CWCD Program, led by a regional government entity, aims to build internal cyber capabilities through a structured, institutionalized approach. Central to the program is a **Cyber Academy**—a physical and digital learning environment that supports both independent and collaborative learning. It also features a **cyber career development framework** that outlines roles, competencies, and career progression pathways tailored to the entity's industry and weaved into their talent management framework.

The initiative also included cyber assessments across various domains and strategically placing the entity's cyber workforce in tailored learning pathways based on their strengths, interests, and the entity's needs, which included identifying necessary training and certifications.

The program also included uplifting the cyber maturity of the entire workforce of the organization through a blend of awareness campaigns, workshops, bootcamps, online courses, and interactive events such as annual cybersecurity weeks.

Key outcomes include improved cyber maturity across departments, and the development of **specialized cybersecurity experts** in emerging risk domains, tailored to the entity's strategic needs.

Lessons learned highlight the value of **collaboration and alignment with top universities**, and strong partnerships with the organization's stakeholders, and consistent performance tracking to demonstrate return on investment.

Case Study 3: GRADUATE DEVELOPMENT PROGRAM (GDP)

The GDP Program was launched by a leading technology company in KSA to recruit and develop top Saudi graduates in cybersecurity and digital fields, building a **sustainable talent pipeline** to support both organizational growth and the Kingdom's digital transformation agenda. The program was structured around a five-phase approach, including benchmarking global practices, assessing current capabilities, designing a graduate development framework, developing training modules with industry experts, and launching through onboarding and skills training.

Key outcomes include the creation of a **scalable graduate program model**, alignment of graduate capabilities with organizational priorities, and the establishment of a sustainable pipeline of Saudi cyber talent.

Lessons learned emphasize the importance of **academic and ministry collaborations** for talent sourcing, clear eligibility and selection criteria, and the integration of both technical and professional skills training to ensure graduates transition effectively into the workforce.

Global best practices

There are numerous real-world examples of successful initiatives focused on transforming the workforce by developing cyber skills throughout the citizen's lifecycle. These case studies offer valuable insights into effective strategies for cultivating a proficient cyber workforce. By analyzing these examples, we can identify best practices and lessons learned that can be adapted to address the current challenges faced both in the Middle East and globally.

International best practices

Globally, countries have taken strategic steps to tackle the cybersecurity skills shortage. These models offer practical lessons for the Middle East.

In the United States, the NICE Framework by NIST standardizes cyber job roles and competencies, serving as a foundation for workforce planning and education alignment.

The UK's CyberFirst program focuses on early engagement, offering scholarships, training camps, and internships for school and university students, resulting in a surge of interest in cybersecurity careers.

Singapore's SG Cyber Talent initiative, led by the Cyber Security Agency, is a holistic public-private ecosystem that includes scholarships, capture-the-flag competitions, and mid-career reskilling schemes.

Meanwhile, Australia's Cyber Security Skills Partnership Innovation Fund, managed by the Australian Government, supports collaborative projects between training providers and employers to build cyber skills aligned with industry needs. It targets underrepresented groups, promotes hands-on experience, and funds sector-specific training initiatives.

Across these programs, common success factors include having inclusive talent engagement, clearly defined cyber career frameworks, immersive and gamified learning environments, and strong collaboration between government, academia, and the private sector.

For the Middle East, adapting these practices will require localizing frameworks to suit regional workforce dynamics, embedding cyber into national education systems, and building incentive structures that promote long-term career progression and retention.

Recommendations & Conclusion

Recommendations & conclusion

Addressing the cybersecurity talent gap in the Middle East requires an integrated approach that connects skills development, experiential learning, and employment through clear pathways. By aligning competency-based learning, outcome-driven measurement, partnerships, and enabling policy, governments and organizations can build a resilient cybersecurity workforce at scale.

Recommendations

Addressing the cybersecurity workforce gap requires coordinated system design rather than isolated interventions. Based on the CORE Loop Model, the following three recommendations are proposed.

1. **Establish integrated, role-aligned cybersecurity talent pathways:** Design end-to-end pathways that connect access, education, training, and employment around clearly defined cybersecurity roles. Treat scholarships as capability investments tied to skill attainment and work placement. Embed internships, apprenticeships, and simulations to ensure learners demonstrate job readiness and transition efficiently into employment.
2. **Adopt competency-based, practice-rich learning models:** Shift from time-based instruction to competency-based education that prioritizes demonstrated performance. Modernize curricula to reflect real operational workflows and evolving threats. Support continuous upskilling through modular learning, micro-credentials, and experiential training, while strengthening communication and cross-functional skills for cyber operations.
3. **Align measurement, partnerships, and policy to scale outcomes:** Measure workforce success through outcomes such as job placement, time-to-hire, retention, and performance progression. Operationalize academia–industry partnerships through shared governance and accountability. Use policy to align funding with outcomes, standardize work-based learning, recognize credentials, and enable system improvement.

Conclusion

Closing the cybersecurity talent gap in the Middle East requires more than expanding training capacity or increasing participation. It demands a system-level approach that deliberately connects access, learning, experience, and employment into a self-reinforcing ecosystem. This paper demonstrates that fragmented interventions, such as isolated scholarships, unaligned curricula, or activity-based metrics, are insufficient to build sustainable cyber capability.

