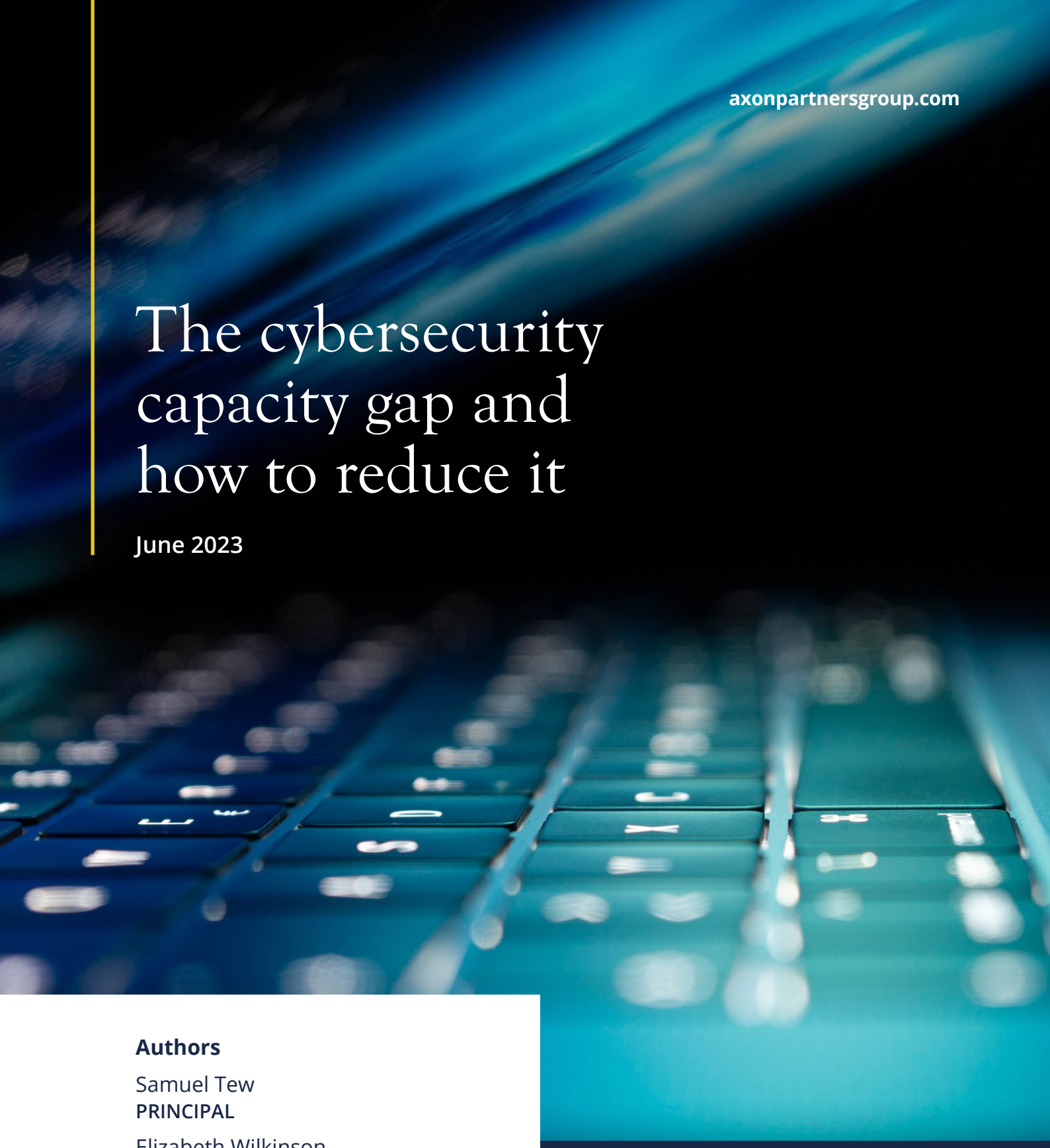

axonpartnersgroup.com

The cybersecurity capacity gap and how to reduce it

June 2023

Authors

Samuel Tew
PRINCIPAL

Elizabeth Wilkinson
SENIOR ASSOCIATE

Alberto Martinez
ASSOCIATE

AXON

Cybercrime is on the rise. But the supply of cybersecurity skills and solutions is failing to match growing demand. Capacity building can solve this problem, paving the way for a cybersecure future and laying the foundations to match short-, medium-, and long-term needs.

This paper explores how it can be done and why a tailored capacity-building strategy is crucial.

