OliverWyman Forum

Oliver Wyman Forum Global Cyber Risk Literacy and Education Index

Paul Mee, Rico Brandenburg, Wenhan Lin

A measurement of population development toward understanding cyber risk

April 2021 – Final release

Table of Contents

1. Foreword

The intent of the Oliver Wyman Forum Cyber Initiative is to keep an increasingly digitized and interconnected world safe from rapidly evolving cyber risks. No year in recent memory is as appropriate for this purpose as 2020. Cybersecurity and the management of cyber risk by individuals, already a major issue before the COVID-19 pandemic, has become much more pressing overnight as enterprises around the world experiment with work from home arrangements.

It is clear that having a more cyber risk aware population will become increasingly important as individuals, corporations, and governments feel the consequences of growing cyber risks. As early as 2014, analysis from IBM found that 95 percent of cybersecurity incidents could be traced back to "human error"[1] as a contributing factor, whether through accidentally clicking on a malicious link, poor patch management, or weak passwords. If true, a better understanding of cyber related risks by individuals should directly reduce the frequency of cybersecurity events. This Index aims to assess population-wide cyber risk literacy and the government commitment and societal infrastructure that help to improve individual cyber risk knowledge as a basis for comparison between geographies. Additionally, the Index serves to illuminate comparisons of policy and planning to drive investment priorities in cyber risk education.

The fast-paced societal progress in digitization around the globe also needs to account for the weakest links in the system; nations must not forget their most vulnerable populations. Much of the world's elderly or less digitally privileged are being thrust into a world that suddenly requires digital and online transactions, from payments and online banking to even the basics of buying tickets for public transportation. Digital progress and the relevant cyber safety awareness and education programs should encompass these underserved populations and teach them to safely use digital methods. However, it remains critical to continue providing and supporting non-digital traditional methods, such as accepting cash payments, where necessary.

The inaugural Oliver Wyman Cyber Risk Literacy and Education Index assesses fifty major geographies, including the European Union, on the development of cyber risk literacy of their populations. Rather than a single test of knowledge, the Index aims to capture the story behind the level of knowledge a population has developed and how nations can improve that knowledge through education and training. The analysis and data underlying the Index can also serve to reveal global best-practices that geographies can compare and potentially adapt to their unique needs.

Our focus on cyber risk literacy and education serves to complement other existing indexes that focus on national defense and government readiness or exposure to cybersecurity attacks. Our Index draws on both existing data sources as well as in-depth analysis, using independently developed frameworks, of both government cybersecurity policies and national education curricula (or a relevant proxy based on curricula used in geographies where no nationally mandated curricula exists).

We developed the Index methodology and the 2020 rankings through an academically rigorous process involving input from a Steering Committee of Oliver Wyman Forum experts, with expertise ranging from public policy to education to cybersecurity, and independent validation by an Index Governance Committee (referred to in this report either as the 'governance group' or 'the IGC') of both external experts and Oliver Wyman Forum experts. Through interviews, over twenty additional external experts were consulted for ideas and hypothesis generated for this Index and the accompanying summary and methodology paper. This summary and methodology paper present our rankings with a comprehensive breakdown of data sources, logical reasonings, weaknesses assessments, findings discussions, and ideas for future development.

After considering external comments and responses from the working draft release in October 2020, we are releasing this final publication summarizing the learnings and outcomes of our inaugural index. During the formal 30-day commenting period between late October and November 2020, we heard and discussed many thoughts and questions from stakeholders. Many government and higher education entities we spoke with were keen to understand how they can customize the research for their purposes and the Index's future development. We continue to invite policymakers, experts, and the general public to provide us with feedback and suggestions for future improvements, and welcome exploration with organizations interested in working with us on advancing the Index research or related outputs.

Paul Mee

Cyber Risk Lead, Oliver Wyman Forum

Rico Brandenburg

Cyber Risk Co-Lead, Oliver Wyman Forum

[1] (IBM 2014)

2. Executive summary

Over the past decade, governments around the globe have begun taking a more active role in geographic cybersecurity, releasing national strategies, dedicating resources to cyber defense, and exploring methods to equip companies with stronger protections. The worldwide information security market is predicted to reach US$170 billion by 2022.[2]

Yet governments often overlook one major issue: How can they cultivate a population that is conscious of cyber risks and continue to seek to understand how to practice safe digital habits? In the United States, 64 percent of Americans have never checked to see if they were impacted by a data breach, and 56 percent would not know what steps to take if they knew their data had been compromised.[3] While many governments pay lip service to the need for a cyber-educated workforce or students who use the Internet safely, few truly understand the magnitude of the challenge or comprehend the foundational overhaul of education and business practice that's required.

Among cybersecurity and other relevant experts, there are two competing approaches to address the challenge in cyber risk literacy. One school of thought argues that technology should be made smarter and more secure, incorporating principles such as security-by-design/default, which proposes incorporating security mechanisms in the foundation of digital products as opposed to adding an element on to a finished product. This in theory can make users safer without requiring widespread education efforts or behavior change, but it is far from foolproof. Conversely, other experts emphasize the importance of educating individuals and equipping them with a basic set of cybersecurity skills to minimize the human contribution to cyber risk events, regardless of advancements in technology security.

Many of the geographies included in this inaugural Oliver Wyman Forum Cyber Risk Literacy and Education Index are embracing both solutions in their cybersecurity strategies. For example, the United Kingdom has set ambitious goals mandating security-by-design in consumer devices but also emphasizes the importance of population cyber risk literacy and education in schools. While the Index accounts for the extent to which national cybersecurity plans encourage security-by-design principles for businesses and manufacturers, this measurement is modest and largely serves the Index's primary aim of measuring each geography's level of cyber risk literacy.

Like financial literacy or health literacy, cyber risk literacy is fundamental knowledge that all individuals should understand. As the world digitizes, governments and businesses increasingly rely on individuals to protect themselves and others in cyberspace, but often fail to provide or disseminate the necessary tools and training. Geographies understand the challenges but do not have a clear sense of what their populations know or where there may be gaps.

The Oliver Wyman Forum's Cyber Risk Literacy and Education Index provides a comprehensive framework for measuring literacy at the population-wide level to enable geographies to discover best global practices and focus their attention on areas of need. Our approach builds on top of existing digital frameworks such as UNESCO's A Global Framework of Reference on Digital Literacy Skills[4] and DQ Institute's Global Standards Report 2019: Common Framework for Digital Literacy, Skills and Readiness.[5] The Index measures not only current populations' ability to understand cyber risk but also whether current structures in governments, education systems, and employers have the tools and incentives to train future generations with essential cyber risk knowledge and skills in an inclusive manner.

The first edition of the Index ranks 50 geographies, including the European Union as a population-weighted aggregate of our ranked EU geographies. The Index, developed through consultations with policy, industry, and academic experts, leverages 42 aggregated indicators[6] across 32 objectives that contribute to scoring 9 "pillars" of cyber risk literacy and education. They in turn fall under five key drivers of cyber risk literacy and education:

1. **Public motivation** — measures the population's commitment to practicing cybersecurity, including metrics such as the rate of adherence to specific safe cyber practices;
2. **Government policy** — evaluates government policies to improve cyber risk literacy and education, including evaluation of metrics that assess the geography's national cybersecurity strategy;
3. **Educational system** — measures the extent to which cyber risk instruction is encouraged or mandated, includes metrics that assess primary and secondary school curricula;
4. **Labor market** – measures the degree to which employers drive demand for cyber literacy skills, including metrics such as the uptake of cybersecurity-related roles and the number of cybersecurity startups; and
5. **Population inclusivity** – measures degree of equal access to digital technologies and formal education in a geography, including metrics such as Internet access and school completion rates.

[2] (Varonis 2020)
[3] (Sowers 2020)
[4] (UNESCO 2018)
[5] (Institute 2019)
[6] Some indicators break down further, resulting in 52 unique indicators when certain indicators are disaggregated

The geographies with the highest rate of cyber risk literacy and education, in descending order, are Switzerland, Singapore, the UK, Australia, and the Netherlands. These geographies scored well across all or nearly all drivers, distinguishing themselves through the integration of cyber risk into their educational systems, labor markets, and government policies. All support robust education from primary to tertiary levels that emphasize quantitative skills and recommend or mandate some level of cybersecurity instruction. Employers in these geographies recognize the significance of cyber risk and demand cybersecurity-skilled workers. Their government policies in cyber risk literacy are expansive and specific, and frequently transparent about funding and the metrics to assess progress and success.

Geographies that are ranked lower overall generally lacked a thorough national level cyber risk literacy strategy and/or emphasis on cyber risk in school curricula. Still, many of these populations often ranked mid-level on "cyber risk awareness and motivation" or their "cultural proclivity towards security risk reduction." This indicates that while some governments may not be prioritizing cybersecurity at this moment, many within their population are beginning to understand the need to take responsibility for improving personal cyber hygiene.

Key findings in the inaugural Index (for details see Section 3)

- Due to a lack of societal structural support and focus on cyber risk literacy, many individuals are inconsistent when it comes to cyber safety practices and prioritize convenience instead.
- While governments set appropriate priorities and goals in cyber risk literacy, they consistently fail to commit the resources necessary for their success.
- Cyber risk education begins too late and lacks standardization, common assessment goals, and reinforcement.
- Globally, employers demonstrate greater commitment to teaching cyber risk literacy than governments, but they remain challenged by their own knowledge lag in the topic.
- Geographies largely do not prioritize or assess the cyber risk education needs of vulnerable or underserved populations, such as seniors or non-native language speakers.

3. Details of Index findings

Due to a lack of societal structural support and focus on cyber risk literacy, many individuals are inconsistent when it comes to cyber safety practices, and prioritize convenience instead.

Within most of the geographies surveyed, there were strong disparities in behavioral change regarding online safety practices. Relatively simple actions, such as avoiding opening emails from unknown addresses, were practiced with far higher regularity than more-active cyber safety practices, such as changing passwords regularly. This reinforces the common perception of cybersecurity as a "tax" on individuals, as opposed to a standard and accepted practice. Even individuals who are aware of the risks can fail to act safely if it is seen as too inconvenient.

To improve, geographies need to ensure that their citizens are both aware of appropriate cyber safety practices and incentivized to apply them. Some experts interviewed stated that media exaggerations of the risks associated with cybercrime or unsafe online practices can be counterproductive, causing individuals to disengage due to a sense of futility or desensitization. Appropriate communication of the risks involved and wide access to educational materials is critical. Geographies should also commit resources to assessing and tracking behavior change in order to understand the scope of the problem and the efficacy of various solutions.

European geographies displayed some of the largest disparities in individual cybersecurity behaviors, indicating that even geographies that prioritize cyber risk literacy are struggling to change individual behavior. There is also a time delay to consider: Many geographies have only recently incorporated cybersecurity into their curricula, and companies have only recently begun to prioritize safe cyber practices. These statistics could improve significantly in the coming years as a greater number of Internet users will receive formal training.

While governments set appropriate priorities and goals in cyber risk literacy, they consistently fail to commit the resources necessary for their success.

All of the geographies ranked in the Index have issued a cybersecurity strategy outlining a vision and strategic priorities. Most address the key aspects of cyber risk literacy – such as education, investment in innovation, and collaboration between the public and private sector – but lack concrete steps, such as an implementation timeline, a sufficient budget, and accountability to the public. Nearly all of the surveyed strategies support the need for a public awareness campaign on cybersecurity, but few include actionable steps or, more critically, metrics to assess reach or behavior change. In many plans, a detailed focus on growing research and development (R&D) or commercial innovation is undercut by a lack of clear and actionable steps to improve and deepen cybersecurity education at the primary, secondary and tertiary level.

Geographies can improve their government policy and long-term vision by pairing their strategy with implementation programs, assigning oversight and responsibility, and regularly assessing progress against their goals. Geographies should be encouraged to be transparent about funding commitments for cyber risk literacy following the Australian model, instead of asking government departments to fund literacy efforts out of existing budgets, which can reduce visibility on funding allocation for the public. Switzerland and Estonia offer two best-in-class examples of detailed, metric-focused cyber risk literacy policies. Switzerland has published an implementation plan as a supplement to its strategic plan that includes project objectives and target milestones. Estonia includes quantitative metrics for tracking progress against its goals. The UK also excels in accountability and released an update on progress against cybersecurity goals at the half-way point of the strategy (in 2019).

Cyber risk education begins too late and lacks standardization, common assessment goals, and reinforcement.

The majority of surveyed geographies included cybersecurity instruction in some form and at some stage of primary or secondary education – but the depth and breadth of this instruction varied, often even within geographies. Many geographies introduce cyber education in lower secondary school or the final years of primary school, but research indicates most children are using the Internet by the age of four.[7] Curricula are generally updated every 10 to 15 years, which lags today's rapid changes in technology and cybersecurity.

To improve, geographies should commit to reevaluating the relevance of their IT and cyber risk instruction more frequently to keep up with technological advancements, and introducing this content earlier in a student's career when they are already being exposed to cyber technologies. Experts we interviewed emphasized the importance of reiterating cybersecurity instruction across disciplines instead of delivering it in a single course or for limited grade levels. Students are using information and communications technology in nearly every class subject, so guidance on how to use it safely should be incorporated throughout the curriculum. Cybersecurity instruction should be compulsory, not

[7] (Australian Government eSafety Commissioner 2018)

relegated to an optional course. It should cover a variety of foundational concepts, from safe password practices to behavior on social media, and from dealing with cyberbullying to understanding the concept of a "digital footprint."

Singapore's dedicated cyber wellness course, which spans multiple school years, offers a best-in-class example of cyber risk education that spans social and practical safety topics. Other strong geographies incorporate cyber risk in their digital skills instruction. Israel's state curriculum, for example, includes safe online practices and privacy protection skills as part of a student's digital literacy targets. Several geographies articulate strong cyber risk literacy curricula, but implementation may vary at the state or regional level or be difficult to assess.

Globally, employers demonstrate greater commitment to teaching cyber risk literacy than governments, but they remain challenged by their own knowledge lag in the topic.

Increasingly, employers are taking concrete steps to introduce basic cybersecurity training and phishing exercises to their employees, but cybersecurity generally is still seen as the responsibility of the Information Security team. The 2019 Marsh Microsoft Global Cyber Risk Perception Survey found that 88 percent of firms identified IT or Information Security as the main owner of cyber risk management.[8] Different sectors are engaging with cyber risk literacy at different rates; for example, the financial sector is often hailed as a trailblazer in cybersecurity and praised for its ability to quantify costs. However, all industries are still lagging in literacy. Some experts see employers as the potential vector of greatest impact, given appropriate incentives, because of their reach across the population. Changes in the business sector can be also be enacted on a shorter timeline than curricula overhauls.

Experts recommend modeling and reinforcing thorough cyber risk literacy in corporations across all industries. Governments and other organizations should provide specific support programs for SMEs, which frequently lack the scale to adequately address cyber risk literacy. Canada has introduced a voluntary certification program whereby Small and mid-size enterprises (SMEs) can implement specific cybersecurity risk controls accredited by a certification body. Experts also emphasize the need for basic toolkits that describe the steps companies need to take to be cyber secure. Israel has issued the "Cyber Defense Methodology for an Organization," which articulates a process for companies to identify their level of cyber risk and develop a proportionate work plan.[9] National governments, businesses, and cyber organizations globally should develop similar toolkits around cyber risk literacy, including strong metrics to assess a business's current and future state.

Geographies largely do not prioritize or assess the cyber risk education needs of vulnerable or underserved populations, such as seniors or non-native language speakers.

As most geographies are struggling to deliver or prioritize cyber risk education in general, it is not surprising that there are few efforts targeted at traditionally underserved populations. This is a serious gap as these populations tend to be the most vulnerable to cyber harms. According to a report from the Aspen Institute, Internet users over the age of 60 in the US lost $650 million in online crime scams in 2018, and Internet crime toward older users has increased fourfold since 2014.[10]

Geographies should expand educational opportunities aimed at specific populations that consider their unique characteristics. For example, in the US, public libraries and community centers would be strong access points for seniors. Materials should be available in multiple languages, and additional public awareness campaigns can address the specific challenges of certain populations. Although no geography exhibited an exemplary program for an underserved population, several did acknowledge serving vulnerable populations as a goal and some, like Australia, have produced specific and localized content relevant to minorities or other traditionally vulnerable populations.

The field of cyber risk literacy lacks reliable, standardized metrics and data collection, which is inhibiting the growth and prioritization of the topic among governments, employers and the general public. Assessing a population's digital behaviors, or variances in educational and government policy across a geography, is a difficult task. There is currently a lack of strong research and reliable data in cyber risk literacy. Government departments that do prioritize cyber education, such as the Office of the eSafety Commissioner in Australia, often find that assessing the impact of public awareness campaigns, cybersecurity webinars, and other educational content is a significant obstacle to understanding outcomes.

This Cyber Risk Literacy and Education Index offers governments a unique tool to identify best practices and strategies for improving cyber literacy. However, it will ultimately be up to governments to take the lead and skillfully deploy policy and resources toward creating the environment required to upskill their populations.

