Global Cyber Security Capacity Centre
OXFORD MARTIN SCHOOL
UNIVERSITY OF OXFORD
DEPARTMENT OF COMPUTER SCIENCE

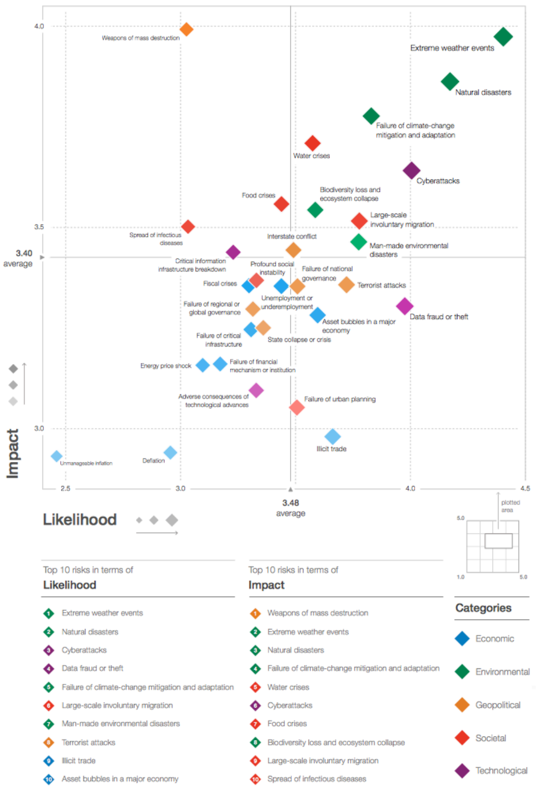
Global Cybersecurity Education Needs Assessment: Discussion Resource Paper

Need for Cybersecurity Capacity-Building

Cybersecurity – An increasing global risk[1]

Cybersecurity risks are growing, both in their prevalence and in their disruptive potential. Attacks against businesses have almost doubled in five years, and incidents that would once have been considered extraordinary are becoming more and more commonplace. The financial impact of cybersecurity breaches is rising, and some of the largest costs in 2017 related to ransomware attacks, which accounted for 64% of all malicious emails. Notable examples included the *WannaCry* attack—which affected 300,000 computers across 150 countries—and *NotPetya*, which caused quarterly losses in excess of US$300 million for a number of affected businesses. Another growing trend is the use of cyberattacks to target critical infrastructure and strategic industrial sectors, raising fears that, in a worst-case scenario, attackers could trigger a breakdown in the systems that keep societies functioning.

Figure I: The Global Risks Landscape 2018



Source: World Economic Forum Global Risks Perception Survey 2017–2018.
Note: Survey respondents were asked to assess the likelihood of the individual global risk on a scale of 1 to 5, 1 representing a risk that is very unlikely to happen and 5 a risk that is very likely to occur. They also assess the impact on each global risk on a scale of 1 to 5 (1: minimal impact, 2: minor impact, 3: moderate impact, 4: severe impact and 5: catastrophic impact). See Appendix B for more details. To ensure legibility, the names of the global risks are abbreviated; see Appendix A for the full name and description.

Getting the International Development Community to Care About Cybersecurity[2]

While aid recipients are increasingly interested in investing in cybersecurity, three factors prevent them from doing so: (1) the complexity and highly technical nature of cybersecurity and risk-management sometimes leaves aid recipients unsure where to start; (2) the perception that internet access and cybersecurity are competing for political attention and finances; and (3) cost.

The Delhi Communiqué[3]

This output from the Delhi *Global Conference on Cyber Space* Provides an example of an effort by the global community to drive workforce development; it is endorsed by all members of the Global Forum on Cyber-Expertise (GFCE) and reaffirms their shared commitment to strengthen cyber-capacity and expertise globally.