Abstract

The growth and complexity of cybercrime have led to increasing demand for cybersecurity solutions and services. However, supply is not keeping pace with this demand. In fact, there is a global lack of capacity to meet current and future cybersecurity needs. This is caused by shortfalls in the human and technological infrastructure, resources, and knowledge needed to properly defend against evolving cyber threats – in both the public and private sectors. One answer to this problem is cybersecurity capacity building, through which countries and organisations proactively ensure their cybersecurity capacity in the face of continuing growth and evolution in the threat landscape. Capacity-building strategies are required both to meet current needs and to lay the foundations for the future. This article explores three essential areas for governmental capacity-building plans – people and skills; technology, infrastructure and R&D; and knowledge-sharing and awareness – by looking at real-world applications of each.

Contents

1. Capacity building in context

In recent years, the demand for cybersecurity solutions and technology has grown – and will continue to grow. Digitalisation and a sharp increase in digital technologies have given rise to new fronts for cybercrime and new types of cyberattacks.[1]

It's true that digitalisation can bring socio-economic development and increased standards of living. However, it can also bring increased systemic risks and profitable opportunities for malicious threat actors. The financial cost of cyberattacks increased over 800% from 2018 to 2022. This trend will continue.

In recent years, the demand for cybersecurity solutions and technology has grown – and will continue to grow

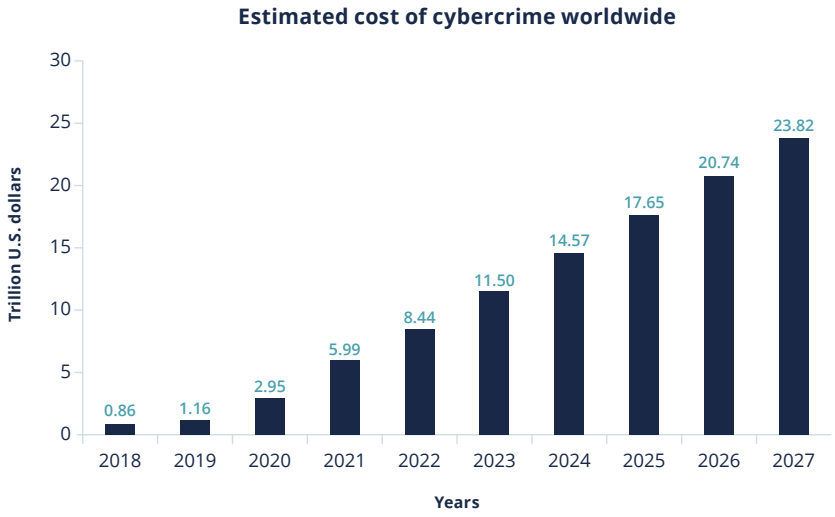

Figure 1: Cybercrime cost is predicted to grow in coming years[2]

However, demand for cybersecurity solutions is outpacing supply. Faster development of cybersecurity capabilities could help to meet this demand and combat the rising number, variety and complexity of cyber threats. Building cybersecurity capacity is key to this. But doing that isn't quite as simple as it sounds.

Faster development of cybersecurity capabilities could help to combat the rising number, variety and complexity of cyber threats

1 Global Cybersecurity Outlook 2023 published by World Economic Forum: https: www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf

2 Statista Technology Market Outlook: https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until 2027/#:~:text=According%20to%20estimates%20from%20Statista's,to%20%2423.84%20trillion%20by%202027

Three elements of cybersecurity capacity are particularly relevant here – and are the main focus of this article:

- **Talent:** the development of human capacity: professionals with the training and skills to tackle cybersecurity challenges.
- **Technology:** increasing the availability of and access to cyber solutions and services.
- **Awareness:** widening access to cybersecurity knowledge and information.

These are fundamental elements of cybersecurity. Developing them requires strategic planning to ensure that they will be sufficiently developed to meet expected future demand.

At the government level, the term 'cybersecurity capacity building' refers to the efforts of countries and organisations to proactively ensure their long-term cybersecurity capabilities in anticipation of the continued growth and evolution of the threat landscape.

Increasing cybersecurity efforts is clearly important, but progress has been limited due to a shortage of resources or capacity in the three areas described above. For example, the global cybersecurity workforce gap expanded from an estimated 2.7 million in 2021[3] to 3.4 million in 2022[4] and could widen further due to accelerated digitalisation across industries and the high employee resignation rate in the cyber field[5]. Nearly 70% of organisations say they have a shortage of cybersecurity workers[5]. This shortage affects companies' ability to meet new threats. Over 32% of organisations were unable to identify the root cause of a breach[6], while only 19% were highly confident in their ability to prevent or respond to a cyberattack[7]. Funds are a particular problem for small businesses; only 8% have a dedicated cybersecurity budget[8].