[8] (Marsh Microsoft 2019)
[9] (National Cyber Security Authority of Israel 2017)
[10] (Fahs, et al. 2019)

4. Who should use the Index?

We envision at least five types of users who would find practical use from this index:

- **Policy makers**
  Cyber risk literacy will remain a significant global challenge and policy makers will need to do more to ensure that their population is protected. Even for geographies that are addressing their digital divide and education disparity, governments will need to address cyber risk literacy to ensure that citizens know how to keep themselves safe in cyberspace for their personal, employer, and national interests.
- **Educators**
  Educators, particularly those who have the authority to influence national curricula, can use our data to consider how to improve their focus on cybersecurity education.
- **Private enterprises**
  Private enterprises (e.g., tutoring companies, banks) can utilize our work to assess cyber risk literacy when considering geographies for investment, or to help build businesses or vocational training that fill systematic needs in geographies where we have identified room for improvement in cyber risk literacy.
- **Academics**
  Cybersecurity is a nascent field and there is a lot of room for research. We supplied our assessment of objectives for good population cyber risk literacy and our hypothesis behind those selections. These hypotheses and their respective metrics have been deeply discussed and debated with cybersecurity experts in the field. However, our work and various hypotheses will stand to benefit from further rigorous academic analysis and testing from independent researchers for future improvements.
- **General public**
  Finally, we hope the release of this Index will encourage the global population at large to take a greater active interest in understanding cyber risk issues. Increasingly in the digital era, every individual stand to gain by furthering their knowledge on not just how to use digital tools, but how to use them in a safe manner that protects themselves and their data.

We discussed the Index with a variety of government, industry, and academic stakeholders during the 30-day commenting period of the working draft release (October 2020). Below three common questions we heard.

What can my geography do to improve in the overall Index rankings, its drivers, and pillars?

The Index measures the cyber risk literacy of the general population and as such, sustainable improvements take time. We recommend interested parties view the rankings as a form of guidance towards international best-practices, building on exemplary examples identified in our research. Rather very specific Index-focused actions, geographies looking to improve either one of the five key drivers (see Section 5) or overall rankings, should holistically work on creating more transparent and accountable government plans, while increasing investments to boost population cyber-risk literacy. The Oliver Wyman Forum looks to continue converging relevant stakeholders on ideas.

How did you ensure geographies achieved or followed through on their plans and statements?

The scoring rubric takes into consideration key aspects of each geography's plans and education curriculums. However, it does not directly consider whether the geography in question followed through on their plans. For cybersecurity strategies, the assessment gave additional points if plans covered specific action steps, and directly attributable success metrics upon completion of these steps. The scoring makes an implicit assumption that greater plan transparency, details, and milestones correlate to real-world actions and follow-throughs to achieve stated goals.

How can we submit additional documents that we think you should consider in your scoring?

In order to find a balance between qualitative assessments and planning, as well as quantitative data, we do not consider niche documents/ plans unless it is directly linked to the geography's national cyber strategies, or part of its national strategy website. Additional information is considered if directly part of the national cybersecurity strategies or as official supplement to the strategies. An important recommendation of this research is to encourage transparency among all governments to have a central website to store publications of each geography's cybersecurity plans and education curriculums for easy access. For development of national cybersecurity plans, we recommend that governments include in the main plan or in supplement materials, detailed actions step and accountable metrics.

We continue to encourage relevant stakeholders such as governments or education boards to submit to us documents potentially relevant to future Index releases. The Oliver Wyman Forum will initiate events and roundtables to further discussions on improving global cyber risk literacy. If you or your organization seek to better understand the index, its potential use cases, and collaboration opportunities, please contact us at OWForum@oliverwyman.com.

5. Understanding the drivers

Cyber literacy needs to be improved through a balanced combination of key factors. We refer to these as our "five drivers." In the rest of this section, we explain these drivers and how each can be developed and fortified.

- **Public motivation:** How motivated is the public to take action to protect their cybersecurity? (Section 5.1)
- **Government policy:** How much support has the government provided to improve citizenry understanding of cyber risks? (Section 5.2)
- **Educational system:** Does the geography have an educational focus on improving the population's cyber risk literacy rate? (Section 5.3)
- **Labor market:** Do employers boost demand for cyber risk literacy skills among the population? (Section 5.4)
- **Population inclusivity:** Does the geography's population have equal access for improving their cyber risk literacy skills through the formal educational system or hands on practice with technology? (Section 5.5)

5.1. Public motivation

This driver measures the population's commitment to practicing cybersecurity, including metrics such as the rate of adherence to specific safe Internet practices.

Experts we interviewed believe that to assess and improve cyber risk literacy, measurements should continuously aim to better understand how the general public thinks about and reacts to cyber risks. Populations that do not believe cyber risks to be an issue, or that do not demonstrate they intend to take basic precautions against risks, are less likely to learn more about cybersecurity. As the growth of the Internet of Things intensifies the connectivity of personal devices, the surface area for cyberattacks will expand – heightening the importance of each person's commitment to practicing cybersecurity.

Therefore, it is important for populations to understand the kind of cyber risks that can emerge, such as identify theft, the exposure to key loggers, cyberbullying, social engineering, malware, and information sharing on social media. Experts say that academic research today lacks understanding of how day-to-day users (the most significant general risk group) view cyber threats.

As the public becomes more motivated to learn about cyber risk, experts hypothesize a positive trickle-down effect as more individuals can share their knowledge and defend against public risk. Many experts we spoke with believed that certain geographies put greater emphasis on general education or independent learning, and likewise, certain geographies may be more primed to understanding that cyber-literacy is an important skill.

More qualitative research into how users perceive and are aware of individual cyber risks would benefit the future development of this driver.

5.2. Government policy

This driver evaluates government policies to improve cyber risk literacy and education; this evaluation includes metrics that assess the geography's national cybersecurity strategy.

Experts interviewed contended that governments should provide the foundational policies and investments that encourage cooperation among various stakeholders, and address issues that the market does not. This could include public-private information sharing (e.g., collecting and sharing anonymized data on threat vectors) as well as industry-wide workshops or knowledge hubs (to discuss best-practices or fault lines).

Experts also viewed stable and sustainable government policy as essential for setting direction and following through on long-term investment in cyber literacy. Governments need to design policy that triggers a progressively transformative shift in their population's cyber literacy over the long term, such as through national cyber literacy initiatives or the issuance of national standards for cybersecurity compliance. To move beyond simple lip-service, cyber risk literacy strategies need to feature measurable goals and methods of accountability, and to be supported by enhancing long-term accountability.

Note that this is the only driver in our Index measured by a single pillar. Experts felt strongly that a long-term government vision, with appropriately allocated funding to enact that vision, was distinct from both education and employers, as employers often retrain to correct for deficiencies that could not be addressed in the educational system. Such a vision is critical for creating an environment that fosters increased cyber literacy.

5.3. Educational system

This driver measures the extent to which geographies encourage or mandate cyber risk instruction, including metrics that assess the primary and secondary school curricula.

Experts we interviewed regarded both the formal education system and the vocational system as critical components to expose people to cyber risk literacy and develop their interest in cybersecurity as a potential career path. In particular, measurements at the primary and secondary levels indicate whether cybersecurity literacy reaches widely across the population, rather than being taught only to individuals that may receive training in tertiary education or professional services employment.

As schools incorporate technology into the classroom, the education system itself is required to train teachers in how to help students identify cyber risks and stay safe from threats. In the increasingly digital world, rather than simply a standalone class, cyber risk education should be incorporated in a multitude of courses so its lessons can be reinforced across different subjects.

Vocational training in cyber risk should also address the upskilling required to maintain a competitive workforce. Such training should be promoted at both the government and employer levels.

5.4. Labor market

This driver measures the degree to which employers foster popular demand for cyber risk literacy skills, including metrics such as the uptake of cybersecurity-related roles and the number of cybersecurity startups.

The labor market plays a strong – and often independent – role in helping to encourage education in a particular area (such as the now-ubiquitous requirement to know how to use word processing software) and to correct for lack of focus in the education system or by the government. Additionally, experts we spoke with considered one of the greatest cyber skill shortages today to be a pipeline of professionals who can design reliably safe and ethical technologies.

Government also plays a role in setting the right incentives for driving cyber risk literacy in the workforce and encouraging innovation through international cooperation and regulation. This can achieve a much-needed balance between security-by-design without stifling digital functionality.

Better cyber risk literacy can also be indicated by the growth of systems, processes and technologies designed to harden targets and mitigate against economic and financial harm, often at the enterprise or governmental level. Experts recommended that the Index capture how industry can build safer, more positive and more human-centered digital environments, and encouraged safety and ethical considerations.

Research on how employers react and prioritize investments in cyber risk, as well as their expectations of employee competence would further develop the measurements behind this driver.

5.5. Population inclusivity

This driver measures the degree of access to digital technology and education in a geography, evaluating metrics such as Internet access and school completion rates.

Experts interviewed stressed that digital inclusivity is a major global issue and extends to other diverse areas such as education, healthcare, and the financial system. Inclusivity remains a key concern for both developed geographies as well as rapidly developing geographies. Our Index measures the average person's cyber risk literacy and their access to education, meaning that everyone within a geography must benefit for the overall geography to be assessed highly. Geographies with lower equality in digital or educational access received lower scores on this driver.

We consider inclusivity to cover both formal and informal education that helps not just students but the broader population to be able to learn about safe use of digital technologies. The metrics assessed define inclusivity to extend through key population divides, such as urban-rural, youth-elderly, and male-female.

Finally, although our Index summed the weighted score of this driver towards the total Index score, we will continue to explore in future versions of this index an alternative view of inclusivity as a scaler factor across the other four drivers of the Index.

6. Cyber Risk Literacy and Education Index rankings

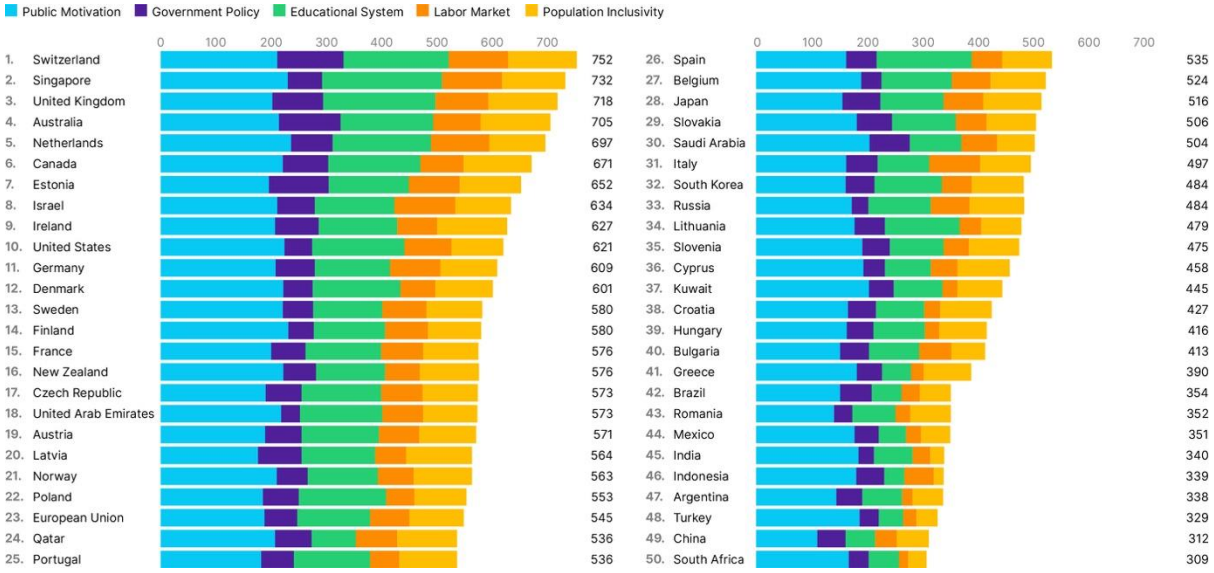
As readers review the rankings, they should keep in mind that this list ranks geographies that are already either considered developed or are economically influential enough for cyber risk literacy to be a topic relevant for their populations. Populations in various other geographies often need to prioritize other considerations before they can focus on, or need to, develop a cyber risk literate population.

Cyber risk education is an evolving topic, one that even major economies may not be fully prepared to undertake if they believe that there are more pressing concerns that warrant attention. A lower score, therefore, does not necessarily mean that a geography's population isn't prepared to understand cyber risks, but rather that other challenges, such as developing infrastructure or investing in basic digital education and rural Internet access, likely take higher priority.

Finally, this Index aims to measure a population-wide average of cyber literacy. This assessment, therefore, naturally leans towards a higher score in smaller developed geographies over more-populous developing geographies. This is particularly true once we factor in population inclusivity, where developed geographies have a natural advantage in technological and educational access. Small communities of highly educated, affluent, or digitally savvy individuals in large developing geographies may demonstrate substantially higher levels of cyber risk literacy than their population-wide average.

The figure below shows a summary of the Index rankings and weighted driver scores.

Figure 1: Summary of Index rankings and weighted driver scores (as of October 2020)[11,12]



Ranking summaries are shown in the tables below

- Table 1: Ranking table of geographies by overall score and drivers (as of October 2020)
- Table 2: Ranking table of geographies by overall score, unweighted driver score, and rank (as of October 2020)
- Table 3: Ranking table of geographies by overall score and rankings in each pillar (as of October 2020)

[11] The European Union scores are a weighted average of all ranked EU countries weighted by population, the score and underlying calculations exclude any EU countries not ranked by the Index

[12] Certain scores of sequentially ranked geographies may appear the same as a result of rounding

Table 1: Ranking table of geographies by overall score and drivers (as of October 2020)

Rank	Overall Index	DRIVER 1: Public motivation	DRIVER 2: Government policy	DRIVER 3: Educational system	DRIVER 4: Labor market	DRIVER 5: Population inclusivity
1	Switzerland	Netherlands	Switzerland	Singapore	Israel	Ireland
2	Singapore	Finland	Australia	United Kingdom	Singapore	Australia
3	United Kingdom	Singapore	Estonia	Switzerland	Switzerland	United Kingdom
4	Australia	United States	United Kingdom	Netherlands	Netherlands	Switzerland
5	Netherlands	New Zealand	Canada	Spain	United Kingdom	Canada
6	Canada	Denmark	Latvia	United States	Estonia	Latvia
7	Estonia	Canada	Ireland	Canada	Italy	Singapore
8	Israel	Sweden	Netherlands	Australia	Germany	Estonia
9	Ireland	United Arab Emirates	Saudi Arabia	Denmark	Australia	Qatar
10	United States	Australia	Germany	Poland	United States	New Zealand
11	Germany	Switzerland	Japan	United Arab Emirates	Sweden	Norway
12	Denmark	Israel	Israel	Estonia	Finland	Japan
13	Sweden	Norway	Qatar	Israel	Canada	Portugal
14	Finland	Germany	Austria	Czech Republic	France	Denmark
15	France	Qatar	Poland	Ireland	Qatar	Germany
16	New Zealand	Ireland	Czech Republic	Austria	Czech Republic	Austria
17	Czech Republic	Saudi Arabia	Slovakia	Portugal	United Arab Emirates	Netherlands
18	United Arab Emirates	Kuwait	France	France	Austria	Israel
19	Austria	United Kingdom	Singapore	Germany	Ireland	Sweden
20	Latvia	France	European Union	Lithuania	Japan	Czech Republic
21	Norway	Estonia	New Zealand	Latvia	European Union	France
22	Poland	Cyprus	Portugal	European Union	Belgium	Belgium
23	European Union	Slovenia	Brazil	Finland	Russia	Russia
24	Qatar	Czech Republic	Italy	Belgium	Saudi Arabia	United Arab Emirates
25	Portugal	Belgium	Norway	Norway	Norway	European Union
26	Spain	Austria	Spain	New Zealand	Denmark	Finland
27	Belgium	European Union	Sweden	Sweden	New Zealand	Cyprus
28	Japan	Turkey	Lithuania	South Korea	Bulgaria	Poland

Rank	Overall Index	DRIVER 1: Public motivation	DRIVER 2: Government policy	DRIVER 3: Educational system	DRIVER 4: Labor market	DRIVER 5: Population inclusivity
29	Slovakia	Poland	Denmark	Slovakia	Latvia	United States
30	Saudi Arabia	India	South Korea	Japan	Slovakia	South Korea
31	Italy	Greece	Bulgaria	Russia	Spain	Croatia
32	South Korea	Slovakia	Croatia	Slovenia	South Korea	Italy
33	Russia	Portugal	Indonesia	Italy	Indonesia	Slovenia
34	Lithuania	Indonesia	China	Saudi Arabia	Portugal	Spain
35	Slovenia	Mexico	Slovenia	Hungary	Poland	Slovakia
36	Cyprus	Lithuania	United States	Bulgaria	Cyprus	Hungary
37	Kuwait	Latvia	Hungary	Kuwait	Slovenia	Greece
38	Croatia	Russia	Argentina	Croatia	China	Kuwait
39	Hungary	South Africa	Greece	Cyprus	Lithuania	Romania
40	Bulgaria	Croatia	Finland	Qatar	Brazil	Lithuania
41	Greece	Hungary	Kuwait	Romania	India	Saudi Arabia
42	Brazil	Spain	Mexico	Argentina	Croatia	Bulgaria
43	Romania	Italy	Cyprus	India	Kuwait	China
44	Mexico	South Korea	Belgium	South Africa	Romania	Brazil
45	India	Japan	South Africa	Brazil	Mexico	Argentina
46	Indonesia	Brazil	Turkey	China	Hungary	Mexico
47	Argentina	Bulgaria	United Arab Emirates	Greece	Turkey	Turkey
48	Turkey	Argentina	Romania	Mexico	Greece	South Africa
49	China	Romania	Russia	Turkey	Argentina	India
50	South Africa	China	India	Indonesia	South Africa	Indonesia