ICT and the SDGs[4]

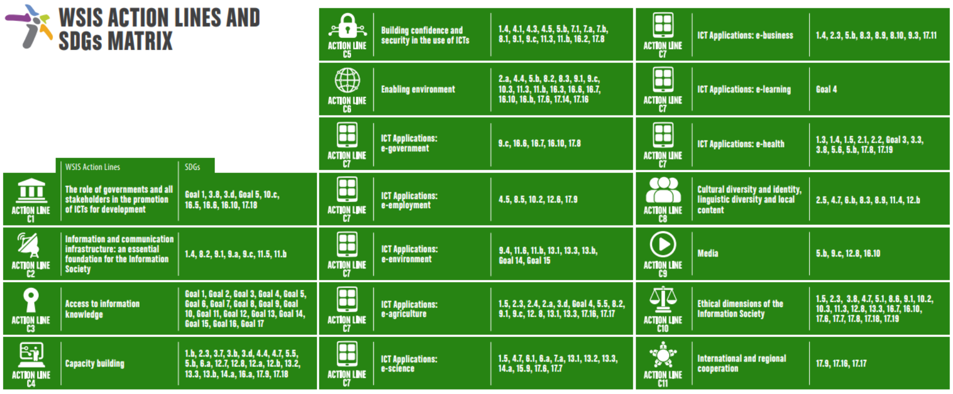
The United Nations' Sustainable Development Goals (SDGs) and associated targets will stimulate action until 2030 in areas of critical importance for humanity and the planet. Information and Communication Technologies (ICTs) form the backbone of today's digital economy and have truly enormous potential to fast-forward progress on the SDGs and improve people's lives in fundamental ways. A paper[5] from the IGF 2017 Best Practice Forum on Cybersecurity provides a mapping of how cybersecurity issues impact upon a number of the SDGs.

1 NO POVERTY
2 ZERO HUNGER
3 GOOD HEALTH AND WELL-BEING
4 QUALITY EDUCATION
5 GENDER EQUALITY
6 CLEAN WATER AND SANITATION
7 AFFORDABLE AND CLEAN ENERGY
8 DECENT WORK AND ECONOMIC GROWTH
9 INDUSTRY, INNOVATION AND INFRASTRUCTURE
10 REDUCED INEQUALITIES
11 SUSTAINABLE CITIES AND COMMUNITIES
12 RESPONSIBLE CONSUMPTION AND PRODUCTION
13 CLIMATE ACTION
14 LIFE BELOW WATER
15 LIFE ON LAND
16 PEACE, JUSTICE AND STRONG INSTITUTIONS
17 PARTNERSHIPS FOR THE GOALS

---

[1] http://www3.weforum.org/docs/WEF_GRR18_Report.pdf
[2] https://www.cfr.org/blog/getting-international-development-community-care-about-cybersecurity
[3] https://www.thegfce.com/documents/publications/2017/11/24/delhi-communique
[4] https://www.itu.int/en/sustainable-world/Pages/default.aspx
[5] http://www.intgovforum.org/multilingual/index.php?q=filedepot_download/4904/1017

Linking WSIS Action Lines with Sustainable Development Goals[7]
The WSIS mapping exercise draws direct linkages to the WSIS Action Lines from the proposed SDGs, to continue strengthening the impact of ICTs for sustainable development. Each UN Action Line Facilitator has analysed the connections and relations of their respective Action Line with the proposed SDGs and their targets. This is a living document and changes can be introduced by Action Line Facilitators, if needed. The goal is to create a clear and direct link and an explicit connection between the key aim of the WSIS, that of harnessing the potential of ICTs to promote and realize the development goals, and the post-2015 development agenda, so as to contribute to the realisation of the latter. As illustrated in the *WSIS Action Lines and SDGs Matrix* below, there is an explicit link between achievement of the SDGs and the work of the world information society. Consideration of cybersecurity and other related ICT factors will be crucial to the safe and efficient achievement of the SDGs, and thereby the improvement of the quality of life of all citizens of the world.