The global cybersecurity workforce gap rose from an estimated 2.7 million in 2021 to 3.4 million in 2022 and is predicted to increase steadily every year

Nearly 70% of organisations say they have a shortage of cybersecurity workers. This shortage affects companies' ability to meet new threats

3 (ICS)2 CYBERSECURITY WORKFORCE STUDY, 2021; Available at: https://iapp.org/media/pdf/resource_center/ISC2_Cybersecurity_Workforce_Study_2021.pdf

4 (ICS)2 CYBERSECURITY WORKFORCE STUDY, 2022; Available at: https://www.isc2.org//-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx

5 Trellix Survey Findings; Available at: https://www.trellix.com/en-us/about/newsroom/stories/perspectives/trellix-survey-findings-a-closer-look-at-the-cyber-talent-gap.html

6 Data Breach Investigations Report; Available at: https://www.verizon.com/business/resources/reports/2020-data-breach-investigations-report.pdf

7 The State of Cyber Resilience Report by Marsh and Microsoft; Available at: https://www.marsh.com/uk/about/media/increased-ransomware-attacks-global-threats-executive-confidence-cyber-preparedness.html

8 Forbes; Available at: https://www.forbes.com/sites/forbestechcouncil/2022/10/03/its-time-for-smbs-to-protect-against-cyberattacks-and-build-resiliency/?sh=1418c5ba7e5f

These capacity gaps have limited short-term solutions and, without further action, will widen. Strategic planning and investment are required for the medium- and long-term. So who can build appropriate strategies? The national security implications of poor cyber-resilience, and the overlap between societal interests and developments in human capacity, technological capacity, and security awareness may provide the answer. Governments are uniquely well-placed to coordinate national strategies to build capacity – in partnership with the resources of the private sector.

Strategic planning and investment are required for the medium- and long-term. So who can build appropriate strategies?

2. Capacity-building initiatives

There are various initiatives that governments can take in their approach to cybersecurity capacity building. These are:

- **People and skills** – Developing human capacity by nurturing talent, increasing the number of cybersecurity professionals, or otherwise improving workforce planning.
- **Technology, infrastructure and R&D** – Increasing the availability of cybersecurity solutions within the market – and increasing access to those solutions.
- **Knowledge-sharing and awareness** – Disseminating cybersecurity knowledge to segments of the population or market that currently lack it.

Each of these areas may be targeted individually, However, addressing all three is fundamental to combatting the growing threat of cyberattacks. How that could be done is explained below.

A widening workforce gap is creating increased demand for cybersecurity professionals. However, supply has so far failed to match demand

2.1. People and skills

As explained above, the global cybersecurity workforce gap stood at 3.4 million in 2022[5] and is set to widen due to accelerated digitalisation across industries, along with more, and more varied, cyberattacks. This widening workforce gap is creating increased demand for cybersecurity professionals. However, supply has so far failed to match demand.

Things may not improve any time soon. Surveys suggest a high turnover of industry workers. In fact, many cybersecurity professionals state that they are planning to leave the industry in the next two years – potentially up to a third of the current workforce[6]. The top frustrations cited by surveyed professionals were a lack of support for the development of skills (36%), a lack of recognition for the good cybersecurity can do for society (36%), and limited support for those trying to gain the necessary qualifications and certifications (32%).

Surveys suggest a high turnover of industry workers. In fact many cybersecurity professionals state that they are planning to leave the industry in the next two years

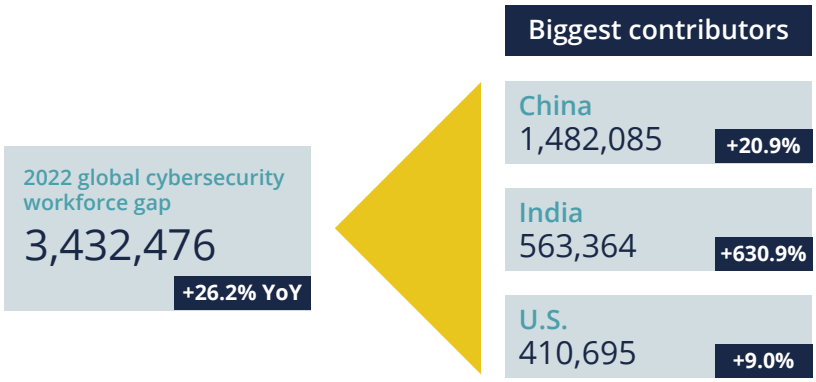

Figure 2: The global workforce gap grew by 26% in 2022, with variation across countries.[5]

Among those planning to leave the profession, the most common reasons cited were tied to a lack of accomplishment or passion for the job. And yet, simply by increasing awareness of the diverse paths available within cybersecurity, providing support for skills development and increasing opportunities for career progression, employers could address these sources of frustrations and retain employees.

Then there is the issue of diversity – or lack of it. Perceptions of the cybersecurity industry as an unfriendly environment for certain ethnic groups (cited by 13% of respondents) or for women (8%) appear among the top 10 reasons for leaving. The industry cannot afford to alienate parts of the available workforce; increasing the available pool of workers means appealing to as many people as possible.

Given that companies already struggle to hire qualified professionals, this situation poses serious challenges for the public and private sectors worldwide as both the rate and complexity of cyberthreats rise.