Table 2: Ranking table of geographies by overall score, unweighted driver score, and rank (as of October 2020)[13]

Geography	Overall		DRIVER 1: Public motivation		DRIVER 2: Government policy		DRIVER 3: Educational system		DRIVER 4: Labor market		DRIVER 5: Population inclusivity	
	Score	Rank	Score	Rank	Score	Rank	Score	Rank	Score	Rank	Score	Rank
Switzerland	752	1	712	11	933	1	732	3	676	3	790	4
Singapore	732	2	774	3	481	19	837	1	683	2	732	7
United Kingdom	718	3	679	19	714	4	785	2	601	5	802	3
Australia	705	4	722	10	875	2	642	8	540	9	807	2
Netherlands	697	5	797	1	586	8	687	4	666	4	648	17
Canada	671	6	745	7	636	5	646	7	487	13	789	5
Estonia	652	7	660	21	845	3	559	12	579	6	709	8
Israel	634	8	710	12	532	12	554	13	692	1	645	18
Ireland	627	9	697	16	614	7	546	15	454	19	814	1
United States	621	10	755	4	389	36	646	6	531	10	604	29
Germany	609	11	700	14	555	10	524	19	571	8	661	15
Denmark	601	12	748	6	414	29	613	9	396	26	664	14
Sweden	580	13	744	8	426	27	480	27	499	11	644	19
Finland	580	14	779	2	358	40	496	23	492	12	613	26
France	576	15	674	20	485	18	529	18	479	14	641	21
New Zealand	576	16	749	5	461	21	483	26	394	27	682	10
Czech Republic	573	17	641	24	505	16	554	14	469	16	642	20
United Arab Emirates	573	18	735	9	266	47	574	11	462	17	627	24
Austria	571	19	638	26	513	14	541	16	461	18	656	16
Latvia	564	20	594	37	616	6	514	21	354	29	758	6
Norway	563	21	708	13	438	25	488	25	406	25	674	11
Poland	553	22	623	29	505	15	611	10	317	35	604	28
European Union	545	23	631	27	468	20	504	22	445	21	613	25
Qatar	536	24	698	15	516	13	310	40	471	15	688	9

[13] Certain scores of sequentially ranked geographies may appear the same as a result of rounding

Geography	Overall		DRIVER 1: Public motivation		DRIVER 2: Government policy		DRIVER 3: Educational system		DRIVER 4: Labor market		DRIVER 5: Population inclusivity	
	Score	Rank	Score	Rank	Score	Rank	Score	Rank	Score	Rank	Score	Rank
Portugal	536	25	612	33	457	22	534	17	330	34	667	13
Spain	535	26	548	42	430	26	664	5	343	31	576	34
Belgium	524	27	639	25	291	44	491	24	437	22	639	22
Japan	516	28	526	45	541	11	441	30	449	20	669	12
Slovakia	506	29	613	32	499	17	445	29	349	30	572	35
Saudi Arabia	504	30	691	17	570	9	360	34	407	24	436	41
Italy	497	31	548	43	444	24	360	33	579	7	589	32
South Korea	484	32	544	44	410	30	471	28	342	32	599	30
Russia	484	33	582	38	231	49	436	31	437	23	633	23
Lithuania	479	34	599	36	425	28	520	20	244	39	466	40
Slovenia	475	35	645	23	394	35	374	32	287	37	579	33
Cyprus	458	36	653	22	302	43	318	39	303	36	607	27
Kuwait	445	37	687	18	352	41	340	37	170	43	518	38
Croatia	427	38	559	40	402	32	337	38	181	42	596	31
Hungary	416	39	551	41	371	37	357	35	161	46	550	36
Bulgaria	413	40	511	47	402	31	352	36	364	28	389	42
Greece	390	41	613	31	361	39	201	47	144	48	550	37
Brazil	354	42	513	46	447	23	210	45	210	40	359	44
Romania	352	43	474	49	256	48	301	41	170	44	469	39
Mexico	351	44	601	35	343	42	189	48	167	45	338	46
India	340	45	622	30	217	50	269	43	203	41	162	49
Indonesia	339	46	609	34	401	33	140	50	333	33	113	50
Argentina	338	47	488	48	363	38	279	42	117	49	355	45
Turkey	329	48	630	28	272	46	170	49	154	47	245	47
China	312	49	372	50	396	34	209	46	245	38	370	43
South Africa	309	50	567	39	282	45	211	44	105	50	210	48

Table 3: Ranking table of geographies by overall score and rankings in each pillar (as of October 2020)[14]

			DRIVER 1: Public motivation		DRIVER 2: Government policy	DRIVER 3: Educational system		DRIVER 4: Labor market		DRIVER 5: Population inclusivity	
			Pillar 1	Pillar 2	Pillar 3	Pillar 4	Pillar 5	Pillar 6	Pillar 7	Pillar 8	Pillar 9
Rank	Geography	Overall score	Cyber risk awareness and motivation	Cultural proclivity towards security risk reduction	Long-term vision and commitment	Formal education	Labor upskilling	Skill demand from employer expectations	Innovation-driven demand for skills	Technological inclusivity	Educational inclusivity
1	Switzerland	752	37	2	1	7	2	2	4	2	8
2	Singapore	732	2	10	19	2	1	1	5	22	7
3	United Kingdom	718	20	19	4	1	4	12	6	5	6
4	Australia	705	11	13	2	19	3	22	8	20	2
5	Netherlands	697	3	1	8	3	17	4	2	4	35
6	Canada	671	13	6	5	10	7	13	22	9	5
7	Estonia	652	24	23	3	27	6	16	7	15	10
8	Israel	634	10	15	12	12	22	8	1	27	13
9	Ireland	627	8	21	7	30	5	23	14	24	1
10	United States	621	15	3	36	4	21	5	18	14	32
11	Germany	609	36	4	10	25	10	7	10	6	27
12	Denmark	601	4	11	29	8	15	25	26	1	33
1	Sweden	580	9	7	27	13	35	9	23	7	31
14	Finland	580	1	8	40	16	30	3	41	16	25
15	France	576	7	31	18	14	24	17	16	11	21
16	New Zealand	576	5	9	21	32	14	18	44	13	18
17	Czech Republic	573	25	29	16	20	12	11	33	30	15
18	United Arab Emirates	573	6	12	47	18	9	10	35	12	30
19	Austria	571	39	16	14	22	13	15	27	23	16
20	Latvia	564	29	39	6	24	16	29	25	31	3
21	Norway	563	32	5	25	17	32	27	17	3	28
22	Poland	553	26	35	15	6	19	34	20	40	12
23	European Union	545	30	27	20	21	23	24	15	19	20

[14] Certain scores of sequentially ranked geographies may appear the same as a result of rounding

			DRIVER 1: Public motivation		DRIVER 2: Government policy	DRIVER 3: Educational system		DRIVER 4: Labor market		DRIVER 5: Population inclusivity	
			Pillar 1	Pillar 2	Pillar 3	Pillar 4	Pillar 5	Pillar 6	Pillar 7	Pillar 8	Pillar 9
Rank	Geography	Overall score	Cyber risk awareness and motivation	Cultural proclivity towards security risk reduction	Long-term vision and commitment	Formal education	Labor upskilling	Skill demand from employer expectations	Innovation-driven demand for skills	Technological inclusivity	Educational inclusivity
24	Qatar	536	16	14	13	47	26	6	37	36	4
25	Portugal	536	34	33	22	11	29	32	24	25	11
26	Spain	535	41	43	26	5	8	40	9	21	34
27	Belgium	524	23	32	44	9	38	19	31	10	26
28	Japan	516	48	37	11	23	34	28	12	18	14
29	Slovakia	506	22	38	17	33	20	31	21	32	23
30	Saudi Arabia	504	17	17	9	46	18	14	46	34	43
31	Italy	497	38	46	24	37	31	21	3	38	17
32	South Korea	484	49	20	30	15	36	30	30	8	38
33	Russia	484	45	26	49	31	25	20	29	37	9
34	Lithuania	479	43	24	28	26	11	37	36	33	41
35	Slovenia	475	27	25	35	29	37	38	19	29	24
36	Cyprus	458	19	30	43	45	28	33	28	17	29
37	Kuwait	445	14	22	41	38	33	39	50	42	22
38	Croatia	427	40	40	32	42	27	43	40	35	19
39	Hungary	416	42	41	37	28	43	47	39	28	36
40	Bulgaria	413	46	45	31	34	39	35	13	41	45
41	Greece	390	18	42	39	41	48	44	45	26	37
42	Brazil	354	35	49	23	43	46	50	11	46	40
43	Romania	352	47	48	48	39	40	41	48	39	39
44	Mexico	351	12	47	42	50	41	46	38	47	42
45	India	340	28	34	50	35	47	42	34	50	47
46	Indonesia	339	44	18	33	44	50	26	47	49	49
47	Argentina	338	31	50	38	40	44	45	49	43	48
48	Turkey	329	21	36	46	49	45	48	32	45	50
49	China	312	50	28	34	36	49	36	43	44	44
50	South Africa	309	33	44	45	48	42	49	42	48	46

7. Conclusion

As more of the world's peoples become global digital citizens, geographies are increasingly realizing the need for the cybersecurity literacy and education of their populations. The Oliver Wyman Forum anticipates significant movement in rankings over the coming years. Our Index will need to evolve to enhance its ability to accurately assess the rapidly changing cyber risk literacy levels of geographies, to account for the varying structures of different geographies with different needs, and to have more direct measurements where possible.

As new data sources become available, we will expand our list of geographies and dive more deeply into jurisdictions within key geographies. Just as governments need to continuously update their cybersecurity plans and incorporate them into their educational curricula, our Index will need to reflect the latest developments in the field of cybersecurity, as well as new ideas on how to provide the structural changes required to advance towards a more cyber risk literate population.

Appendix A. Index methodology

Consider how you might measure a population's understanding of fundamental mathematic principles. You would want to assess mathematical understanding across various forms, from basic arithmetic through to advanced calculus, as well as measure the quality of the educational infrastructure for making mathematics instruction available to the people: This analogy reflects how our Cyber Risk Literacy and Education Index works. It measures key determinants of how well citizens of the world's major economic geographies understand the elements of cybersecurity, their motivation to further their knowledge, and the tools available to them.

Our Index has the following components:

- **Drivers** – Factors that drive changes to a population's average cyber risk literacy today and the potential for future improvement. Our five drivers are public motivation, government policy, educational system, labor market, and population inclusivity. (Please see Figure 2. For an in-depth discussion, see Section 5)
- **Pillars** – Items that track trends or changes in the average cyber literacy level of each geography as generated by each of the five drivers. (For definitions, please see Figure 2)
- **Objectives** – Goals that a geography needs to accomplish to address the needs of each corresponding pillar. (Please see Section A.2 for full list of objectives)
- **Indicators** – One or more datasets that measure or serve as a proxy for a geography's performance on a specific objective. (Please see Section A.2 for full list of indicators and Appendix D for data sources of indicators). In limited cases, indicators may itself comprise of sub-indicators (e.g., different patents). Unless specifically stated, we listed the aggregated number of indicators as in Figure 2 and Section A.2.

These listing of drivers, pillars, and objectives are visualized in Figure 2. Please refer to Appendix B: Detailed discussion of pillars, objectives and indicators for a detailed explanation of why we believe they are crucial for advancing cyber risk literacy.

Figure 2: Drivers and pillars of cyber risk literacy and education

Driver 1. Public motivation	Driver 2. Government policy	Driver 3. Educational system	Driver 4. Labor market	Driver 5. Population inclusivity
Pillar 1 **Cyber risk awareness and motivation** *2 objectives* (across 5 indicators) Have a population that is aware of cyber risks associated with the digital age and motivated to address these concerns Pillar 2 **Cultural proclivity towards security risk reduction** *5 objectives* (across 5 indicators) Demonstrate a culture that may be more inclined towards personal/ societal cyber risk conscious mindset	Pillar 3 **Long-term vision and commitment** *4 objectives* *(*across *4 indicators)* Have an overall government mandate and vision for advancing baseline population cyber risk literacy and education and actively aims to attract and retain a cyber risk conscious workforce	Pillar 4 **Formal education** *5 objectives* *(*across *6 indicators)* Incorporates cyber risk as part of early through higher education curricula to create a workforce pipeline that is aware of cyber risk issues Pillar 5 **Labor upskilling** *3 objectives* *(*across *4 indicators)* Ability and actions to upskill current labor force to strengthen cyber risk consciousness in the geography workforce	Pillar 6 **Skill demand from employer expectations** *3 objectives* *(*across *3 indicators)* Employers believe in hiring for cyber risk skills and the importance of building a cyber risk conscious workforce to meet their future business needs Pillar 7 **Innovation-driven demand for skills** *4 objectives* *(*across *5 indicators)* Cyber risk research and development output establishes a current need towards hiring cyber-risk conscious workers	Pillar 8 **Technological inclusivity** *2 objectives* *(*across *3 indicators)* Equality in digital access, and a high level of existing digital pervasiveness across population Pillar 9 **Educational inclusivity** *4 objectives* *(*across *7 indicators*[15]*)* Availability of programs and resources geared towards vulnerable populations (e.g., elderly) and actively seeks to conduct outreach to encourage such non-traditional communities to learn about foundational cybersecurity issues
Current cyber risk literacy rate	Structural support for building and improving cyber-risk literacy in population		Demand pull to encourage upskilling	Access equality for literacy improvement
Overall population cyber-risk literacy and education development				

[15] Note that one of the four listed objectives was given a 0% weighting and did not have its own indicator due to data unavailability (see Section B.9.2), otherwise 8 aggregated indicators would be used for this pillar

In all, we selected 50 geographies including an aggregated European Union score of the European geographies ranked in our profile.[16] Below is the step-by-step methodology used to produce the scores, with further details discussed in the sections below.

1. Select geographies (Section A.1.1)
2. Conduct research and expert interviews (Section A.1.2)
3. Assess drivers, build pillars, and define objectives (Section A.1.3)
4. Select indicators and data (Section A.1.4)
5. Normalize data (Section A.1.5)
6. Impute data (Section A.1.6)
7. Weight indicators and aggregate scores (Section A.1.7)

A.1. In-depth methodology

We reviewed and based our methodology on a host of similar indices, including the ICT Development Index (IDI), conceptual framework and methodology,[17] as well as the Oliver Wyman Forum's previously released Global Cities AI Readiness Index and Urban Mobility Readiness Index. Additionally, we extensively reviewed the guidance from the Organisation for Economic Cooperation and Development's Handbook of Index Construction, including on constructing a composite indicator, imputation, normalization, weighting, and aggregation.[18]

In this inaugural edition of the Index, we did not conduct multivariate analysis or in-depth sensitivity analysis. However, we compared the ranking outputs based on various combinations of normalization and weighting methodologies to assess an outcome that we think is most intuitive for the reader.

A.1.1. Geography selection

We selected Index constituents at the geography level based on the following criteria: they are economically, politically, culturally, or militarily influential (or part of an influential regional bloc); and they demonstrate a demand for cybersecurity. Because the majority of our ranked geographies are countries, the reader will generally see a reference to "geography," but may see references to "countries," even if by a strict definition, the European Union is union of 27 countries. Future versions of this Index may explore additional jurisdictions of key geographies.

The availability of reliable data and the transparency of national governments in publishing polices and regulations were also contributing factors. Several geographies were initially considered but later dropped due to data constraints, including Pakistan, Iran, Iceland, Luxembourg, Malta, and Liechtenstein.

In future versions, we hope to expand our Index to encompass provinces or other jurisdictions of major geographies to study regional differences in regional cyber risk literacy and education. In the US, for example, there are large differences across its decentralized education system. Exploring different conditions set by our various drivers as they pertain to major cities, provinces, or regional governments would present interesting case studies for future rankings.

Summaries of these 50 geographies, as classified by the World Bank, are summarized in the tables below by income group and region. Note that we separately grouped the European Union into the "High Income" group.

Table 4: Summary of Index geographies as classed by income group (Source: World Bank)

Income group	Number of geographies
High income	40
Upper middle income	9
Lower middle income	1
Total	50

[16] EU countries we considered but dropped due to a lack of data include Luxembourg and Malta
[17] (Global Cybersecurity Index 2018)
[18] (OECD 2008)

Table 5: Summary of Index geographies as classed by region (Source: World Bank)

Region	Number of geographies
East Asia & Pacific	7
South Asia	1
Europe & Central Asia	31
Middle East & North Africa	5
Sub-Saharan Africa	1
North America	2
Latin America & Caribbean	3
Total	50

A.1.2. Research and expert interviews

We conducted secondary research and a review of the academic literature on the definition, importance, and evaluation of cyber risk literacy and education at the national level. We discovered that although there is some strong scholarship, the field is still new, particularly in methods of assessment and comparison across geographies.