The CORE Loop Model provides a practical framework for translating strategy into execution by integrating six mutually reinforcing elements: Catalyze Access, Orchestrate Pathways, Reinforce Skills, Evidence Outcomes, Academia–Industry Partnerships, and Policy Reform. When designed and governed as a flywheel, these elements compound over time, increasing workforce readiness, employer confidence, and institutional resilience.

By emphasizing competency-based education, practice-rich learning, and outcome-driven measurement, the model aligns talent development with real operational demand. Operational partnerships and enabling policy act as force multipliers, accelerating scale while reducing fragmentation. Implemented collectively, this approach enables governments, industry, and academia to move beyond short-term fixes and build a resilient, future-ready cybersecurity workforce aligned with national priorities and long-term economic growth.

Appendix

Abbreviations:

AI = Artificial Intelligence

CORE = Catalyze Access, Orchestrate Pathways, Reinforce Skills, Evidence Outcomes

CISO = Chief Information Security Officer

CWCD = Cyber Workforce Capability Development

GDP = Graduate Development Program

GRC = Governance, Risk, and Compliance

HR = Human Resources

ICT = Information and Communications Technology

ITU = International Telecommunication Union

KPI = Key Performance Indicator

KSA = Kingdom of Saudi Arabia

NICE = National Initiative for Cybersecurity Education

OECD = Organization for Economic Co-operation and Development

OJT = On-the-Job Training

PPP = Public-Private Partnership

STEM Science, Technology, Engineering, and Mathematics

WEF = World Economic Forum

Bibliography:

- World Economic Forum. Global Cybersecurity Outlook. World Economic Forum.
- Organization for Economic Co-operation and Development (OECD). Skills for a Digital World. OECD Publishing.
- International Telecommunication Union (ITU). Global Cybersecurity Index. United Nations.
- National Institute of Standards and Technology (NIST). National Initiative for Cybersecurity Education (NICE) Framework. U.S. Department of Commerce.
- World Bank. Building Digital Talent and Skills for the Future. World Bank Group.
- United Nations Educational, Scientific and Cultural Organization (UNESCO). Future of Education and Skills 2030. UNESCO.
- Deloitte. Global Cybersecurity Workforce and Skills Insights. Deloitte.
- Deloitte. Cyber Workforce Transformation: Bridging Skills, Experience, and Outcomes. Deloitte Middle East.

References:

1. “Global Cybersecurity Outlook 2025”, World Economic Forum, 13 January 2025
2. “Global Cybersecurity Index, 5TH Edition”, International Telecommunication Union, 2024
3. “NICE Cybersecurity Workforce Framework (NIST SP 800-181 Rev. 1)”, National Institute of Standards and Technology (NIST), 2020
4. “The Future of Jobs Report 2025”, World Economic Forum, 7 January 2025
5. “The Global future of Cyber Survey, 5th Edition”, Deloitte, 2024
6. “How the GCC is strengthening its cyber resilience in the digital age”, World Economic Forum, 2025
7. Kimheaney, “Cyber Security in the Middle East: 2025 Trends and Talent”, Engage-ID, 5 September 2025
8. “How to Combat Cybersecurity Talent Gap in the Middle East”, MENews247, 2024
9. Ludo Fourrage, “United Arab Emirates Cybersecurity Job Market: Trends and Growth Areas for 2025”, 25 Feburary 2025
10. “Digital Jobs and Skills”, World Bank Group, 10 April 2025
11. “Skills for a Digital World”, OECD, 2 June 2016

Authors

Amira Khattab
Partner

Amira has over 20 years of experience in Education, Talent Development, Cyber, and Technology Services and leads the Cyber Education practice across the MENA region, working with regional and multinational organizations.

Shagun Ahuja
Director

Shagun is a Defense Human Capital leader with over 16 years experience in workforce transformation. She leads learning advisory and has steered several capability development initiatives including building resilient organizations.

Angela Terry
Director

Angela has wide experience leading the design and delivery of workforce transformation projects across the public sector within national and local government organizations, primarily operating within the defense industry.

Lindsay Thorburn
Director

Lindsay has over 25 years' experience in the delivery of highly secure, available and interoperable networks for Defense. He has experience in AI governance implementation, risk management and maturity assessments.

Daniel McCoy
Senior Manager

Daniel has a wide range of experience leading large-scale programs in Government, Defense, and Financial Services, implementing GRC frameworks, identifying, managing and mitigating risks, and promoting security awareness.

Ahmed Ovais
Senior Manager

Ovais has 22 years of experience advising Defense, Public Sector, and Financial Institutions on risk management and cyber resilience. His work includes strengthening organizational preparedness and building national cyber resilience capabilities.

Sulaiman Almaiman
Senior Manager

Sulaiman specializes in public sector strategic transformation and has deep experience in the KSA Defense context, focusing on human capital development and the localization of emerging technologies capabilities.

Habiba Emara
Business Analyst

Habiba is part of the Cyber Strategy & Transformation team and specializes in developing and delivering Cybersecurity Training & Awareness programs. She has supported multiple projects across the UAE and KSA, within the defense & financial sectors.

Deloitte.

Together makes progress