WSIS ACTION LINES AND SDGs MATRIX

	WSIS Action Lines	SDGs
ACTION LINE C1	The role of governments and all stakeholders in the promotion of ICTs for development	Goal 1, 3.8, 3.d, Goal 5, 10.c, 16.5, 16.6, 16.10, 17.18
ACTION LINE C2	Information and communication infrastructure: an essential foundation for the Information Society	1.4, 8.2, 9.1, 9.a, 9.c, 11.5, 11.b
ACTION LINE C3	Access to information knowledge	Goal 1, Goal 2, Goal 3, Goal 4, Goal 5, Goal 6, Goal 7, Goal 8, Goal 9, Goal 10, Goal 11, Goal 12, Goal 13, Goal 14, Goal 15, Goal 16, Goal 17
ACTION LINE C4	Capacity building	1.b, 2.3, 3.7, 3.b, 3.d, 4.4, 4.7, 5.5, 5.b, 6.a, 12.7, 12.8, 12.a, 12.b, 13.2, 13.3, 13.b, 14.a, 16.a, 17.9, 17.18
ACTION LINE C5	Building confidence and security in the use of ICTs	1.4, 4.1, 4.3, 4.5, 5.b, 7.1, 7.a, 7.b, 8.1, 9.1, 9.c, 11.3, 11.b, 16.2, 17.8
ACTION LINE C6	Enabling environment	2.a, 4.4, 5.b, 8.2, 8.3, 9.1, 9.c, 10.3, 11.3, 11.b, 16.3, 16.6, 16.7, 16.10, 16.b, 17.6, 17.14, 17.16
ACTION LINE C7	ICT Applications: e-government	9.c, 16.6, 16.7, 16.10, 17.8
ACTION LINE C7	ICT Applications: e-employment	4.5, 8.5, 10.2, 12.6, 17.9
ACTION LINE C7	ICT Applications: e-environment	9.4, 11.6, 11.b, 13.1, 13.3, 13.b, Goal 14, Goal 15
ACTION LINE C7	ICT Applications: e-agriculture	1.5, 2.3, 2.4, 2.a, 3.d, Goal 4, 5.5, 8.2, 9.1, 9.c, 12. 8, 13.1, 13.3, 17.16, 17.17
ACTION LINE C7	ICT Applications: e-science	1.5, 4.7, 6.1, 6.a, 7.a, 13.1, 13.2, 13.3, 14.a, 15.9, 17.6, 17.7
ACTION LINE C7	ICT Applications: e-business	1.4, 2.3, 5.b, 8.3, 8.9, 8.10, 9.3, 17.11
ACTION LINE C7	ICT Applications: e-learning	Goal 4
ACTION LINE C7	ICT Applications: e-health	1.3, 1.4, 1.5, 2.1, 2.2, Goal 3, 3.3, 3.8, 5.6, 5.b, 17.8, 17.19
ACTION LINE C8	Cultural diversity and identity, linguistic diversity and local content	2.5, 4.7, 6.b, 8.3, 8.9, 11.4, 12.b
ACTION LINE C9	Media	5.b, 9.c, 12.8, 16.10
ACTION LINE C10	Ethical dimensions of the Information Society	1.5, 2.3, 3.8, 4.7, 5.1, 8.6, 9.1, 10.2, 10.3, 11.3, 12.8, 13.3, 16.7, 16.10, 17.6, 17.7, 17.8, 17.18, 17.19
ACTION LINE C11	International and regional cooperation	17.9, 17.16, 17.17

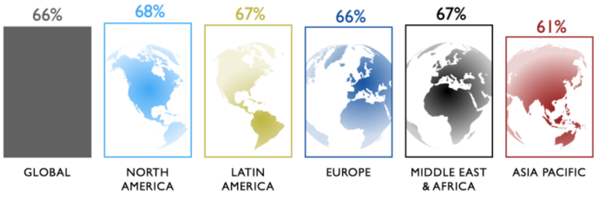
Need for Cybersecurity Education and Training

Global cybersecurity skill shortage

- The deficit of cybersecurity talent is a challenge for every industry sector. The lack of trained personnel exacerbates the already difficult task of managing cybersecurity risks.[8]
- A joint 2017 Enterprise Strategy Group (ESG) research project with the Information Systems Security Association (ISSA) found that 70% of cybersecurity professionals claimed their organisation was impacted by the cybersecurity skills shortage.