At a government level, action can be taken in a range of areas, from initiatives to increase the availability and quality of cybersecurity degrees and skills programmes for young people and future professionals, to retraining the current workforce through targeted programmes. Other options include increasing the size of the available workforce through diversity schemes and reducing reliance on human professionals through the adoption of technology alternatives such as AI.

Cybersecurity requires a high level of training or experience. Increasing the number, quality, and accessibility of cybersecurity qualifications and attracting students is therefore the main route towards building cybersecurity talent for the future. This need for development in education and training programmes aligned with the requirements of the cybersecurity industry is emphasised by the OECD[9], which recommends engaging employers in the design and delivery of programmes. But increasing the quality or availability of cybersecurity training requires funds to turn such initiatives into a practical reality and increase their uptake.

The government can increase the availability and quality of cybersecurity degrees, retrain the current workforce, promote diversity schemes, and adopt AI technology to reduce reliance on human professionals

Action must also be taken to remedy the shorter-term workforce gap. Practical apprenticeship schemes which combine study with experience on the job or retraining of existing staff are attractive and efficient ways to do this. Organisations that offer initiatives to train internal talent, such as rotating job assignments, mentorship programmes and encouraging employees outside of cybersecurity to join the field, tend to have fewer shortages in cybersecurity staff[5].

As for diversity, while the representation of women has risen significantly from around 10% in 2013 to 25% in 2022[10], fewer women choose cybersecurity careers than men. A huge part of the population is not being leveraged for cybersecurity. Increasing its appeal to ethnic minority groups may likewise offer an untapped pool of potential in many countries.

But there is another, newer way to address the workforce gap: the application of artificial intelligence to automate routine tasks and augment cybersecurity capabilities. This frees up professionals for the more complex tasks which require human judgement. It may also increase the capabilities open to cybersecurity teams in the fight against cybercrime. AI has even been used to help identify employees with strong skills in different roles who may be open to retraining[11].

These four aspects can and should be integrated into a cybersecurity skills strategy designed to address the workforce gap.

The UK's Department for Education coordinates a wide variety of cybersecurity training programmes that lead to formal qualifications. Programmes range from degrees, lower-level basic skills modules and government-funded skills bootcamps to corporate apprenticeships through active government engagement with companies. Multiple policies have been implemented in the UK in an effort to attract young and adult learners from diverse backgrounds to the field. These include learning experiences for women and guidance on how to engage with local learning pathways. These policies are supported by financial subsidies to increase participation in cybersecurity education and training, especially targeting the most disadvantaged young people and adults[12].

Fewer women choose cybersecurity careers than men. A huge part of the population is not being leveraged for cybersecurity

There is another, newer way to address the workforce gap: the application of artificial intelligence to automate routine tasks and augment cybersecurity capabilities

9 OECD report, "Building a Skilled Cyber Security Workforce in Five Countries"; Available at: https://www.oecd-ilibrary.org/employment/building-a-skilled-cyber-security-workforce-in-five-countries_5fd44e6c-en

10 Women in Cybersecurity 2022 Report; Available at: https://cybersecurityventures.com/wp-content/uploads/2022/09/Women-In-Cybersecurity-2022-Report-Final.pdf

11 Forbes; Available at: https://www.forbes.com/sites/forbestechcouncil/2023/04/06/can-ai-help-solve-the-workforce-skills-gap/

12 UK National Cyber Strategy 2022; Available at: https://www.gov.uk/government/publications/national-cyber-strategy-2022

2.2.
Technology, infrastructure and R&D

In 2021, the value of the global cybersecurity market reached USD 150 billion, growing at an impressive rate of 12.4%[13] . Considering that in 2021 80% of the observed threat groups and 40% of the observed malware had never been seen before, the market clearly needs to be constantly evolving to cope with new cyberthreats. Nonetheless, the addressable market for cybersecurity is estimated to stand at a staggering USD 2 trillion, or about ten times the size of the market currently covered by vendors and solutions.

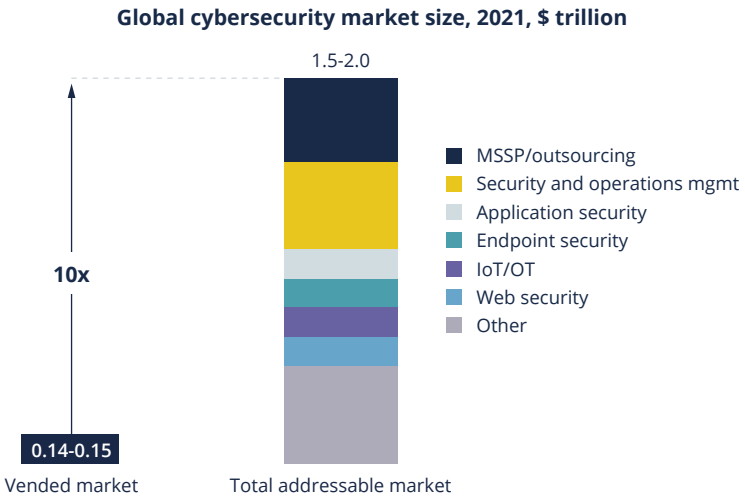

Figure 3: Global cybersecurity market size, 2021. Comparison between addressable and vended market