To supplement this research, we interviewed top global cybersecurity academics, industry experts, policy makers and think tanks to gain a variety of perspectives on the current state of cyber risk literacy and education, and best practices for geographies to follow. We used the critical insights from these interviews to set our priorities, identify geography objectives, and guide indicator selection.

Finally, we also reviewed the methodologies of prominent indexes to collect best practices and compare aggregation and scoring techniques.

A.1.3. Drivers, pillars, and objectives development

The five drivers (see Section 5) can be thought of as sub-indices that measure specific changes related to public motivation, government policies, educational systems, labor markets, and population inclusivity . Each driver is comprised of one to two pillars that differentiate the measurement. These pillars measure the extent to which our selected geographies have fulfilled designated objectives underneath them, which our experts believe are crucial for developing a cyber-resilient population. These various elements were developed in conjunction with research and expert interviews and tested by our internal team and Steering Committee members. Objectives were sorted and categorized based on a natural order/ progression of achievement by geographies (i.e., more readily achievable objectives are listed first). Under these objectives sits our selection of indicators (see Section A.1.4 below), which measure the extent to which each objective is fulfilled in each geography.

A.1.4. Indicator selection

Indicators aim to measure the stated objective. We aimed to select indicators with data that both covered all or the vast majority of ranked geographies, and that would likely be updated over time. Additionally, indicators needed to reflect independent academic rigor and be relevant to the objective being measured, as judged by our internal advisors.

Generally, each objective corresponds to a single indicator. Data for these indicators was collected by the Oliver Wyman Forum through:

- **Existing statistical data** – This can come in the form of general statistics (e.g., malware encounter rates from Microsoft) or indicators from an already existing index (e.g., Adoption of e-commerce and cybercrime legislation from UNCTAD's Global Cyberlaw Tracker). This data is easily comparable between geographies and is used with some statistical adjustment for normalization where necessary.
- **Independent analysis** – We followed an academic format to develop our Oliver Wyman Forum database assessment frameworks, compiling documents and coding data relevant data into an Excel database. We leveraged existing document databases and layered above them our own research and analysis of additional relevant documentation. We conducted two major assessments of geography policies and documentation,

firstly of national cybersecurity strategies and secondly of national curricula, creating just under 10 indicators to use for various objectives in the Index.

The independent analysis consisted of the following two components:

1) National Cybersecurity Strategies Assessment

Every geography we assessed has released a national cybersecurity strategy detailing the government's vision and priorities. Evaluating and comparing these plans reveals a geography's priorities, areas of investment, and degree of commitment to cybersecurity. Our research was based on existing databases of government cybersecurity plans, including ENISA National Cyber Security Strategies and the UNIDIR Cyber Policy Portal, supplemented with additional research to capture the most up-to-date documentation. We expect that some geographies have plans that are not publicly available. However, our assessment can only capture plans that are publicly available.

These plans ranged from six pages in length to nearly 100 pages. Some plans included detailed implementation steps or measurable goals while others included case studies or budgets. Nearly all were published in English, as they are internationally facing and prioritize multinational cooperation.

Once compiled, we assessed these national strategies for content in three categories related to cyber risk literacy: An education focus from primary to graduate school; research and development (R&D), workforce and industry development; and civilian awareness, with a focus on underserved populations such as seniors. For example, if a geography's national plan included a goal of incorporating cybersecurity as a component of ICT classes in primary school, that would be considered in the education category.

Our method scored national strategies on their breadth of inclusion of specific cyber risk literacy topics, such as security-by-design or private-public partnerships in cybersecurity research. We then conducted an assessment of robustness, evaluating the extent to which national plans listed specific action items and metrics to assess success. We also considered the date of publication and the number of updates the geography's government made to the strategy. These qualitative insights were converted to a numeric scoring framework.

In future iterations of the Index, we will need to reassess any newly available information and re-conduct the scoring exercise as geographies update their plans in the future.

2) Assessment of National (or proxy) Curricula for Cybersecurity Instruction

In order to determine if and how cybersecurity skills were being taught in schools, we collected national curricula for primary and secondary schools from government websites and supplemented the data with further research on relevant education laws. In geographies where national curricula do not exist (e.g., the US), regional or provincial plans were used as proxies (e.g., the state curricula of California and Texas).

National curricula vary distinctly by geography, just as education systems do. Several geographies would not refer to their education standards as a "curriculum," but they still articulate learning goals and targets for each grade level. Curricula typically state high-level learning aims for a course and grade level, and then specify skill targets, which can be defined as what a student should be able to do after taking the course. We assessed plans for both aims and skill targets related to cybersecurity.

As in our assessment of National Cybersecurity Strategies, we assessed National Curricula for the breadth of inclusion of high-level cybersecurity instruction targeting skills in one or more of the following categories: data safety, privacy protection, personal cyber hygiene, managing cyber risks, and identifying inappropriate content on the Internet. Our focus was on general safety practices and guidelines as opposed to technical skills. Additionally, we assessed plans for their robustness, defined as the number of our cyber risk literacy skills targets articulated in each category, and whether cyber risk literacy instruction was integrated into other subjects where students are frequently using ICT. Finally, we also considered the publication date. We converted these qualitative insights into a numerical framework. We conducted separate assessments for primary and secondary school curricula.

Similar to cybersecurity plans mentioned above, this analysis will change with each iteration of the Index as new information becomes available.

A.1.5. Data imputation

Not all indicators have complete datasets across the geographies selected for the Index. We considered a few imputation techniques to estimate missing data values, each with its own strengths and weaknesses. We aim to ensure that imputed data reflect a geography's actual population levels.

Our primary choice was to use a second source of data directly comparable to the primary source. However, this was rarely possible due to small variances in how survey questions were asked or how metrics were compiled, which could lead to large incompatibility between two datasets.

When a second data source was not available, we followed methods similar to ITU's ICT Development Index (IDI). We utilized hot-deck imputation, which uses data from geographies with similar characteristics, such as GDP per capita and geographic location or cultural similarity. For example, where one geography has a missing data point, we evaluated a comparable geography with a similar GDP per capita, regional location or cultural values. We employed consistent automation to always utilize the same geography to estimate the data of another geography. We then utilized expert judgement to assess the appropriateness of the proxy geography data before making any final changes.

A.1.6. Data normalization

The indicators selected for the Index are often based on different units of measurements or scales. Thus, we needed to normalize the indicators such that they become comparable between geographies and allow geographies to understand their progress over time.

A review of the OECD Handbook as well as existing indices revealed two methods that we assessed to be most relevant for our Index: The "distance to frontier" approach and the "standardization" (or z-scores) approach. We evaluate the strengths and weaknesses of these two methodologies below.

Ultimately, we chose to utilize the distance to frontier approach. It is used by several well-known indices including the Legatum Prosperity Index (2019) [19], and the World Economic Forum (WEF) Global Competitiveness Report (2019).[20] Upon discussion with our internal experts, we also believe that the distance to frontier approach is more intuitive for the reader to understand the scoring gap between various geographies.

For a comparison of rankings under various approaches, please see Appendix G: Impact of alternative normalization and weighting methods on rankings .

Distance to frontier approach (selected normalization method)

We utilized this approach to normalize each objective's indicators. This method is also utilized by the Legatum Prosperity Index. This allows a transformation (0=lowest performance to 1=frontier performance) and enables us to compare a geography's position relative to other geographies at the objective level. The aggregate of these objective scores can then be compared at the pillar level, the driver level, and finally across the overall Index.

The distance to frontier approach compares a geography's performance on an indicator with the best logical value on that indicator. The reference geography can be the average geography, the group leader, or an external benchmark.[21] For consistency, rather than set a natural floor or ceiling for indicators, we set the minimum performance of a geography in the given set as the floor, and the performance of the top geography as the ceiling.[22]

In cases above, geographies that perform particularly poorly or well on a certain indicator would be heavily penalized or awarded on the corresponding objective. As is the case with the Legatum Prosperity Index, we assessed that normalized values (between 0 and 1) had relatively consistent standard deviation across indicators.

After normalizing the data, the individual series were rescaled to identical ranges, from 1 to 1000, in order to allow conceptually easier comparisons between pillars.

Rankings in this approach are relative; they change as other geographies improve or decline. The strength of the distance to frontier approach is an intuitive comparison to other geographies in the Index. The major weakness of this approach is that it gives an implicit weighting at the indicator level based on extreme outliers.[23] However, our challenger assessment of the z-score approach showed that geographies shifted by only one or two positions, depending on the approach.

Impact of alternative normalization and weighting methods on rankings , shows sensitivity test results between the normalization and weighting approaches.

[19] (Legatum Institute 2019)
[20] (The Global Competitiveness Report 2019) (p. viii)
[21] (OECD 2008) (p. 86)
[22] Note: Some other indices such as ITU's IDC Index set alternative ideal values for certain indicators such as their usage of "Fixed telephone line subscription per 100 in habitants" which is set by adding two standard deviations to the mean, (Global Cybersecurity Index 2018)
[23] (OECD 2008) (p. 28)

Standardization, or z-scores, approach (challenger model)

We tested an alternative normalization approach that we believed to be relevant and defensible for the Index. The standardization (or z-scores) approach converts indicators to a common scale with a mean of zero and standard deviation of one. We wanted to understand the ranking variances that would occur using the two methods, and whether implicit weights in the distance to frontier method had an outsized impact that would warrant the use of the z-score method instead.

The strength of this approach is that indicators no longer have an implicit weight on a dataset's score. However, as stated in the discussion on distance to frontier, the challenger model did not yield significant differences; geography rankings primarily shifted by one or two places.

The challenges associated with the z-scores approach makes the scores themselves less intuitive and less informative for the reader. Under the z-scoring approach, some countries end up with the same scores, making it harder to differentiate between countries.

However, when compared with the distance to frontier approach, the z-score approach is less impacted by implicit weightings of individual frontier data points within an indicator dataset, and thus likely produces rankings that are more defensible even if the scores are less intuitive. This makes this approach an important challenger model to ensure that our distance to frontier approach did not produce dramatically different outcomes.

Outliers

A very limited number of our indicators had excessive skews or long tails due to reasons outside of the ranked-geography's control. For example, the number of Certified Information Systems Security Professional (CISSP) members skew strongly in favor of the US because the certificate issuing body, the International Information System Security Certification Consortium, known as (ISC)², is a US-based organization. Thus, it stands to reason that the majority of its members will also be US-based, followed by other primarily English-speaking nations, making the indicator less reliable as a measure of the objective of a population's "willingness to uptake cybersecurity education." (see B.5.3).

Some indices use the 5th and 95th percentiles for observed values to exclude outliers. However, given the limited number of geographies (and thus, data points) in our Index, we chose not to utilize this method.

After considering several data adjustments to account for indicator bias, we decided to apply a log-normalized transformation to some indicators demonstrating skew or long-tails. This allows observations to be comparable within a narrower range, reducing the standard deviation of indicators so that values in a particular pillar do not excessively reflect an extreme outlier.

Among the indicators used, only the number of CISSP members and publications / citations in cyber-related topics utilized this transformation. Log-normalizing certain indicators with skew is a common technique utilized by several other indexes, including the World Economic Forum's Global Competitiveness Index and the Legatum Institute Prosperity Index.[24] However, we remind readers that all indicators will continue to have some skewness.

A.1.7. Weighting and aggregation

We chose to use an expert-informed weighting, adjusted for indicator quality. We discussed many other logical approaches, such as equal weighting or customized user weighting.

Weighting of objectives and pillars impacts how the Oliver Wyman Forum reached the final rankings. Pillars have different relative weights in the Index, and objectives have different relative weights within their respective pillars. In general, objectives that used indicators our governance group believed to be more complete and less biased ranked higher. We emphasized greater weights on pillars that had stronger indicators or were more relevant for assessing the overall national cyber risk literacy picture. As we broaden our ability to capture the highest quality indicators that are most relevant to each objective, we may tweak the weightings of objectives in future versions of the Index. As both indicator quality and relevance to objective improves, there will be a natural adjustment of weightings as well (see Figure 3).

With respect to data that utilized opinion-based indicators such as expert surveys, our governance group generally assigned less overall weight as it introduces a greater degree of personal bias over pure statistics.

[24] (Legatum Institute 2019)

We considered whether indicators were relevant for all geographies so that any irrelevant indicators would be excluded for some objectives. With consideration, we decided that all indicators were relevant across all geographies.

Weighting and aggregation are conducted in conjunction with the Oliver Wyman Forum Index Governance Committee. This committee is made up of a global team of internal Oliver Wyman experts on cybersecurity, education, and policy, and external cybersecurity experts. The composition of this committee can be found in our Acknowledgements section at the end of this report.

For a comparison of rankings under various approaches, please see Appendix G: Impact of alternative normalization and weighting methods on rankings

We conducted the following exercise to generate, debate, and majority vote on committee opinions:

1. All Index Governance Committee members conducted their assessment of input to weight at the pillar level (the sum of weights for all pillars equal 100 percent).
2. Committee members then assessed the input of weights for each objective for their importance to their corresponding pillar (the sum of weights of all objectives under each pillar equal 100 percent).
3. The Index model then took into consideration that certain underlying indicators of objectives had overall better characteristics, either better statistical quality (e.g., large sample statistics) or better alignment to objectives, and formulaically assigned greater weighting to objectives that used these indicators (see Figure 3).

   In general, on Figure 3, objectives cannot be considered to have "high indicator analytical quality" if they utilized indicators that either used a supplement source or used a significant number of proxies. Achieving a high, medium, or low "relevance of indicator to objective" is strictly based on the views formulated by our Index's cybersecurity experts.
4. For any objective that had more than one indicator, each indicator was assigned equal weighting. In instances where there are no indicators, that objective is given a weight of 0, and remaining objectives are equally weighted.
5. Scores from the pillars were summed into driver scores, and the driver scores summed into the overall Index score based on their respective weights. Per our expert group, the use of a summation of scores implicitly assumes that drivers work independently of one another; that is, poor government policy can be compensated by a very motivated public.
6. Committee members formalized agreement to the various final weightings that determined the final Index rankings.

Alternative aggregation sensitivity tests conducted

We tested our expert weighting against an equally weighted approach to assess potential differences. While the top spots traded places between the two approaches, geographies that tended to perform strongly generally held higher scores among a broad number of pillars and the underlying objectives both with and without the application of weights. Other geographies, particularly those on the lower end of the scale, were more likely to deviate as a result of expert weightings over equal weightings as their performance relative to the frontier geography varied more widely across the different objectives.

Finally, our governance group suggested an alternative aggregation methodology that entailed multiplying the various driver scores and their respective weights together in order to demonstrate the linkage between all drivers; that is, assuming that successful development of population cyber risk ability must be achieved by success in all drivers. Our analysis found that there was limited movement in the rankings.

Figure 3: Weighting adjustments based on indicator analytical quality and relevance to objective

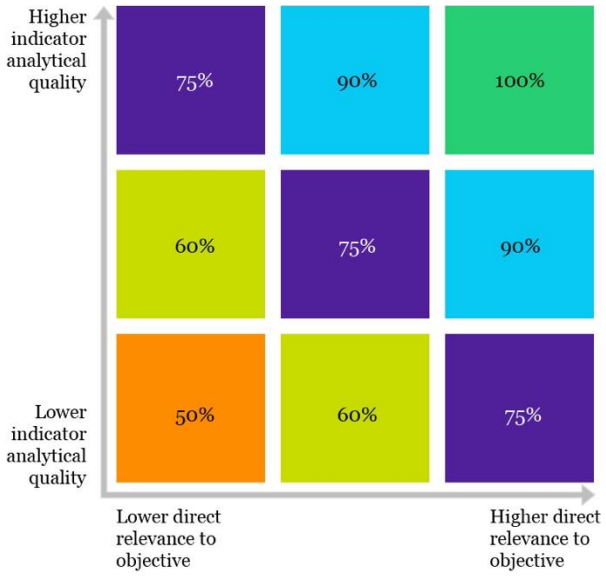


Table 6: Example of indicator reweighting

Pillar A	Original weight in Pillar %	Indicator analytical quality	Indicator relevance	Intermediate adjusted weight	Final adjusted weight
Objective A	50	Lower	Lower	25 = 50 × 50%	25/65 ≈ 38
Objective B	20	Higher	Lower	15 = 20 × 75%	15/65 ≈ 23
Objective C	20	Lower	Higher	15 = 20 × 75%	15/65 ≈ 23
Objective D	10	Higher	Higher	10 = 10 × 100%	10/65 ≈ 15
Total	100			65 = 25 + 15 + 15 + 10	100

A.2. Summary of indicators

To assess good cyber risk literacy among a population, we looked at a variety of indicators to determine scores for a total of 32 objectives (31 of which are measured using one or more indicators). Those scores were sorted and weighted to produce values for the Index's nine pillars, which in turn were sorted and weighted to generate values for the five drivers: Public Motivation, Government Policy, Educational System, Labor Market, and Population Inclusivity.

Note that the indicator names listed in the table below have been simplified for clarity.