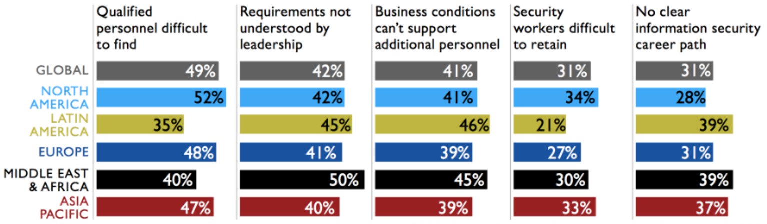
Regional perspectives on skills shortages[9]
In 2015, Frost & Sullivan forecasted a 1.5-million-worker shortage by 2020. In the light of recent events and shifting industry dynamics, that forecast has been revised to a shortage of 1.8 million workers by 2022. This is reflected by the extraordinarily high number of professionals across the globe who indicate that there are not enough workers in their departments.

Too Few Information Security Workers in My Department:



Source: *2017 Global Information Security Workforce Study, (n = 19,175)*

Reasons for Worker Shortage by Region:



Source: *2017 Global Information Security Workforce Study, (n = 12,709)*

---

[7] https://www.itu.int/net4/wsis/sdg/

[8] https://www.mcafee.com/us/resources/reports/rp-hacking-skills-shortage.pdf

[9] 2017 Global Information Security Workforce Study *Benchmarking Workforce Capacity and Response to Cyber Risk.* A Frost & Sullivan Executive Briefing.

ASEAN: A nascent local cybersecurity industry with shortages of home-grown capabilities and expertise[10]

The cybersecurity industry in the ASEAN region faces structural challenges because of its highly fragmented nature. In addition, the shortage of skilled talent impacts the competitiveness of the local industry. Building capacity is a long-term effort. With the majority of ASEAN member states lacking a structured and long-term approach to developing competent cybersecurity professionals, the emerging member states must rapidly adopt best practices from countries that have implemented capacity-building frameworks.

Building Cybersecurity & Resilience in a Digital Africa[11]

Cybersecurity talents are becoming increasingly difficult to find in today's ever-growing and dynamic technology world. Solving the growing cybersecurity challenges requires skilled young cybersecurity professionals who are proactive and willing to combat existing cybersecurity threats. There is also a clear need for governments and enterprises to provide an enabling environment buoyed by a relevant educational curriculum designed to attract and groom these talents. One major solution to this would be developing policies to suit our peculiar environment and identifying critical barriers to innovation to address, and thus enable Africa to achieve increased productivity and structural transformation of its economies.

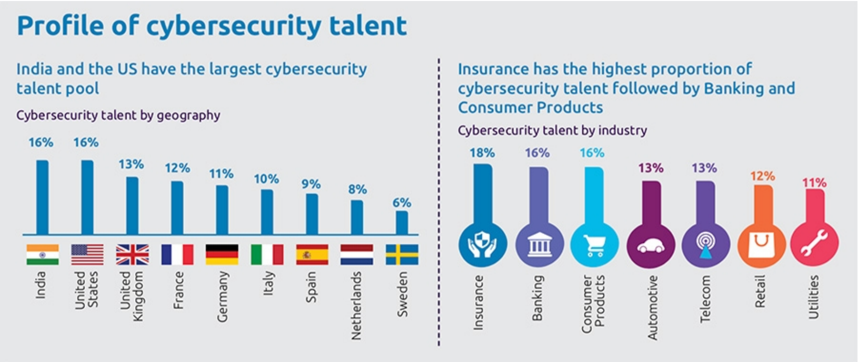
Developed/Higher-Income Nations[12]