The addressable market for cybersecurity is estimated to stand at a staggering USD 2 trillion, or or about ten times the size of the market currently covered by vendors and solutions

According to McKinsey, the segments with the greatest supply gap are security and operations management and managed security services, which together represent about 40-50% of the total addressable market, with an application, endpoint, IoT/OT and Web security together representing about 30%. This demonstrates a need for the availability of both a services market (personnel and infrastructure offered as outsourced solutions) and technology development (availability of cybersecurity products).

13 McKinsey; Available at: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/new-survey-reveals-2-trillion-dollar-market-opportunity-for-cybersecurity-technology-and-service-providers

The current market gap may be partly down to a lack of skills. However, there are other factors. For example, regulatory certification schemes for cybersecurity vendors have gained popularity in recent years, as they allow markets to be governed more easily and may ensure high levels of quality and service. However, they can also create high entry barriers, which can in turn raise prices within that market. Regulation can be a double-edged sword.

The problem calls for active initiatives to be employed to keep pace with the market growth and decrease the gap between the addressable versus vended market

Other initiatives are therefore needed. Governments must mobilise efforts to drive innovations within the industry and support companies in enhancing their existing capabilities. This can be done by targeting various areas. Here we highlight three:

- Fostering innovation.
- Increasing access for businesses.
- Market stimulation.

Governments must mobilise efforts to drive innovations within the industry and support companies in enhancing their existing capabilities

Innovation in the market most often comes from corporate and academic R&D or the start-up field. Supporting one of these areas, or simply promoting collaboration and the sharing of ideas within them, can help to increase the level of capability within a country. In less developed markets, such innovation doesn't have to be ground-breaking; it can simply consist of bringing contemporary technologies and business models to a country.

Initiatives such as provision of access to finance can be effective ways of supporting innovation. For example, the European Union Agency for Cybersecurity (ENISA) has launched the first Access-2-Finance[14] series. This aims to mobilise more investment in cybersecurity in Europe. The European Investment Bank (EIB)[15] also provides financing for cybersecurity projects in Europe.

14 ECCC, Access-2-Finance Series; Available at: https://cybersecurity-centre.europa.eu/news/first-access-2-finance-series-2023-03-29_en

15 EIB, 2022; Available at: https://www.eib.org/en/press/all/2022-279-eib-and-gd-ventures-to-invest-in-cybersecurity-and-trust-tech-startups

CyberCall, the Cyber Security Agency of Singapore (CSA)'s Cybersecurity Call for Innovation, invites cybersecurity companies to participate in developing innovative solutions to address targeted cybersecurity challenges. These solutions are then made available for commercial adoption.[16] CSA regularly invites ideas from industry to identify high-priority target areas and gathers lists of end users who are looking for solutions to specific problems. Participants are then invited to develop innovative and commercially adaptable solutions to these problems which will later be marketed in the country. The 2022 security areas included five emerging technology categories – among them AI, cloud and OT.

Small and medium-sized businesses often have limited budgets for cybersecurity, making it difficult for them to invest in the necessary tools and services to fully protect their digital assets

Small and medium-sized businesses often have limited budgets for cybersecurity, making it difficult for them to invest in the necessary tools and services to fully protect their digital assets. Around 60% of SMBs experienced at least one cyberattack in the last year[17], yet only 8% of businesses with fewer than 50 employees have a dedicated budget for cybersecurity. Many of these organisations still include cybersecurity in their overall IT (or other technology departments') budget[18]. It could therefore be a viable option for government to support such businesses with their cybersecurity budget through public mechanisms such as grants and other funding, promoting investment in the local market while circumventing additional cybersecurity costs that may ultimately be borne by public vehicles such as national or regional CERTs.

16 Cybercall 2022; Available at: https://cybercall.sg/wp-content/uploads/2022/08/CyberCall-2022-Challenge-Statements.pdf

17 State of IT security in SMBs; Available at: https://cdndevolutions.blob.core.windows.net/documents/survey-report/survey-report-2022-2023.pdf

18 Forbes; Available at: https://www.forbes.com/sites/forbestechcouncil/2022/10/03/its-time-for-smbs-to-protect-against-cyberattacks-and-build-resiliency/?sh=1418c5ba7e5f

In order to improve national resilience towards cyberthreats, Finland's government provides a funding scheme for companies registered in Finland operating in a critical sector[19]. The initiative provides:

- up to €15,000 for the inspection and assessment of information systems, procurement aimed at improving information security, training of personnel or skills development or any other corresponding measure that develops the information security of enterprises. This fund is only open to small or medium-sized enterprises.
- up to €100,000 for an attack-prevention test – a test of the readiness level of the main electronic services or a direct measure that improves information security as a result.