Table 7: Pillars, objectives, and indicators of the Cyber Risk Literacy and Education Index

Objective number	Objective	Indicator number	Indicators (*Log-normalized)	Favorable direction	Pillar	Driver
1.1	Population has a basic understanding of cybersecurity risks	1.1.1	Average percentage of machines running Microsoft that encountered malware;	Lower	PILLAR 1 Cyber risk awareness and motivation	DRIVER 1 Public motivation
		1.1.2	Local infections on computers with Kaspersky security software			
1.2	Population understands its role in protecting itself and others from cyber attacks	1.2.1	Percentage of individuals who report avoiding opening emails from unknown addresses;	Higher		
		1.2.2	Percentage of individuals who report changing passwords regularly;			
		1.2.3	Market share of all non-Internet Explorer and 25 percent of non-legacy Edge browsers			
2.1	Population sees security as its own responsibility	2.1.1	Duckduckgo.com search engine market share	Higher	PILLAR 2 Cultural proclivity towards security risk reduction	
2.2	Population values individual privacy and confidentiality	2.2.1	Discloses less personal information online	Higher		

Objective number	Objective	Indicator number	Indicators (*Log-normalized)	Favorable direction	Pillar	Driver
2.3	Population places a priority on the pursuit of education	2.3.1	Average total years of schooling of adult population	Higher		
2.4	Population has trust in and follows government guidance	2.4.1	Percentage of population that has confidence in the national government	Higher		
2.5	Population believes that personal effort contributes to reducing overall security risk	2.5.1	Percentage of population that feel physically safe in their geography	Higher		
3.1	Government institutes long-term sustainable plans and policies that demonstrate cyber risk literacy and education is important for the geography's development	3.1.1	Overall score of National Cybersecurity Strategy (Oliver Wyman Forum database assessment)	Higher	PILLAR 3 Long-term vision and commitment	DRIVER 2 Government policy
3.2	Government has measurable and accountable goals and vision on cyber risk literacy and education	3.2.1	Measurable score of National Cybersecurity Strategy (Oliver Wyman Forum database assessment)	Higher		
3.3	Government implements strong foundation of laws and regulations on cybersecurity	3.3.1	Adoption of e-commerce and cybercrime legislation	Higher		

Objective number	Objective	Indicator number	Indicators (*Log-normalized)	Favorable direction	Pillar	Driver
3.4	Geography attracts and retains new digitally savvy professionals	3.4.1	Net migration for jobs with cybersecurity skills from global LinkedIn profiles	Higher		
4.1	National education systems prioritize quantitative topics	4.1.1	Program for International Student Assessment (PISA) math score;	Higher	PILLAR 4 Formal education	DRIVER 3 Educational system
		4.1.2	Program for International Student Assessment (PISA) science score			
4.2	School systems have the necessary teaching infrastructure and are digitally wired	4.2.1	Use of internet in schools for learning purposes	Higher		
4.3	Cybersecurity is part of the primary school formal curriculum	4.3.1	Primary school education curriculum analysis (Oliver Wyman Forum database assessment)	Higher		
4.4	Cybersecurity is part of the middle/ high school (or equivalent) formal curriculum	4.4.1	Secondary school education curriculum analysis (Oliver Wyman Forum database assessment)	Higher		
4.5	Cybersecurity is a priority for higher education	4.5.1	Coursera Technology Skill ranking	Higher		
5.1	Government conducts, promotes, and incentivizes continued cybersecurity awareness among working population	5.1.1	Workforce score of National Cybersecurity Strategy (Oliver Wyman Forum database assessment)	Higher	PILLAR 5 Labor upskilling	

Objective number	Objective	Indicator number	Indicators (*Log-normalized)	Favorable direction	Pillar	Driver
5.2	Employers conduct, promote, and incentivize continued cybersecurity awareness among employees	5.2.1	Percent growth in computer and network security employment;	Higher		
		5.2.2	Percent growth in computer networking employment			
5.3	Population demonstrates a willingness to pursue cybersecurity education	5.3.1	*Number of (ISC)² members holding the CISSP certification per 100,000 of population	Higher		
6.1	Employers understand that cyber threats pose significant risk to their companies	6.1.1	Relative ranking of "cybersecurity" as a risk in WEF Executive Opinion Survey of Risks Facing Employer	Higher	PILLAR 6 Skill demand from employer expectations	DRIVER 4 Labor market
6.2	Employers demand digitally savvy and security-conscious workers	6.2.1	Extent to which population possesses sufficient digital skills (computer skills, basic coding, digital reading)	Higher		
6.3	Cybersecurity-specialized skill demanding jobs are fulfilled by qualified candidates	6.3.1	Percentage of people moving to a position in computer and network security in the geography	Higher		

Objective number	Objective	Indicator number	Indicators (*Log-normalized)	Favorable direction	Pillar	Driver
7.1	Geography outputs intellectual ideas on new cybersecurity technologies	7.1.1	* PCT Patents per 100,000 of population (in telecommunications, digital communication, computer technology, IT methods for management, and basic communication processes);	Higher	PILLAR 7 Innovation-driven demand for skills	
		7.1.2	* Number of publications/citations per publication (H-Index) in artificial intelligence, computer networks and communications, computer science applications, information systems, and software			
7.2	Geography translates cybersecurity research and development into commercial solutions	7.2.1	Cybersecurity related companies founded inclusively between 2015 - 2019 per 100,000 of population	Higher		
7.3	Geography collaborates between government, industry, and academia on cybersecurity issues and solutions	7.3.1	Private public partnership score of National Cybersecurity Strategy (Oliver Wyman Forum database assessment)	Higher		
7.4	Government pursuing security-by-design through edict	7.4.1	Security by design score of National Cybersecurity Strategy (Oliver Wyman Forum database assessment)	Higher		
8.1	Population has access to necessary computing technologies regularly	8.1.1	Percent of households with computer access;	Higher	PILLAR 8 Technological inclusivity	DRIVER 5 Population inclusivity
		8.1.2	Percent of individuals using the Internet			
8.2	Population has access to high speed (25Mbps+) Internet regularly	8.2.1	Fixed broadband subscriptions per 100 inhabitants	Higher		

Objective number	Objective	Indicator number	Indicators (*Log-normalized)	Favorable direction	Pillar	Driver
9.1	Geography provides equal opportunities for educational access across its population segments	9.1.1	Difference between Urban – Rural lower secondary completion rate	Lower (with floor at 0%[25])	PILLAR 9	Educational inclusivity
		9.1.2	Difference between Urban – Rural upper secondary completion rate			
		9.1.3	Difference between Male – Female primary completion rate			
		9.1.4	Difference between Male – Female lower secondary completion rate			
		9.1.5	Difference between Male – Female upper secondary completion rate			
9.2	Government provides funding for the development of national cyber risk literacy and education campaigns across different demographics[26]	9.2.1	N/A - *Note: Our research indicates that this objective did not have a measurable indicator or data and thus has a weight of 0 percent on this pillar.*	N/A (would be "Higher" if data was available)		
9.3	Government promotes cybersecurity awareness messages, has effective delivery mechanisms, and stimulates interest on the topic	9.3.1	Awareness score of National Cybersecurity Strategy (Oliver Wyman Forum database assessment)	Higher		
9.4	Government conducts, promotes, and incentivizes continued cybersecurity awareness among underserved populations	9.4.1	Underserved score of National Cybersecurity Strategy (Oliver Wyman Forum database assessment)	Higher		

[25] A floor of 0% was set for situations where rural population completion rates were higher than those of urban population, or where female completion rates were higher than those of males, assuming that it means the geography has achieved full equality for that indicator

[26] Unweighted as a result of no reliable data

Appendix B. Detailed discussion of pillars, objectives and indicators

In Section 5, we identified and explained why experts we interviewed believed in the importance of the five drivers: Public motivation, government policy, educational system, labor market, and population inclusivity. These drivers break down into our nine pillars of cyber risk literacy and education discussed in detail in this appendix.

Having rigorously discussed and agreed upon the pillars with our Steering Committee, we identified data variables that can measure a series of objectives experts believe are critical for achieving the stated intentions of these pillars.

Through internal discussions and external expert input and advice, we derived a logical argument and hypothesis for why we believe that each indicator is a relevant measure of its related objective. For readability purposes, we listed the numbered indicator(s) under each objective under a simplified name when warranted. The full name and source of these indicators can be found in Appendix D: Summary of Index indicator data and sources.

The Index is based on the hypothesis that better performance on each objective is positively correlated with better overall cyber risk literacy and education. However, we note that some experts highlighted that second and third-order effects might result in a segment of the population that performs counter-intuitively to our stated hypothesis. In future releases we will continue to test and re-ground these hypotheses, and we also encourage others in the global academic community to independently test our various hypotheses so that we can improve our Index and its measurements.

B.1. Pillar 1: Cyber risk awareness and motivation

Description

Have a population that is aware of cyber risks associated with the digital age and motivated to address these concerns.

Objectives

- **Objective 1.1:** Population has a basic understanding of cybersecurity risks
  - *Hypothesis:* A population should be aware of the various forms of cyber risks (e.g., phishing, malware, fake news, etc.) in order to become adept at defending themselves against these risks.
- **Objective 1.2:** Population understands its role in protecting itself and others from cyber attacks
  - *Hypothesis:* Populations should understand that cyber protection is not just the responsibility of software or hardware developer, but that they have a major role in ensuring that they operate safely.

B.1.1. Objective 1.1: Population has a basic understanding of cybersecurity risks

Indicators to measure objectives

- Indicator 1.1.1: Average percentage of machines running Microsoft that encountered malware
  - *Source:* Microsoft Security Intelligence Report (2020)[27]
- Indicator 1.1.2: Local infections on computers with Kaspersky security software
  - *Source:* Kaspersky Lab (2020)

Reason for indicator selection

"As security defenses evolve and attackers rely on new techniques, Microsoft's unique access to billions of threat signals every day enables us to gather data and insights to inform our response to cyberattacks," -Mary Jo Schrade, Assistant General Counsel, Microsoft Digital Crimes Unit, Microsoft Asia.[28]

[27] Years in parenthesis after source names refer to the year of each source's release
[28] (Microsoft News Center India 2020)

Microsoft Windows is the most widely distributed operating system in the world. The "encounter rate" is the percentage of computers running Microsoft real-time security software that report detecting malware, or report detecting a specific threat or family of threats, during a period.[29] Kaspersky Lab is a multinational cybersecurity and anti-virus provider with a wide distribution of its security product. Both provide a sampling of global malware encounter and infection rates by geography.

Users with low malware encounter rates and low rates of infections should thus correlate with a population that understands how to avoid cyber risks (e.g., not opening unknown files, avoiding opening bad actor websites).

Weaknesses of indicators

Data from both Microsoft and Kaspersky are limited to machines that utilize their respective products. We believe however that this operating system and anti-virus software are deployed widely enough that they can be taken as representative. Users of Kaspersky anti-virus software, which is generally not preinstalled in most existing computer purchases, require conscious selection on the part of the user and therefore may skew toward technologically savvier populations. These "power users" might be naturally less likely to encounter infections.

We considered other direct measures of understanding of cyber risks such as the Open Institutes' Media Literacy Index[30], which ranks European populations against their resilience to fake news. However, the ranking was limited to European geographies, making it difficult to compare with others in our Index. We also considered reflecting encounter or infection rates for mobile devices, used by many as the only source of Internet access, or IoT devices; however, the paucity of available data across all our geographies, as well as counsel from our experts advising that computer-based metrics would reflect similar skills required for population-wide literacy rates adequately, led us to exclude these considerations in this iteration of the Index.

Discussion of findings

Our data generally showed that both Microsoft and Kaspersky data followed similar trends in similar geographies and were generally in agreement with each other. For example, computers in China and Russia tended to encounter more malware than those in other geographies, according to Microsoft, and also had greater local infections, according to Kaspersky. In the case of China, this is likely due to a combination of a large number of machines running outdated versions of Microsoft Windows and the natural consequences of a geography digitizing faster than individuals can adapt to understanding the associated new risks. As a developing nation, digital piracy also remains a challenge in China and can result in novice software pirates installing malware-embedded software.

B.1.2. Objective 1.2: Population understands its role in protecting itself and others from cyber attacks

Indicators to measure objective:

- Indicator 1.2.1: Percentage of individuals who report avoiding opening emails from unknown addresses
  - *Sources:* Eurobarometer 499 public opinion survey (2019) and the CIGI-Ipsos Survey on Internet Security (2019)
- Indicator 1.2.2: Percentage of individuals who report changing passwords regularly
  - *Sources:* Eurobarometer 499 public opinion survey (2019) and the CIGI-Ipsos Survey on Internet Security (2019)
- Indicator 1.2.3: Market share of all non-Internet Explorer and 25 percent of non-legacy Edge browsers
  - *Source*: Statcounter.com (2020)

Reason for indicator selection

We utilized metrics that aimed to measure whether consumers understood what they needed to do to keep themselves safe online. The avoidance of opening emails and changing passwords regularly demonstrates that a population understands two key actions required to keep themselves safe.

The above relies on the joining of two surveys that ask similar questions but have different samples. As a result, the same sampled geography may have two different results. Thus, we added the third indicator of "market share of non-Internet Explorer desktop browsers" that is less prone to survey sampling and self-response pollution. Use

[29] (Rains 2014)
[30] (Lessenski 2019)

of this indicator implicitly assumed that any non-Internet Explorer browser is a more secure choice than all versions of Internet Explorer.

Internet Explorer (IE) continues to be preinstalled in Microsoft Windows, the most widely used operating system for desktop in the world.[31] However, in 2019 Chris Jackson, Microsoft's Principal Program Manager in the Experiences and Devices Group specializing in cybersecurity, explicitly wrote on Microsoft's Windows IT Pro Blog that individuals should not utilize IE as a web browser.[32]

We explicitly excluded mobile and tablet browsers as those browsers tend to utilize current security standards and automatically update without user intervention. We utilized the 2019 market share date in order to exclude the new Chromium-based Edge, automatically deployed by Microsoft starting in 2020.

To exclude users who consciously made the choice to use Legacy Edge browser, itself a generally regarded as a modern and secure browser, as their browser of choice rather than as their default choice with recent Windows installations, we assigned a 75 percent haircut to Edge Legacy's existing market share – thereby assuming that the remaining 25 percent of users are simply using Legacy Edge due to users' lack of acknowledgement of the fact that they could directly download alternative and more secure browsers.

Though Microsoft's Edge Legacy browser can also be considered a more dated browser, it is harder to accurately assess its true market share as users are automatically upgraded to the new Chromium-based Microsoft Edge after June 2020 via Windows update.[33] Thus, users who used Edge Legacy out of convenience will ultimately use the more privacy-driven new Microsoft Edge browser without intentional user intervention. Over time however, all users will likely automatically migrate away from Internet Explorer use, particularly once Microsoft sunsets Internet Explorer and Edge Legacy in 2021[34] in favor of Chromium Edge.

Weaknesses of indicators

Both "avoiding opening emails from unknown addresses" as well as "changes passwords regularly" rely on survey data and may differ from reality with a margin of error. We combined data from two different surveys asking similar questions, but exact wording and sampling between these two surveys showed that for the same geography there may be differences in responses (as discussed in Section C.6). As a result, we gave less weight to this data.

Additionally, although Internet Explorer continues to be installed with Windows 10,[35] Microsoft has made it more difficult to find the Internet Explorer option on newer versions of Windows to drive users toward the Chromium-based Microsoft Edge browser, automatically installed on Windows 10. This could artificially improve the use of more secure browsers without explicit user intention or understanding of the reason to do so. Prior to the new Chromium-based Edge, the legacy browser namesake was not available in Windows 7 or 8.[36]

According to Statcounter.com, Legacy Edge had only around a 5 percent global market share. Thus, it appears likely that users of a particular geography are intentionally choosing alternative browsers to Internet Explorer, rather than simply choosing Microsoft's default recommendation.

For a period of time in the European Union, Microsoft also included a Browser Choice ballot in Windows to give users a choice of browsers. However, this was discontinued in 2014 and experts do not believe it significantly changed choice of browsers.[37] Finally, corporate users may not have a choice in the types of browsers they utilize and may skew a population towards use of Internet Explorer even if users themselves use more secure browsers.[38]

Discussion of findings

Across all geographies, data showed that a low percentage of people change their passwords regularly. In general, only about a fifth to a third of participants in these two surveys said they changed their passwords on a regular basis. This was the case even for geographies that are generally stronger in other elements of cyber risk literacy. For example, fewer than 15 percent of respondents from Latvia, Japan, Spain, and Portugal changed their passwords regularly.

The surveys found that respondents were more likely to not open unknown emails. This is likely because changing passwords require a conscious action by individuals, while ignoring an email reflects a form of inaction. This

[31] Data from NetMarketShare.com show that Windows represents a 87.62% market share globally on desktop/ laptops as of September 2020, followed by Mac OS (9.4%) and Linux (2.4%)
[32] (Windows IT Pro Blog 2019)
[33] (Hoffman 2020)
[34] (Microsoft 365 Blog 2020)
[35] (Microsoft Support 2020)
[36] (Warren 2019)
[37] (Keizer 2014)
[38] (Bott 2015)

demonstrates a well-known feature of individuals' cyber-secure habits: They are inconsistent. Fiserv's 2019 Cybersecurity Awareness Survey[39] categorized 44 percent of Americans as ambivalent toward cybersecurity: Willing to protect themselves when it is easy, but not when it's inconvenient. The data from the Eurobarometer CIGI Ipsos surveys suggests this might be an appropriate characterization for other geographies as well.