The eight countries selected for this study—Australia, France, Germany, Israel, Japan, Mexico, the United Kingdom (UK), and the United States (USA)—reflect a diversity of sizes, educational systems, income levels, and political structures. This study looked at four dimensions of their cybersecurity workforce-development efforts: total cybersecurity spending, education programs, employer dynamics, and public policies. The study's findings are based on open-source data, targeted interviews with experts, and an eight-nation survey of information technology (IT) decision makers in both public and private sector organizations.

- Respondents in all countries surveyed said cybersecurity education was deficient. Eighty- two percent of respondents report a shortage of cybersecurity skills. More than three out of four (76%) respondents believe their government is not investing enough in cybersecurity talent.
- This shortage in cybersecurity skills does direct and measurable damage, according to 71% of respondents. One in three say a shortage of skills makes their organisations more attractive targets for hacking. One in four say that insufficient strength of cybersecurity staff has damaged their organisation's reputation and led directly to the loss of proprietary data through cyberattack.
- High-value skills are in critically short supply, the most scarce being intrusion detection, secure-software development, and attack mitigation. These skills are in greater demand than soft skills in communication and collaboration. A majority of respondents (53%) said that the cybersecurity skills shortage is worse than talent deficits in other IT professions.

Multi-Nation profile of cybersecurity talent[13]

Globally, the nations which are currently best placed in terms of this skills gap are India and the USA. The countries host a combined 32% of the world's cybersecurity talent (16% each). The UK is third, closely followed by France (12%), and Germany (11%), and while these nations are the best endowed in terms of talent, they still exhibit a gap. In terms of provision by business sector, Insurance leads the way, hosting 18% of cybersecurity talent. Banking and consumer products follow closely behind, at 16% each.



Global digital skills deficit[14]

As we see new demand for digital capability exponentially escalate, organizations across many industries are in danger of a human capital shortage. Shortages in critical digital skills sets could see digital and technology specialists commanding rising salaries. Organizations need a new employment and engagement models that takes a different approach to matching current capability with a strategic plan and the future capability requirements. Otherwise, we are likely to see a repeat of the capability crises in mining and oil, with organizations finding themselves over paying for skills that quickly become redundant.

---

[10] Cybersecurity in ASEAN: An Urgnet call to action - ATKearney

[11] Building Cyber Security & Resilience in a Digital Africa. Publication by KPMG in Nigeria - May 2017

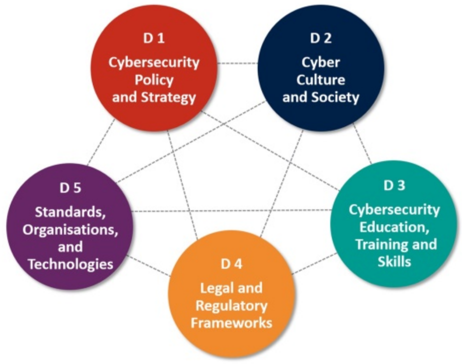
[12] Hacking the skills shortage. A study of the international shortage of cybersecurity skills. Centre for strategic and international studies. McAfee.

[13] https://www.consultancy.uk/news/16068/majority-of-companies-now-hit-by-a-cybersecurity-skills-gap