Where countries have limited social and economic resources, alternative methods may be more feasible. These include public-private partnerships, whereby governments may partner with the private sector and/or international organisations. This can be a powerful option for strengthening technical capabilities in the market. An example is Cybersecurity Defence Africa (CDA) a cybersecurity services company created by the Republic of Togo in 2019 through a public-private partnership with Asseco Data Systems (ADS). CDA offers a range of services, including Security Operations Centre (SOC) services (for profit) and Computer Emergency Response Team (CERT) services (non-profit) for government agencies and critical infrastructure providers. The CDA was established based on a 2:1 split of ownership between the Togolese government and ADS; it was financed using debt from a local bank.

Where countries have limited social and economic resources, alternative methods may be more feasible. These include public-private partnerships.

19 Finnish Transport and Communications Agency Traficom; Available at: https://www.kyberturvallisuuskeskus.fi/en/apply-support-development-information-security

Due to an urgent need for cyber protection of national infrastructure, and given limited financial and human resource availability, Cybersecurity Defence Africa (CDA) was established in the Republic of Togo as a private entity catering for government and private sector cybersecurity needs.

The services it offers include a Security Operations Centre (SOC), providing 24/7 real-time monitoring and event management services for organizations. In addition, CDA provides audit and penetration testing services to test, assess and improve the security level of an organisation's information systems by identifying strengths and weaknesses. CDA also offers training to company teams to develop their skills and capabilities in cybersecurity.

In turn, the creation of a stable market offering has made feasible the creation of cybersecurity regulatory controls for critical infrastructure providers. CDA is aiming to develop its offering further and to expand in order to provide its services throughout Africa.

Market stimulation initiatives aim to establish connections between suppliers and businesses and promote trade

Finally, market stimulation initiatives aim to establish connections between suppliers and businesses and promote trade. In Europe, the European Cyber Security Organisation (ECSO) has launched several initiatives to support the cybersecurity industry[20]. One of these initiatives is Cyber Investor Days – matchmaking events where cybersecurity investors, SMEs and start-ups meet to explore investment opportunities via pitch and training sessions, B2B meetings and other networking activities[21]. There is also the European Cybersecurity Investment Platform (ECIP), which aims to promote investments in European cybersecurity start-ups and SMEs[22].

The ECSO Market Radar[23] is a tool which provides representation for the European cybersecurity market, including cybersecurity product vendors, service providers and consultancy offerings. It gathers over 200 companies and provides visibility to the European cybersecurity industry while increasing market transparency. The tool is divided into five categories: identification, protection, detection, response and recovery.

20 ECS; Available at: https://ecs-org.eu/activities/market-deployment-investments-and-international-collaboration/

21 Cyber Investor Days; Available at: https://ecs-org.eu/activities/cyber-investors-days/

22 European Cybersecurity Investment Platform; Available at: https://ecs-org.eu/activities/european-cybersecurity-investment-platform/

23 Market Radar; Available at: https://ecs-org.eu/activities/market-radar/

2.3. Knowledge-sharing and awareness

Cyber-attackers may use not only technological avenues but also target people, for example obtaining user credentials to access private or corporate systems via phishing emails or scams. Up to 94% of malware may be delivered by email through socially engineered phishing scams; this is also a key entry point for ransomware attacks[24].

Cybersecurity awareness and education for all citizens have been recognised as priorities by intergovernmental organisations

While anti-phishing tools provide improved detection capabilities, a key driver for preventing such attacks is still people and their ability to recognise false emails, messages and interfaces. As a result, cybersecurity awareness and education for all citizens have been recognised as priorities by governments, such as the USA, UK, Singapore and Australia.

Raising cybersecurity awareness among the public can be done through information campaigns. In the USA, one such awareness initiative is the website 'Stop.Think.Connect', which offers educational resources and practical tips on cybersecurity through topics such as social media security, online shopping, mobile security and identity theft prevention. The campaign was launched in 2010 as a joint initiative between the U.S. federal government and several private sector and non-profit organizations. In Europe, meanwhile, European Cyber Security Month (ECSM), the EU's annual cybersecurity awareness campaign in October targeting citizens and organisations, noted that 73% of member states found that the campaigns reduced cyber incidents[25].

In the corporate sphere, providing security awareness training to employees has many benefits:

- 80% of organisations that provide cybersecurity awareness training to their employees have seen improvements, including a reduction in cyber incidents[26] and increased employee awareness of security risks[27].
- After user behaviour analytics and privileged access management – both of which require technical implementation – simple user training and awareness provided the biggest cost saving: an average of $3 million per year[28].
- 80% of businesses that provide regular security awareness training to their employees experience a quantifiable reduction in susceptibility to phishing attacks[27].
- Employees who received regular awareness training could be up to 5.2 times less likely to click on risky links than those without[29].