Not all geographies, however, demonstrate this pattern. A high percentage of respondents in South Africa stated that they change their password regularly and avoid opening unknown emails. This suggests that while South Africa may have unequal levels of digital literacy and access to technology, thus making cybersecurity a secondary priority for government and education, the digitally literate population may also be reasonably cyber risk literate.

[39] (Fiserv 2019)

B.2. Pillar 2: Cultural proclivity towards security risk reduction[40]

Description

Demonstrate a culture that may be more inclined toward personal/ societal cyber risk-conscious mindset.

Objectives

- **Objective 2.1:** Population sees security as its own responsibility
  - *Hypothesis:* People that see security as their responsibility are more likely to take actions that protect their personal information online.
- **Objective 2.2:** Population values individual privacy and confidentiality
  - *Hypothesis:* Populations that show a greater desire for privacy and confidentiality are more incentivized to ensure that their online and digital information are secure.
- **Objective 2.3:** Population places a priority on the pursuit of education
  - *Hypothesis:* Populations more willing to pursue education are also more likely to understand the defensive actions required to keep themselves safe in the digital world.
- **Objective 2.4:** Population has trust in and follows government guidance
  - *Hypothesis:* As governments are trying to convince its civilians to be more careful when online, societies that are more trusting that their government is acting in their best interest are likely more willing to follow guidelines.
- **Objective 2.5:** Population believes that personal effort contributes to reducing overall security risk
  - *Hypothesis:* Geographies where individuals feel their actions had a positive impact on security risk mitigation are likely to believe that they can take individual action that protects against cyber risks.

B.2.1. Objective 2.1: Population sees security as its own responsibility

Indicator to measure objective

- Indicator 2.1.1: Duckduckgo.com search engine market share
  - *Source:* Statcounter.com (2020)

Reason for indicator selection

While several privacy-centric search engines are available (e.g., Qwant, Startpage), DuckDuckGo.com (DDG) is currently the most-widely used globally. In fact, other privacy search engines generally do not have large enough market shares to register on StatCounter.com and other browser market share tracking websites.

People who utilize services like DDG are not simply stating a preference for personal privacy but are actively taking steps to protect that privacy. As Forbes Magazine has pointed out: "The company [DuckDuckGo] doesn't store a single byte of your history, and its extension prevents you from being tracked elsewhere. Making the switch isn't the only thing you should do to protect your privacy, but it's a significant… first step."

This is also reflected in DuckDuckGo Community Manager Daniel Davis' statement to Forbes: "Our increasing traffic and exposure reflects the increasing public awareness and growing concern that personal data is not being treated properly online, and our fundamental right to privacy is not being properly respected by many companies," Davis says. "Put simply, people have had enough, and are now doing something about it."[41] DuckDuckGo users are not relying on government or company polices to protect their data but are taking action themselves.

Weaknesses of indicator

Generally, all geographies showed some form of limited DDG usage on StatCounter.com. We proxied data for a select few geographies that have low DDG access based on the closest relevant population.

[40] References to "culture" in this report are not intended to suggest innate cultural tendencies, but rather current societal norms and trends that reflect that a population may be primed for cyber-risk building and education
[41] (Evangelho 2018)

The StatCounter data used for this indicator may have bias due to the language preferences of the geographies surveyed.[42] DDG is optimized for English and populations that utilize non-English languages will likely prefer a local engine, lowering usage rates. On the flip side, an argument can be made that if DDG market share in a non-English speaking geography has an equivalent market share to that of an English-speaking geography, the population likely values their privacy more as they are willing to sacrifice a more efficient local search engine in favor of a privacy-focused search engine. We did not adjust the data to give additional points for non-English speaking geographies using DDG.

Discussion of findings

No single geography showed over 1.5 percent market share for DuckDuckGo. The US and English-speaking geographies like Australia, the UK, Canada, and New Zealand (around 0.75 percent to 1.5 percent each) showed comparably heavier usage than others. However, we saw that DuckDuckGo also had comparably high usage in some non-English speaking geographies such as Finland, Austria, Germany, France, and Spain (around 0.5 percent each), which could imply that citizens of these geographies are somewhat more concerned for their personal privacy.

B.2.2. Objective 2.2: Population values individual privacy and confidentiality

Indicator to measure objective

- Indicator 2.2.1: Discloses less personal information online
  - *Sources:* Eurobarometer public opinion survey 499 (2019) and CIGI-Ipsos Survey on Internet Security (2019)

Reason for indicator selection

Disclosing less personal information online demonstrates that an individual is looking to actively limit the amount of personal information that websites have about him or herself.

Weakness of indicator

It relies on survey data between two sources that ask similar questions. Sampling differences between the two surveys may produce different results (as discussed in Section C.6).

Discussion of findings

We found a number of clusters in this data by region and population type. Populations in Western European geographies were less likely to disclose personal information about themselves. For example, nearly 60 percent of those living in the Netherlands answered that they disclose less information about themselves online. The EU has generally been a leader in fighting for the personal privacy rights of its citizens, including first-mover regulations such as the General Data Protection Regulation (GDPR), which covers data protection and privacy rights in the EU and the European Economic Area.

Eastern European geographies such as Romania, Poland, and Hungary were less likely to say that they disclose less information about themselves online. Although these EU nations are subject to laws such as the GDPR, a lack of stringent supporting legal frameworks domestically may be limiting the encouragement of individual privacy and confidentiality concerns amongst the population. Geographies with relatively more diverse international populations or local ethnicities, such as the US, Canada, Australia, UK and China, sat in between these two extremes in personal information sharing.

B.2.3. Objective 2.3: Population places a priority on the pursuit of education

Indicator to measure objective

- Indicator 2.3.1: Average total years of schooling of adult population
  - *Source:* United Nations Development Program (2019)

[42] Refer to https://gs.statcounter.com/faq#methodology for StatCounter's methodology

Reason for indicator selection

In general, populations that consider education more important will likely experience increased number of schooling years through a mixture of parental choice and government mandate.

Weaknesses of indicator

Developed geographies will naturally have governments that mandate higher levels of schooling (e.g., K-12), while developing geographies may mandate lower levels of education. Therefore, a population may have a strong cultural inclination toward education, but a lack of economic development may lower the ability of that population to attain higher levels of education. For example, while the Chinese government mandated nine years of free compulsory education (six years of primary education and three years of secondary education) on July 1, 1986,[43] the government also recognizes and is addressing the fact that the average individual in rural China and urban China does not have the same level of schooling opportunities due to socio-economic disparities. This variance will also reflect regional tendencies toward valuing education; that is, relative to the average urban family in China, a rural family in China may see a lower education threshold as necessary.

Discussion of findings

As expected, the data generally showed that more developed geographies experience more average schooling, with the highest being Germany at 14.1 years followed closely by the US at 13.4 years. An exception to this pattern is European geographies that have historically suffered from lower rates of upper secondary school completion, such as Spain and Italy. In large developing markets, particularly those with large populations such as China and India, education disparities between urban and rural populations resulted in average schooling of only 7.8 years and 6.4 years, respectively, even if schooling across many of their urbans centers are on par with developed nations.

B.2.4. Objective 2.4: Population has trust in and follows government guidance

Indicator to measure objective

- Indicator 2.4.1: Percentage of population that has confidence in the national government
  - *Sources:* Welcome Global Monitor (2019); Edelman Trust Barometer (2020)

Reason for indicator selection

Indicator directly measures civilian trust in their governments. We assume that populations that trust their governments will be more encouraged to follow government guidance (including guidance in areas such as developing cyber literacy). As COVID-19 has shown in 2020, populations with larger distrust of their government were less likely to follow government guidance on health safety issues such as mask wearing. Thus, experts we spoke with felt that lower trust of government in some geographies may make citizens less likely to adhere to government messages around cyber safety.

Weaknesses of indicator

We combined two sources of data asking similar questions and differences in sampling between the two sources may result in differences in the response (as discussed in Section C.6).

Discussion of findings

Data showed that populations in East Asian, Middle Eastern, and Scandinavian geographies tended to have higher trust in their governments. They were followed by Western European and North American geographies, with the notable exceptions of France, Italy and Spain, which have lower trust scores than the rest of Western Europe. South American as well as Eastern European geographies generally responded with lower levels of trust in their government.

[43] (Ministry of Commerce People's Republic of China 1986)

B.2.5. Objective 2.5: Population believes that personal effort contributes to reducing overall security risk

Indicator to measure objective

- Indicator 2.5.1: Percentage of population that feel physically safe in their geography
  - *Source:* Gallup Global Law and Order Report (2019)

Reason for indicator selection

Populations that deemed themselves to live in safer geographies, are assumed to also feel that the can make a positive contribution to maintain the mitigation of security risks (including cybersecurity). That is, a healthy sense of safety would also serve to keep populations "engaged" that their actions are not futile but rather positively contribute towards a safer society.

Weaknesses of indicator

Survey data often faces inherent methodological weakness (as discussed in Section C.6). Additionally, an alternative argument can be made that the indicator may not fully reflect whether individuals feel they have made a personal contribution, or if they simply believe that their governments have done enough to keep the population safe from harm.

Discussion of findings

While during our fact-gathering process, select experts opined that populations that feel physically safe in their geographies may become complacent and lack awareness of cyber risks. However, others argued that populations who feel safer are more aware that they can contribute to their personal security risk mitigation. The trends we study show that there is a correlation between populations that believe they live in a secured geography and better tendencies towards security hygiene. We thus ranked geographies higher if more of their citizenry responded that they felt safer within their geography.

B.3. Pillar 3: Long-term vision and commitment

Description

Have an overall government mandate and vision for advancing baseline population cyber risk literacy and education and actively aims to attract and retain a cyber risk conscious workforce.

Objectives:

- **Objective 3.1:** Government institutes long-term sustainable plans and policies that demonstrate cyber risk literacy and education is important for the geography's development
  - *Hypothesis:* Similar to governments that have invested in building a STEM-literate population, governments that commit to a population cyber risk literacy plan over the long-term – rather than intermittently shifting short-term priorities – will generally succeed in training a more cyber risk literate population.
- **Objective 3.2:** Government has measurable and accountable goals and vision on cyber risk literacy and education
  - *Hypothesis:* Governments that actively work to create a cybersecurity-literate population with clearly measurable and accountable goals are more likely to be incentivized to reach their targets.
- **Objective 3.3:** Government implements strong foundation of laws and regulations on cybersecurity
  - *Hypothesis:* A strong foundation of laws and regulations for cybersecurity will serve to encourage population or employer awareness of cybersecurity issues and the need for cyber risk reduction.
- **Objective 3.4:** Geography attracts and retains new digitally savvy professionals
  - *Hypothesis:* Geographies that can attract digitally savvy professionals will more effectively propagate digital skills among its population. In the long-term, this produces an overall population that is more inclined toward cybersecurity savviness.

B.3.1. Objective 3.1: Government institutes long-term sustainable plans and policies that demonstrate cyber risk literacy and education is important for the geography's development

Indicator to measure objective

- Indicator 3.1.1: Overall score of National Cybersecurity Strategy (Oliver Wyman Forum database assessment)
  - *Source:* Oliver Wyman analysis of national cybersecurity plans (as of September 2020)

Reason for indicator selection

Internal analysis was required as there are no known existing indicators that can measure or proxy the objective. We based our research on existing databases of cybersecurity plans, including ENISA National Cyber Security Strategies and the UNIDIR Cyber Policy Portal, supplemented with additional research to capture the most up-to-date documentation.

Government plans were assessed for the breath of inclusion of three categories related to cyber risk literacy: education focus, from primary to graduate school; R&D, workforce, and industry development; and civilian awareness. The categories were then evaluated for robustness, including whether the plan listed specific action items and metrics to assess success. The inclusion of metrics within these plans enable government accountability for their strategic visions and ensure governments can identify successful and lagging initiatives. Finally, the date of publication and the number of updates the geography's government has made to the strategy were considered. These qualitative insights were converted to a numeric framework.

Weaknesses of indicator

Please see Weaknesses of Oliver Wyman Forum database assessments (Section C.3) for weaknesses that apply to Oliver Wyman Forum database assessments.

Discussion of findings

The national cybersecurity strategies assessed had bold visions and logical, attainable goals in cyber risk literacy and education, but they largely lacked specific programs for implementation, allocated budgets, department responsibility for execution, and metrics to measure success. High-scoring geographies published specific plans with measurable goals that made them accountable and updated their plans every three to five years.

Many geographies with low scores had not updated their cybersecurity strategies in seven to 10 years. Given the fast pace of change in the industry and field, strategies can quickly become out of date if geographies are not regularly refreshing them to meet the new demands of cybersecurity. Other geographies with low scores had plans that lacked specificity or did not touch on cyber risk literacy. Belgium's 15-page cybersecurity strategy contains few specifics and focuses mainly on state defense. Finland's 12-page strategy prioritizes international cooperation and national incident management, and although it acknowledges the importance of the population's cybersecurity competence, it includes few specifics on implementation.

B.3.2. Objective 3.2: Government has measurable and accountable goals and vision on cyber risk literacy and education

Indicator to measure objective

- Indicator 3.2.1: Measurable score of National Cybersecurity Strategy (Oliver Wyman Forum database assessment)
  - *Source:* Oliver Wyman analysis of national cybersecurity plans (as of September 2020)

Reason for indicator selection

Internal analysis was required as there are no known existing indicators that can measure or proxy the objective. We based our research on existing databases of cybersecurity plans, including ENISA National Cyber Security Strategies and the UNIDIR Cyber Policy Portal, supplemented with additional research to capture the most up-to-date documentation.

Government plans were assessed for the breath of inclusion of three categories related to cyber risk literacy: education focus, from primary to graduate school; R&D, workforce, and industry development; and civilian awareness. This indicator captures whether the plan listed specific metrics, qualitative or quantitative, to assess success. The inclusion of metrics within these plans enable government accountability for their strategic visions and ensure governments can identify successful and lagging initiatives.

Weaknesses of indicator

Please see Weaknesses of Oliver Wyman Forum database assessments (Section C.3) for weaknesses that apply to Oliver Wyman Forum database assessments.

Discussion of findings

Fewer than 10 of the assessed geographies included any metrics or targets related to cyber risk literacy and education in their strategic plans. Per our assessment criteria, even when a certain government has a plan that is inclusive of all categories mentioned above, if it lacks an assessment of measurable success then it would score lower on this indicator relative to a geography with a plan that incorporated such measurements.

Switzerland offers an exceptional, best-in-class example for this indicator. In addition to a full strategic plan, Switzerland published a thorough action plan that articulates detailed implementation projects with discrete milestones and timelines. This level of transparency is exceedingly rare in the national cybersecurity strategies we reviewed. Another successful approach is that of Estonia. Its plan articulates quantitative targets for many of its objectives. For example, as part of its research and development plan for the cyber sector, Estonia sets targets for the number of new cybersecurity startups and the export volume of companies in the cybersecurity sector. Other geographies can likely adopt important best practices from these two approaches in order to increase transparency and accountability and demonstrate commitment to cyber risk literacy and education.

B.3.3. Objective 3.3: Government implements strong foundation of laws and regulations on cybersecurity

Indicator to measure objective

- Indicator 3.3.1: Adoption of e-commerce and cybercrime legislation
  - *Sources:* United Nations Conference on Trade and Development (UNCTAD), Global Cyberlaw Tracker (2020)

Reason for indicator selection

The UNCTAD Global Cyberlaw Tracker assigns geographies a point for having legislation in each of the following four areas: privacy laws, cybercrime laws, consumer protection laws, and e-transaction laws. Each of these legislative areas is relevant to cybersecurity, and geographies that have robust regulation have prioritized cybersecurity at the national level.

Weaknesses of indicator

The Tracker does not capture differences related to the quality, comprehensiveness, or effectiveness of the legislation, nor does it include the length of time legislation has been in place.

Discussion of findings

We found that across the world, all geographies have implemented some form of foundational cybersecurity law. Most European, North American, and Asian geographies surveyed have legislation in all four areas, while several geographies in the Middle East, such as Saudi Arabia and the United Arab Emirates, have legislation in only two categories. Some countries such as Russia scored lower on this indicator as it has legislation in only one category: electronic transaction laws. However, Russia does have draft legislation pending in consumer protection and privacy law. We expect that governments will build and improve upon these foundations over the next five to 10 years as they seek out leading practices from other geographies.

Finally, we note one alternative expert viewpoint that a potential second- or third-order effect could result in stronger laws and regulations that ultimately create a moral hazard for individuals. The expert argued that all else being equal, strong laws and regulations that make people objectively safer in cyberspace will decrease the number of cyber risk savvy individuals because when people no longer perceive hazard, they will also relax vigilance. This could be demonstrated during the COVID-19 pandemic when social gatherings increased in many geographies after individuals felt they were less likely to be impacted by the virus.

B.3.4. Objective 3.4: Geography attracts and retains new digitally savvy professionals

Indicator to measure objective

- Indicator 3.4.1: Net migration for jobs with cybersecurity skills from global LinkedIn profiles
  - *Source:* World Bank analysis of LinkedIn data (2019)

Reason for indicator selection

LinkedIn is a widely used professional networking website. According to the World Bank, its data are best at representing skilled labor in the knowledge-intensive and tradable sectors. The World Bank has conducted a rigorous assessment of LinkedIn data through big data analysis to generate real-time insights on developmental trends that can inform policy. It evaluates LinkedIn data covering more than 100 geographies with at least 100,000 LinkedIn members, distributed across 148 industries and 50,000 skill categories.