[14] Is digital creating a workforce capability crisis - Ernst and Young

Lessons learnt from the research of the GCSCC

The Cyber Security Capacity Maturity Model (CMM) considers national cybersecurity capacity across five dimensions. These five dimensions cover the broad expanse of areas that make up the essential national cybersecurity capacity. They consist of a number of factors, and all factors are considered with respects to five levels of maturity. The CMM outlines what a country should expect to be able to do in each factor of each dimension, for each level of maturity, and so the evidence that is required to convince that a level has been achieved. It is a guided self-assessment model that can help a country understand both its current maturity in each dimension, and also the types of capacity-building that would need to be undertaken to further mature capacity in any area, as prescribed by the model. Countries are then able to prioritise capacity-building investments, according to their needs, the harms they wish to address, and the risks that concern them most. The dimensions naturally overlap, as capacity in some areas will depend upon capacity in others. The relationships between aspects of dimensions and the harms that countries seek to address are a topic for on-going research at the GCSCC, where we seek to develop an increasing data-driven evidence-base for these connections, and also identify the most effective capacity-building measures for addressing harms. In order for a country to develop capabilities across all five dimensions, education and training will be critical. Firstly, there is a need to ensure that the government's own education and training programmes can connect all of this information together and convert it into appropriate content and channels to meet their local context most effectively. Secondly, there will be specific education and training requirements needed to support the development of maturity within and across all dimensions of the CMM for all stakeholders involved in delivering the national capacity. Here lessons can be drawn from Dimension 3 of the CMM, "*Cybersecurity Education, Training and Skills*", which provides an insight into types of national cybersecurity capacity-building requirements.


D 1
Cybersecurity Policy and Strategy
D 2
Cyber Culture and Society
D 3
Cybersecurity Education, Training and Skills
D 4
Legal and Regulatory Frameworks
D 5
Standards, Organisations, and Technologies

The GCSCC is in the process of developing a holistic and robust model for understanding the harm experienced by nations as a result of a lack of capacity, and how this can be reduced. Grounded theory is applied to understand how cyber-harm manifests for a nation and its citizens, the current limitations in detecting and measuring it, as well as the needs for enhanced response strategies and controls. Our initial focus-groups and interview results suggest that an overwhelming majority of research participants (85% of them) identified education as a fundamental area where capacity-building is required. There is an educational need across the full range of possible stakeholders affected by cyber-harm, specifically for groups of people who hold key roles in their organisations (board members and managers) as well as more vulnerable groups (such as teenagers and elderly people). Apart from training courses in cybersecurity and general education regarding phishing emails and other trending threats, it is also evident from our research that cyber-risk is underestimated. Risk appetites are socially determined, and unless cybersecurity risk becomes part of the mainstream, people will continue to overlook it. Therefore, educational efforts should focus on making these risks more tangible to individuals. Developing education courses focusing on understanding harm, and proposing effective channels to communicate its effects to a wider public are essential. For these education topics, in many cases the knowledge already exists, but needs to be developed into an educational offering. In other cases, there is a knowledge gap that will require research before educational offerings can be designed. One clear priority area for research is in the area of understanding harm arising from cyber-attacks or a lack of cybersecurity.

In conclusion, while the International Community has developed offerings in specific areas (e.g., training for law-enforcement officers and judges in the law as it applies to cyberspace and cybersecurity; training for first-responders on malware techniques; education for CNI business leaders on risk awareness in the face of cyber-threat), there is no broad coverage of the entirety of the education and training need. The resulting risk is that we may be investing in areas of educational capacity but limiting their impact because they depend upon other aspects of cybersecurity capacity that are not sufficiently invested in. What is required is an analysis of the full spectrum of educational requirements, and the development of a template national education strategy that countries can easily adopt and adapt as they seek to mature aspects of their national cybersecurity capacity.

Consequence of inaction

> *"The cybersecurity skills shortage represents an existential threat to developed nations that rely on technology as the backbone of their economy, critical infrastructure, and society at large."* [15]

Significant improvements in the way the global community approaches the education and training of cybersecurity competencies and professionals is required in order to begin to close the skills deficit. Failure to do so will result in wide ranging and globally linked barriers to the achievement of the sustainable development goals and the ability to harness and share in the benefits of technological development.

---

[15] https://www.csoonline.com/article/3247708/security/research-suggests-cybersecurity-skills-shortage-is-getting-worse.html