24 Acronis Cyberthreats Report 2022; Available at: https://www.acronis.com/en-us/blog/posts/acronis-cyberthreats-report-2022-unveils-cyberthreat-predictions/

Despite this, as of 2019, only 57% of organisations provided regular cybersecurity training for their employees[30]. As a result, governments are stepping in to increase cyber awareness not only among their state employees but also among the wider public and staff in critical industries.

Governments are stepping in to increase cyber awareness not only among their state employees but also among the wider public and staff in critical industries

Scotland's Cyber Resilient Strategic Framework[31] aims to increase cyber resilience through awareness-raising and engagement by disseminating general and targeted cyber awareness messages to individuals, groups, and communities, and ensuring these are available in accessible or alternative formats.

With this in mind, the CyberScotland Partnership was launched as a source of information and resources on cybersecurity awareness, including cyber services and incident response as well as other related capacity-building issues. CyberScotland functions as a collaboration of key strategic stakeholders, running awareness campaigns such as "DIGI Ken" adverts for basic public cybersecurity, and CyberScotland Week, a week focused on awareness-raising.

In addition, funding of £500,000 is provided to extend cyber resilience training to more than 250 organisations[32] through online and in-person workshops for public services and third-sector health, housing, and social care bodies with critical roles in societal functioning.

25 European Cybersecurity Month (ECSM) 2021 Deployment Report; Available at: https://www.enisa.europa.eu/publications/european-cybersecurity-month-2021-deployment-report

26 2021 State of the Phish Report; Available at: https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-state-of-the-phish-2021.pdf

27 ISACA State of Cybersecurity 2022 report; Available at: https://www.isaca.org/-/media/files/isacadp/project/isaca/resources/white-papers/state-of-cybersecurity-2022_whpsc22_res_eng_0322.pdf?mod=djemCybersecruityPro&tpl=cy

28 Cost of Insider Threats Global Report 2020, IBM; Available at: https://www.ibm.com/downloads/cas/LQZ4RONE

29 Mimecast, 2020; Available at: https://www.mimecast.com/blog/cyber-awareness-training-helps-defend-users-from-brand-spoofing-attacks/

30 GetApp survey, 2019; Available at: https://www.getapp.com/resources/cybersecurity-statistics/

31 Scottish Government; Available at: https://www.gov.scot/publications/strategic-framework-cyber-resilient-scotland/pages/3/

32 Scottish Government, 2022; Available at: https://www.gov.scot/news/cyber-security-boosted/

Developing countries often face specific cybersecurity challenges, including awareness at the policymaker level. This makes it harder to respond to the emerging threat landscape as access to the internet and online channels increases[33]. In fact, threats coming from online channels are often more developed than the capability within the country to combat them.

In order to improve cybersecurity in developing countries, critical infrastructure must be strengthened, and existing regulatory/policy frameworks must be developed. Accessing international best practices and knowledge can boost a country's capacity-building efforts. There are also free initiatives and resources that can be accessed to help developing nations learn from each other and improve their knowledge and cybersecurity.

There are free initiatives and resources that can be accessed to help developing nations improve their knowledge and cybersecurity

The ITU's 'Cyber4Good Initiative' (C4G) aims to give developed countries (LDCs) access to digital services, tools, products, and insights that they would not otherwise have been able to access – or would not have had the resources to access. Participant service providers offer products, tools, and services to LDCs under favourable conditions to allow for the quick uptake of digital services by target beneficiary countries. Axon Partners Group has actively participated in this initiative, providing five LDCs with services relating to the development of their national cybersecurity strategies.[34]

There is also the Global Forum on Cyber Expertise (GFCE), a multi-stakeholder community with more than 170 members and partners across the world aiming at strengthening cyber capacity and expertise globally. The community hosts several initiatives and programmes related to capacity building. One such initiative is the African Cybersecurity Conference, which aims to raise awareness and build capacity on cybersecurity resilience to assist Africa's digital transformation. Knowledge is transferred through workshops in order to develop the capacity of key African stakeholder groups (such as law enforcement, policymakers, the judiciary, parliamentarians and diplomats)[35].

33 NUPI Report, Cyber Security Capacity Building in Developing Countries; Available at: https://cybilportal.org/wp-content/uploads/2020/06/NUPIReport03-15-Muller.pdf

34 Cyber for Good, ITU; Available at: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Cyber4Good/Cyber4Good.aspx

35 GFCE, 2022; Available at: https://thegfce.org/regional-initiatives-on-cyber-security-awareness/

3. Considerations for initiative implementation

From a public policy perspective, many areas need to be addressed to improve cybersecurity capacity. While each area can be addressed individually, it is crucial to recognise the interrelationship of three in particular:

- People and skills.
- Technology, infrastructure and R&D.
- Knowledge-sharing and awareness.