We selected migration data from profiles self-reporting cybersecurity skills in World Bank's LinkedIn sample. Migration data suggests both where skilled workers are willing to relocate, as well as which geography's immigration policy structure is more likely to welcome and absorb the cybersecurity talent. Geographies that receive net migrations (and therefore are net more attractive for workers) are scored positively, while those experiencing brain drain (and net less attractive) receive negative scores. An unlikely score of 0 means no movement of people within that industry.

Weaknesses of indicator

This indicator relies on LinkedIn data and biases, many of which the World Bank has taken care to reflect in their analyses. Among other weaknesses, the World Bank points out that historical LinkedIn data are less reliable and representative globally because they depend heavily on whether members can recall their work history accurately.[44]

Discussion of findings

Geographies with more open skill-based immigration policies such as Canada in North America, Singapore in Asia, and Qatar in the Middle East, ranked highly. Open mobility policies in the European Union ensured that nations such as digitally-focused Estonia and the economic powerhouse of Germany ranked No. 1 and 2, respectively, on attracting foreign workers. The data showed that India was by far the largest geography that experienced brain drain in cybersecurity talent to other geographies. The US attracted the bulk of cybersecurity workers from India but only ranked No. 31, likely due to a comparatively restrictive immigration policies relative to the number of jobs that could otherwise be filled.

[44] (Zhu, Fritzler and Orlowski 2018)

B.4. Pillar 4: Formal education

Description

Incorporates cyber risk as part of early through higher education curricula to create a workforce pipeline that is aware of cyber risk issues.

Objectives:

- **Objective 4.1:** National education systems prioritize quantitative topics
  - *Hypothesis:* Geographies that have education systems geared toward the teaching of quantitative topics will incline students toward the study of related topics such as computer science, and by extension cyber risk.
- **Objective 4.2:** School systems have the necessary teaching infrastructure and are digitally wired
  - *Hypothesis:* Schools that are more digitally wired would be more likely to teach students about cybersecurity fundamentals. It is less likely that schools without practical digital access could teach students about cyber risk literacy.
- **Objective 4.3:** Cybersecurity is part of the primary school formal curriculum
  - *Hypothesis:* Education systems that prioritize cybersecurity in primary school programs are more likely to develop students proficient in cybersecurity.
- **Objective 4.4:** Cybersecurity is part of the middle/ high school (or equivalent) formal curriculum
  - *Hypothesis:* Education systems that prioritize cybersecurity in middle and high school are more likely to develop students proficient in cybersecurity.
- **Objective 4.5:** Cybersecurity is a priority for higher education
  - *Hypothesis:* Geographies with higher education systems that that ensure students reach a level of proficiency in cybersecurity are more likely to develop a population that is proficient in cybersecurity fundamentals.

B.4.1. Objective 4.1: National education systems prioritize quantitative topics

Indicators to measure objective

- Indicator 4.1.1: Program for International Student Assessment (PISA) math score
- Indicator 4.1.2: Program for International Student Assessment (PISA) science score
  - *Source*: Organisation for Economic Co-operation and Development (OECD), (2018)

Reason for indicator selection

The Program for International Student Assessment is a worldwide study by the Organisation for Economic Co-operation and Development that evaluates educational systems by measuring 15-year-old pupils' scholastic performance on mathematics, science, and reading. Its purpose is to compare education attainment across the world.

Geographies where students score higher on various PISA subjects will likely have prioritized education in those subject areas. For example, proficiency in math and science is highly prioritized by parents in China and thus prioritized by the Chinese educational system. As a result, PISA math and science scores from Chinese students are consistently ranked among the top in the world. Thus by 2019, approximately 5,000 of Britain's 16,000 primary schools had adopted Shanghai's teaching methods.[45] The focus of these schools under the new curriculum showed up in test scores where scores showed that the performance of these British schools in PISA improved after adopting China's teaching methods.[46]

[45] (Scores bolster case for Shanghai math in British schools 2019)
[46] (Turner 2019)

Weaknesses of indicators

In some geographies, PISA scores test only a segment (generally more privileged) of the population. Thus, we also compared GRE math scores (a voluntary graduate admissions test) between geographies and found data to largely reflect PISA scores even in geographies where PISA test takers may not represent economic backgrounds of the broader geography. This comparison is imperfect because even though it draws upon a larger sampling pool, students taking the GRE are likely making larger investments in their graduate level educations than the general public.

Discussion of findings

By a wide margin, China had the highest PISA math and science scores among all geographies. This is in part because only students in a few key cities in China are tested rather than students across the entire geography, creating some inherently upward bias. However, China (along with high-scoring Japan and South Korea) traditionally puts greater emphasis on quantitative education and evaluates students through rigorous and high stakes national college entrance exams (i.e., China's Gaokao). India also scored highly in these quantitative PISA examinations. We saw similar levels of quantitative aptitude when we externally compared GRE and GMAT scores from test takers in China, Japan, South Korea, and India with the scores of students based in Western geographies.

B.4.2. Objective 4.2: School systems have the necessary teaching infrastructure and are digitally wired

Indicator to measure objectives

- Indicator 4.2.1: Use of Internet in schools for learning purposes
  - *Source:* WEF Executive Opinion Survey (2017-2018)

Reason for indicator selection

The survey of experts directly measures the objective. More informed and statistically comparable data covering all geographies was unavailable.

Weaknesses of indicator

While the indicator directly measures our objective, survey data faces inherent methodological weaknesses (as discussed in Section C.6). In this instance, the data is based on expert opinion and subject to the individual biases (e.g., potentially respondents can have an overly positive or overly negative opinion about Internet connectivity in a geography due to personal experiences).

Discussion of findings

Unsurprisingly the opinion survey found that experts largely believed that the developed geographies also had more digitally connected schools, led by Singapore, New Zealand, and Switzerland. We were surprised to find that experts considered some European geographies, such as Germany and France, to be less well connected. The survey indicated that experts believed schools in China and India were equally well connected while Italy's survey response ranked lower than both developing geographies. Better geography-specific data may be required to supplement these expert surveys.

B.4.3. Objective 4.3: Cybersecurity is part of the primary school formal curriculum

Indicator to measure objectives

- Indicator 4.3.1: Primary school education curriculum analysis (Oliver Wyman Forum database assessment)
  - *Source:* Oliver Wyman analysis of national/ relevant regional educational plans (as of September 2020)

Reason for indicator selection

Independent analysis was required as there are no known indicators that can measure or proxy the objective. We collected national curricula for both primary and secondary school from government websites and supplemented the data with further research on relevant education laws. In geographies where national curricula do not exist

(e.g., United States), regional or provincial plans were used as relevant proxies (e.g., the state curricula of California and Texas).

We assessed the breadth of inclusion of high-level, standard cybersecurity instruction aims and the specific cybersecurity skill targets for students in the following categories: data safety, privacy protection, personal cyber hygiene, managing cyber risks, and identifying inappropriate content on the Internet. Our focus was on general safety practices and guidelines as opposed to technical skills. We also assessed plans for their robustness, defined as the number of our defined skill targets articulated in each category, and whether cyber risk literacy instruction was integrated into other subjects where students frequently use ICT. Finally, publication date was also considered. These qualitative insights were converted to a numeric framework.

Weaknesses of indicator

Please see Weaknesses of Oliver Wyman Forum database assessments (Section C.3).

Discussion of findings

Most geographies that have updated their curricula in the past three to five years, which covers just over half of the index universe, include some educational aims in cyber risk literacy and education – but the breadth and depth of these aims vary considerably.

The UK offers an example of strong cyber risk literacy curricula for primary school. The curricula of England, Scotland and Wales were assessed as the UK has no countrywide curricula. The curricula of Scotland and Wales were particularly comprehensive, though they take different approaches to cyber education. The Scotland curriculum incorporates cyber risk literacy education into its technology course, articulating one or two cybersecurity skill targets for each grade level. The Wales curriculum has a comprehensive digital competence framework that cuts horizontally across traditional subjects and is incorporated into subject course learning. This model was reasonably common among geographies with strong cyber risk literacy curricula in primary school.

Israel's curriculum is another example of the horizontal approach, incorporating cyber risk literacy content around safe habits online and privacy protection to students' digital literacy skillsets.

An additional geography that stood out in this category was Poland, which has a strong cybersecurity curriculum in primary school while many other European geographies begin to teach cybersecurity in earnest in lower secondary. Poland also ranks highly in math and science PISA scores, indicating that the geography likely has a strong quantitative educational system.

Curricula that score low in this indicator tend to be limited to general aims around student safety online and lack the specificity of other plans. Plans with higher scores tend to articulate skill targets around strong password creation, knowledge of cookies and digital footprints, as well as a high-level understanding of how encryption works.

B.4.4. Objective 4.4: Cybersecurity is part of the middle/ high school (or equivalent) formal curriculum

Indicator to measure objectives

- Indicator 4.4.1: Secondary school education curriculum analysis (Oliver Wyman Forum database assessment)
  - *Source:* Oliver Wyman analysis of national/ relevant regional educational plans (as of September 2020)

Reason for indicator selection

Same as for the objective above (Section B.4.3).

Weaknesses of indicator

Please see Weaknesses of Oliver Wyman Forum database assessments (Section C.3).

Discussion of findings

A greater percentage of geographies assessed had more robust cyber risk literacy education at the secondary level, particularly in lower secondary school. Singapore is a best-in-class example of thorough cyber risk literacy education, with a dedicated cyber wellness course on engaging safely online that was introduced to the curriculum in 2014. Unlike curricula in many other geographies, Singapore offers multiple computer science courses that

incorporate safety topics. Lithuania's secondary curriculum offers another successful model, incorporating online safety skill targets not only in information technology but across subjects such as moral education, foreign language and literature.

B.4.5. Objective 4.5: Cybersecurity is a priority for higher education

Indicator to measure objectives

- Indicator 4.5.1: Coursera Technology Skill ranking
  - *Source:* Coursera (2020)

Reason for indicator selection

In general, the curricula and competencies of higher education institutes are not under any globally standard requirements from governments. Therefore, measuring the number of accredited cybersecurity programs in institutes of higher education for each geography would result in a dataset that is likely non-standard and non-comparable. We opted therefore to utilize a more standardized measurement to reflect the prioritization of cybersecurity in the higher education space of a given geography: Competency levels for college-level courses delivered through Coursera. Coursera lessons and exams are standardized for all test takers, allowing for cross-geography comparison.

Weaknesses of indicator

Coursera courses are delivered in English, resulting in language barriers for students in geographies where English is not the native or dominant language, and likely result in artificially lower scores. This phenomenon is seen in other standardized testing such as the GRE, where results from English-speaking geographies (e.g., US, Canada, Australia) on the verbal section are generally higher than those of non-English speaking geographies, while those non-English speaking geographies (e.g., China, Japan, South Korea) tend to vastly outperform on quantitative sections.[47]

Discussion of findings

Top-ranked geographies tended to be those that have developed talent and expertise in technology, including Russia, Finland, Poland, Switzerland, and the Netherlands. Italy notably also ranked exceptionally highly among European geographies. Surprisingly, Singapore, an international city-state with wide English use and one of the strongest education systems (as measured in other objectives) did not score well on this metric, ranking at only No. 35. This could imply that either language or cultural barriers play a role in the success of students when measured using this indicator.

[47] (ETS 2019)

B.5. Pillar 5: Labor upskilling

Description

Ability and actions to upskill current labor force to strengthen cybersecurity consciousness in the geography workforce.

Objectives:

- **Objective 5.1:** Government conducts, promotes, and incentivizes continued cybersecurity awareness among working population
  - *Hypothesis:* Similar to marketing campaigns, governments that increase awareness programs will likely have some positive effect on developing overall citizenry cybersecurity knowledge.
- **Objective 5.2:** Employers conduct, promote, and incentivize continued cybersecurity awareness among employees
  - *Hypothesis:* Employers have an incentive and responsibility to ensure that their workers are trained in cybersecurity. Geographies where employers take this task more seriously will develop a workforce that is more conscious of cybersecurity.
- **Objective 5.3:** Population demonstrates a willingness to pursue cybersecurity education
  - *Hypothesis:* Populations that are more willing to pursue upskilling efforts in cybersecurity education should naturally correspond with a more cybersecurity savvy population in the future.

B.5.1. Objective 5.1: Government conducts, promotes, and incentivizes continued cybersecurity awareness among working population

Indicator to measure objective

- Indicator 5.1.1: Workforce score of National Cybersecurity Strategy (Oliver Wyman Forum database assessment)
  - *Source:* Oliver Wyman analysis of national cybersecurity plans (as of September 2020)

Reason for indicator selection

Internal analysis was required as there are no known existing indicators that can measure or proxy the objective. We based our research on existing databases of cybersecurity plans, including ENISA National Cyber Security Strategies and the UNIDIR Cyber Policy Portal, supplemented with additional research to capture the most up-to-date documentation.

Government plans were assessed for content in three categories related to cyber risk literacy: education focus, from primary to graduate school; R&D, workforce and industry development; and civilian awareness. This indicator assesses the plan for content related to developing a cybersecurity workforce and increasing the cybersecurity skills and practices of companies and their employees. This indicator also captures whether the plan listed specific metrics, qualitative or quantitative, to assess success. The inclusion of metrics within these plans enable government accountability for their strategic visions and ensure governments can identify successful and lagging initiatives.

Weaknesses of indicator

Please see Weaknesses of Oliver Wyman Forum database assessments (Section C.3).

Discussion of findings

Workforce development was a generally common element of most national cybersecurity strategies. Many geographies included assistance programs for small and medium-sized enterprises (SMEs), which consistently struggle with cybersecurity given limits in resources and funding. Geography programs also tended to attempt to incentivize the development of cybersecurity careers.

Workforce development is a cornerstone of Australia's national strategy, combining a Cyber Security National Workforce Growth Program, assistance for SMEs, and strong ties between academia and industry to encourage needed innovation. Australia is also considering several relevant legislative changes relating to data privacy

protection, the cybersecurity responsibilities of management and the obligations of IoT manufacturers. The strongest government leadership in workforce development leverages the legislative and investment powers of the government to make cybersecurity a priority.

B.5.2. Objective 5.2: Employers conduct, promote, and incentivize continued cybersecurity awareness among employees

Indicators to measure objective

- Indicator 5.2.1: Percent growth in computer and network security employment
- Indicator 5.2.2: Percent growth in computer networking employment
  - *Source:* World Bank analysis of LinkedIn data (2019)

Reason for indicator selection

We did not find any survey that directly measured whether global employers (encompassing all of our Index geographies) actively trained their employees in cyber risk knowledge. However, World Bank analysis of LinkedIn data on the job growth of different fields across geographies reflect the changes in LinkedIn profiles in those geographies. We used the data under the assumption that geographies where cybersecurity-related jobs (i.e. network security and networking) are increasing means that there is a general increase in overall employer efforts to train their organization personnel in cybersecurity. We note in "weaknesses of indicator" below why we think this is one of our weaker indicators in this paper.

An alternative path we considered but ultimately did not choose was to assess anonymized external, potentially proprietary, industry data on how employers of different geographies invested in cybersecurity training for their employees. However, given the lack of dominance of a single company (e.g., in the same way that Microsoft Windows remains the dominant desktop/ laptop operating system), collecting data from a single cybersecurity company would not represent a statistically sufficient sample.

Weaknesses of indicator

There are at least two alternative ways that growth in jobs can be interpreted:

(1) A geography launched their equivalent of a Cybersecurity Silicon Valley or a free trade zone with favorable policies for cybersecurity innovation, and thus created high growth in cybersecurity-related jobs even if the rest of the geography's employers did not pay attention to cybersecurity

(2) Companies understood that they needed cybersecurity departments and simply created cybersecurity jobs without emphasizing and training the rest of their organization

Additionally, LinkedIn has been blocked in Russia since 2016[48] resulting in a proxy requirement for the geography. For these reasons, we gave this objective lower weight than others due to our quality assessment of the indicator as it pertains to the objective.

Discussion of findings

An imperfect measure at best, we saw that on a percentage basis, Singapore, Australia, Kuwait, and the UAE, all had strong job growth. Israel, generally considered a cybersecurity powerhouse, ranked less highly on this indicator, potentially because it is starting from a larger base of jobs. Despite Russia being a geography with a strong presence in cybersecurity, we nonetheless could not confidently measure Russian job growth for employer awareness of cybersecurity issues based on available data.

B.5.3. Objective 5.3: Population demonstrates a willingness to pursue cybersecurity education

Indicator to measure objective

- Indicator 5.3.1: Number of (ISC)² members holding the CISSP certification per 100,000 of population
  - *Source:* (ISC)², (2020)

[48] (Lunden 2017)

Reason for indicator selection

The International Information System Security Certification Consortium, or (ISC)², is a nonprofit organization that specializes in training and certifications for cybersecurity professionals. It issues the Certified Information Systems Security Professional (CISSP) certification globally. As of July 1, 2020, there were 141,607 (ISC)² members holding the CISSP certification worldwide. We utilized the number of CISSP-certified individuals as a proxy for how popular the independent study of cybersecurity education is across geographies.