Policymakers should consider establishing comprehensive initiatives that span these areas.

Below, we offer a high-level phased approach that policymakers can adopt as a starting point for their cybersecurity capability development programme.

Stage 1 – Make a maturity assessment

A useful first step, as always with policy development, is to gain an understanding of the current situation. An initial study, assessing the current state of maturity across the three areas, is essential to identify current capacity levels and gaps.

By conducting such a study, policymakers, organisations and stakeholders can gain valuable insight into the strengths and weaknesses of their current cybersecurity capabilities. This will help them prioritise efforts and allocate resources effectively.

For example, on the human capability side, such an assessment could be based on the availability (or otherwise) of qualified cybersecurity professionals, their average years of experience, their capabilities and know-how, and the adequacy of existing training and education programmes. It might also examine the available infrastructure and technological capabilities, assessing factors such as the levels of compliance of local security systems with local or international standards, the use of advanced technologies, and the integration of key cybersecurity services across different sectors and organisations. Finally, on the awareness side, the survey might measure current levels of awareness of cybersecurity risks and best practices among individuals, businesses

From a public policy perspective, many areas need to be addressed to improve cybersecurity capacity. While each area can be addressed individually, it is crucial to recognise the interrelationship of three in particular

and the general public. This could involve general surveys or the use of quantitative data around human-related cybersecurity incidents.

By analysing the results of this study, policymakers should be able to identify the broad areas requiring implementation and prioritise whatever is most needed to address the national gaps identified within each area.

Stage 2 – Assess suitable options for initiatives

Having decided which areas most urgently need public capacity-building initiatives, the next step should be to determine which initiative fits which problem, taking into consideration needs and goals but also constraints and limitations within a country or state (such as resources, capabilities and budget).

Policymakers should explore a variety of options (such as those presented in this article), either as standalone initiatives or as part of a wider programme and assess their suitability to the identified situation. Possible initiatives should be well-defined, with consideration of different options for their implementation. For example, assessment of the suitability of an initiative might involve considering:

- Funding mechanisms such as a grant or loan or a public-private partnership. Whether training materials are free or paid for might also need to be considered.
- An owner and/or champion of the initiatives from the entity/department perspective.
- Partners, such as educational institutions, private entities or other government agencies.
- Economic requirements for the realisation and continuation of initiatives, such as job creation.
- Expected duration of the initiatives.
- Expected goals and outcomes, including the overall impact and how that would be measured.

Having done this, the set of initiatives should be prioritised using a framework that grades them according to feasibility, impact and likelihood of success/ease of implementation. It is important to utilise factors such as available budget, existing demand, availability of potential partners and level of public support for this.

Stage 3 – Develop a roadmap

Once one or more initiatives have been identified, the next step is to plan the implementation using a roadmap. Such a tool allows for the identification of what needs to be achieved, by whom, and how. This in turn enables the allocation and prioritisation of tasks – especially where parallel initiatives are being deployed.

When developing a roadmap, it is essential to:

- Define a vision for the expected outcome of one or more initiatives and use that to set clear and achievable goals.
- Identify the key initiatives and activities required to achieve those goals.
- Establish a logical sequence for the tasks, taking into consideration the availability of stakeholders and resources as well as the dependency between tasks.
- Clearly assign responsibilities and allocate resources, including budget, personnel, technology and time.
- Establish tracking and evaluation indicators that can be used to monitor the progress of the initiative(s) and/or success, and, in turn, to identify any sticking points that should be revised.

The developed roadmap will serve as a centralised plan for reference between necessary stakeholders throughout the implementation of the initiative(s) and, if done properly, beyond that.

About Axon Consulting

Axon is an international firm founded in 2006 that provides investment and advisory services to a broad client base in the ICT and digital space in more than 70 countries across the world.

Axon's cybersecurity practice is central to its business and an increasingly important service area for clients. Its work in this field includes strategy, policy/regulation, and research at the business and governmental level. Axon works closely with national representatives to help them understand their cybersecurity needs and to define actionable recommendations aimed at improving their cybersecurity ecosystems.

Tel: +34 913 102 894
Email: marketing@axonpartnersgroup.com

Madrid (HQ)
Calle Sagasta 18,
3rd Floor,
28004, Madrid

Brussels
91, Avenue du Roi,
1190, Brussels

Istanbul
Buyukdere Cad.
No. 255 Nurol Plaza,
B0434450 Maslak,
Istanbul

Bogota
Calle 100 #13-95,
Torre Empresarial FD,
100 Piso 6,
Bogota

Riyadh
3141 Anas ibn,
Malik Road,
Building B, 2nd Floor,
Al Malqa, Riyadh

AxonPG

axon-partners-group