Weaknesses of indicator

As the (ISC)² is a US-based institution, the number of CISSP-certified members of (ISC)² skew heavily toward the United States. The indicator also has skew as a result of any geographies where (ISC)² conducts greater marketing efforts for their certificates. We adjusted for this skew by applying a log transformation to the data. Finally, the cost of training and testing toward the certificate may be prohibitive for developing geographies and deflate their figures even if there would otherwise be significant interest.

Discussion of findings

English-speaking geographies naturally had a greater number of CISSP-certified individuals over non-English-speaking geographies. Singapore had the greatest number of CISSP-certified individuals normalized against its population. Because this indicator is at best a biased proxy for national interest in cybersecurity education, in the next iteration of the Index, we will likely seek to assess direct opinions from populations of these geographies as to their interests in cybersecurity education.

B.6. Pillar 6: Skill demand from employer expectations

Description

Employers believe in hiring for cyber risk skills and the importance of building a cyber risk conscious workforce to meet their future business needs.

Objectives

- **Objective 6.1:** Employers understand that cyber threats pose significant risk to their companies
  - *Hypothesis:* In order to encourage a cyber-conscious workforce, employers must first understand that cybersecurity is an important concept for business risk reduction.
- **Objective 6.2:** Employers demand digitally savvy and security-conscious workers
  - *Hypothesis:* In the same way that almost all new university graduates have some level of proficiency in Microsoft Word, Excel, and PowerPoint as a result of employer demand, geographies where employers demand workers with digital skills and security basics will incentivize students to train in these skills.
- **Objective 6.3:** Cybersecurity-specialized skill demanding jobs are fulfilled by qualified candidates
  - *Hypothesis:* Geographies where there are significant cybersecurity skill demands and where those skill demands are being filled will likely correlate with a higher number of qualified candidates with fundamental cybersecurity understanding in the population.

B.6.1. Objective 6.1: Employers understand that cyber threats pose significant risk to their companies

Indicator to measure objective

- Indicator 6.1.1: Relative ranking of "cybersecurity" as a risk in WEF Executive Opinion Survey of Risks Facing Employer
  - *Source:* World Economic Forum Executive Opinion Survey (2019)

Reason for indicator selection

Marsh conducted a joint 2019 Global Cyber Risk Perception Survey with Microsoft with relevant survey questions for this objective. However, the data was limited to regions rather than the geography level. Thus, we selected the World Economic Forum Executive Opinion Survey, as the WEF has broad global membership and the survey contained a question that directly reflects whether respondents believed that cybersecurity (in the form of cyberattacks) was a highly ranked prevalent threat. This was the most relevant and comparable proxy we found to be available.

Weaknesses of indicator

The World Economic Forum provided only a limited number of spaces for employers to rank what they considered to be their biggest risks. Our method chose to consider employers that ranked cyberattacks as a risk more favorably over employers that ranked cyberattacks lower or not at all. However, it is possible that in certain geographies, other risks are simply more prevalent for the employer (e.g., failure of national government). Oliver Wyman Forum will look to conduct additional independent research around this topic in the future.

It is also important to note that although this indicator reflects our objective, survey data faces inherent methodological weaknesses (as discussed in Section C.6). In this instance, the data is based on expert opinion and subject to personal biases (e.g., if an expert had an overly positive or overly negative opinion about certain risks in a geography).

B.6.2. Objective 6.2: Employers demand digitally savvy and security-conscious workers

Indicator to measure objective

- Indicator 6.2.1: Extent to which population possesses sufficient digital skills (computer skills, basic coding, digital reading)
  - *Source:* Network Readiness Index from the WEF Executive Opinion Survey (2019)

Reason for indicator selection

The World Economic Forum's Executive Opinions survey asked respondents to judge the active population's digital skills. Higher levels of digital skills would likely correlate with employer demands for those skills as it incentivizes the population to train toward those skills for employment.

Weaknesses of indicator

As mentioned, survey data faces inherent methodological weaknesses (as discussed in Section C.6). In this instance especially, the data is based on expert opinion and subject to personal biases.

Discussion of findings

As with other opinion-based surveys, we found that opinions showed that the usual set of economically developed geographies such as Sweden, Switzerland, the US, and others ranked highest. We were surprised that opinions on Japanese population digital skills were on the lower end of the spectrum, but independent experts we spoke with also affirmed that the Japanese population have a large digital divide, particularly among urban and rural populations when it comes to the workforce.

B.6.3. Objective 6.3: Cybersecurity-specialized skill demanding jobs are fulfilled by qualified candidates

Indicator to measure objectives

- Indicator 6.3.1: Percentage of people moving to a position in computer and network security in the geography
  - *Source:* World Bank analysis of LinkedIn data (2019)

Reason for indicator selection

We hypothesize that more LinkedIn profiles indicating movements into the computer and network security industry mean that more individuals are filling jobs – leading to a virtuous cycle of employers expanding their expectations of cyber risk requirements.

Weaknesses of indicator

The data relies on samples from LinkedIn profiles, which likely skew toward developed nations. However, the World Bank's data analysis team has attempted to adjust for these biases prior to publishing the results.

Discussion of findings

Russia leads this metric, likely reflecting the geography's ability to train and place new talent in this area. Several Eastern and Southeastern European geographies also performed well on this metric, including Bulgaria, Cyprus, Croatia, and the Czech Republic. India, however, despite being a global IT powerhouse, ranked poorly, perhaps a reflection of a shift in the attractiveness of alternative roles in the country or the loss of talent to foreign countries leading to domestic jobs going unfilled.

B.7. Pillar 7: Innovation-driven demand for skills

Description

Cyber-risk research and development output establishes a current need towards hiring cyber-risk conscious workers.

Objectives:

- **Objective 7.1:** Geography outputs intellectual ideas on new cybersecurity technologies
  - *Hypothesis:* Geographies that produce more intellectual property on cybersecurity technologies will likely also have a demand for workers who are trained in the fundamentals of cybersecurity.
- **Objective 7.2:** Geography translates cybersecurity research and development into commercial solutions
  - *Hypothesis:* Geographies that are translating R&D into commercial solutions will have a need for employees who are trained in the fundamentals of cybersecurity.
- **Objective 7.3:** Geography collaborates between government, industry, and academia on cybersecurity issues and solutions
  - *Hypothesis:* Greater positive collaboration between institutions results in a higher number of opportunities to train the population in cybersecurity fundamentals and encourage innovation to meet government and population needs.
- **Objective 7.4:** Government pursuing security-by-design through edict
  - *Hypothesis:* Government edicts mandating/ encouraging cybersecurity features in technology products will drive innovations in the security space in each geography, which will likely drive demand for workers trained in the fundamentals of cybersecurity to build safer products.

B.7.1. Objective 7.1: Geography outputs intellectual ideas on new cybersecurity technologies

Indicators to measure objective

- Indicator 7.1.1: PCT Patents per 100,000 of population (in telecommunications, digital communication, computer technology, IT methods for management, and basic communication processes)
  - Note: Geographies with more patents in cybersecurity-related technology fields were weighted higher in the aggregated indicator.
  - *Source:* World Intellectual Property Organization (WIPO), (2019)
- Indicator 7.1.2: Number of publications/citations per publication (H-Index) in artificial intelligence, computer networks and communications, computer science applications, information systems, and software
  - Note: The H-Index reflects the number of publications and the number of citations per publication; documents included are defined by Scopus, an abstract- and citation-based database of peer-reviewed literature.
  - *Source:* Scimago Journal & Geography Rank (2019)

Reason for indicator selection

Not all patents and publications measure for cybersecurity-related roles. However, a larger number of patents in fields related to cybersecurity likely represents an increased number of high-skilled individuals who understand how to protect themselves against cybersecurity risks. Likewise, publications that relate to cybersecurity are used as a proxy for measuring the level of talent within the geography that likely has a level of cybersecurity training and understanding.

Weaknesses of indicator

While we normalized the number of patents and number of publications by population, this indicator does not capture patents that are not already captured by the World Intellectual Property Organization. A log

transformation was applied to both indicators to account for a large positive skew, as a few geographies had far higher levels of patents and publications than the other geographies surveyed even once adjusted for population.

Discussion of findings

As expected, several geographies are strong in both cybersecurity-related patents and publications, including Singapore and Israel. Both geographies are well-known as leaders in cybersecurity innovation and have active cybersecurity startup cultures. Their governments have also made cybersecurity a national priority and have publicly committed extensive financial resources toward achieving this goal.

B.7.2. Objective 7.2: Geography translates cybersecurity research and development into commercial solutions

Indicator to measure objective

- Indicator 7.2.1: Cybersecurity related companies founded inclusively between 2015 - 2019 per 100,000 of population
  - *Source:* Crunchbase.com (2020)

Reason for indicator selection

Crunchbase provides a dataset of startups that can be broken down specifically to the cybersecurity industry. We captured the number of companies founded in last five years so that there is a recent measure of companies. Any duplicated companies were removed from our database. Companies also must achieve a Crunchbase Rank of 100,000 or higher, this serves to largely remove the smallest companies that may be registered in name only.

Weaknesses of indicator

Crunchbase crowdsources its estimates, the gaps would likely mean that its data is less likely to be accurate for Europe and Asia while artificially inflating US-related figures. Additionally, a geography can theoretically launch an Apple-sized cybersecurity company that generates more innovation than a number of smaller companies combined. However, we chose not to weight companies based on their revenues, as this data was more available for certain geographies (e.g., the US), which would have skewed the data.

Discussion of findings

Geographies that are strong in cybersecurity startups and focused on technical innovation have strong economies, including the US, China, Singapore, and Israel, as well as prominent European geographies such as France, Germany, Switzerland, and Spain. A strong startup community in cybersecurity is an important element of a cyber risk literate geography as it is major source of innovation and investment.

B.7.3. Objective 7.3: Geography collaborates between government, industry, and academia on cybersecurity issues and solutions

Indicator to measure objective

- Indicator 7.3.1: Private public partnership score of National Cybersecurity Strategy (Oliver Wyman Forum database assessment)
  - *Source:* Oliver Wyman analysis of national cybersecurity plans (as of September 2020)

Reason for indicator(s) selection

Internal analysis was required as there are no known indicators that can measure or proxy the objective. We based our research on existing databases of cybersecurity plans, including ENISA National Cyber Security Strategies and the UNIDIR Cyber Policy Portal, supplemented with additional research to capture the most up-to-date documentation.

Government plans were assessed for content in three categories: education focus, from primary to graduate school; R&D, workforce, and industry development; and civilian awareness. This indicator assesses the plan for content related to public-private partnerships among industry, academia and the public sector in education and research. This indicator also captures whether the plan listed specific metrics, qualitative or quantitative, to assess

success. The inclusion of metrics within these plans enable government accountability for their strategic visions and ensure governments can identify successful and lagging initiatives.

Weaknesses of indicator

Please see Weaknesses of Oliver Wyman Forum database assessments (Section C.3).

Discussion of findings

While many national strategies encourage the sharing of data breach and threat information between the government and private companies, fewer extend this cooperation to innovation, investment and research. Just over 10 percent of assessed geographies articulated specific action items to encourage collaboration between industry and academia, often funded or guided by the government, although most of them did articulate a general goal in this area. More practical, executable measures for forming successful public-private partnerships in research are needed. Australia, for example, has committed AUD$26.5 million for a Cyber Skills Partnerships Innovation Fund, which will encourage businesses and academia to partner together to find innovative new ways to improve cybersecurity skills.

B.7.4. Objective 7.4: Government pursuing security-by-design through edict

Indicator to measure objectives

- Indicator 7.4.1: Security by design score of National Cybersecurity Strategy (Oliver Wyman Forum database assessment)
  - *Source:* Oliver Wyman analysis of national cybersecurity plans (as of September 2020)

Reason for indicator selection

Internal analysis was required as there are no known indicators that can measure or proxy the objective. We based our research on existing databases of cybersecurity plans, including ENISA National Cyber Security Strategies and the UNIDIR Cyber Policy Portal, supplemented with additional research to capture the most up-to-date documentation.

Government plans were assessed for content in three categories: education focus, from primary to graduate school; R&D, workforce, and industry development; and civilian awareness. This indicator assesses the plan for content related to the government's pursuit of security-by-design, a strategy in which systems and technology are built with appropriate security features, as opposed to having security features added on once the technology has been built and released. This approach of making technology smarter takes the cybersecurity onus off civilians alone and makes technology and industry a partner in cybersecurity.

Weaknesses of indicator

Please see Weaknesses of Oliver Wyman Forum database assessments (Section C.3).

Discussion of findings

Many governments are exploring security-by-design as a new cybersecurity option, particularly for consumer protection in Internet of Things products. Most governments are still in the initial stages of engaging with security-by-design, although the UK has set an ambitious goal to have the majority of new online products and services be "secure by default" by 2021, where consumers are empowered to choose products that have built-in security as a default setting.

Several other geographies, including the Netherlands, are considering standardization or certification initiatives for IoT products and other consumer products, in order to prevent digital security risks in hardware and software.

It is worth noting that a few experts highlighted that the removal of incentives for individuals (within the workforce or outside of it) to be cyber risk savvy in the use of technology could produce the net-effect of fewer individuals being cyber risk literate or educated rather than maintaining a virtuous cycle of teaching people of cyber risk reduction through the use of safer products. The salience of this potential trend will be monitored as we revise our approach to this Index.

B.8. Pillar 8: Technological inclusivity

Description

Equality in digital access, and a high level of existing digital pervasiveness across population.

Objectives

- **Objective 8.1:** Population has access to necessary computing technologies regularly
  - *Hypothesis:* A population needs access to computing equipment before the issue of cyber risk becomes relevant. Geographies that have not done enough to ensure equality in computing technology access will likely be at a lower stage of development where cyber risk literacy is not equally disseminated across the population.
- **Objective 8.2:** Population has access to high speed (25Mbps+) Internet regularly
  - *Hypothesis:* Access to high speed Internet is important for demonstrating a geography's ability to provide digital infrastructure to improve its community's general digital literacy. By extension, a more digitally literate population would also be more likely to become more aware of the associated cyber risk issues.

B.8.1. Objective 8.1: Population has access to necessary computing technologies regularly

Indicators to measure objective

- Indicator 8.1.1: Percentage of households with computer access
  - *Source:* ITU (2018)
- Indicator 8.1.2: Percentage of individuals using the Internet
  - *Source:* ITU (2018)

Reason for indicator selection

Both computer access and Internet usage determine the access individuals have to the digital economy. Geographies with more equality in access should directly have populations that are more literate in cybersecurity whereas the opposite is true for geographies without access.

Weaknesses of indicators

Survey data often faces inherent methodological weakness (as discussed in Section C.6).

Discussion of findings

India, though a global IT powerhouse, is also the only geography on our list defined by the World Bank as lower middle-income. Large disparity issues in the country resulted in India coming in last for inclusivity in computer access. Other geographies scoring lower on this metric were also developing geographies including South Africa, Indonesia, China, and Mexico. Several Middle Eastern geographies performed particularly well on individual access to the internet – with Kuwait and Qatar scoring at the top – while western nations, encompassing areas generally defined as high income by the World Bank, topped the measure of household access to the Internet.

B.8.2. Objective 8.2: Population has access to high speed (25Mbps+) Internet regularly

Indicators to measure objective:

- Indicator 8.2.1: Fixed broadband subscriptions per 100 inhabitants
  - *Source:* World Bank (2018)

Reason for indicator selection

Indicator directly measures the stated objective.

Weaknesses of indicators

General weaknesses of sampling data apply. In particular, it might be especially difficult to gather comparable data across developing geographies for an accurate assessment (as discussed in Section C.6).

Discussion of findings

Similar to access to computing technologies, our source data shows that India came in last for inclusivity in technology with the lowest number of broadband subscriptions per 100 inhabitants. This can likely be attributed to its large population size and wide-ranging differences in privilege and access.

Singapore also ranked lower on this indicator than would have been expected of a highly developed city-state; this outcome is possibly a reflection of Singapore's relatively high levels of income inequality compared with other developed nations.[49] The Singaporean government however recognizes the connectivity divide. The government's Digital Readiness Blueprint, launched in 2018 by Minister for Communications and Information S. Iswaran, aims to achieve universal digital access where "every Singaporean, young or old, disabled or able, rich or poor, is empowered with access and skills to thrive in the digital future" while acknowledging the uneven adoption of digital technologies in the geography.[50]

[49] (Solt 2020)
[50] (Yip 2020)

B.9. Pillar 9: Educational inclusivity

Description

Availability of programs and resources geared toward vulnerable populations (e.g., elderly) and actively seeks to conduct outreach to encourage such communities to learn about foundational cybersecurity issues.

Objectives:

- **Objective 9.1:** Geography provides equal opportunities for educational access across its population segments
  - *Hypothesis:* Geographies must develop educational systems that provide equality in access rather than simply focusing on a segment of the population to ensure that cybersecurity education is also made available across the entire population.
- **Objective 9.2:** Government provides funding for the development of national cyber risk literacy and education campaigns across different demographics
  - *Hypothesis:* Governments that allocate a greater level of funding across a variety of demographics show a stronger commitment to inclusive cyber risk literacy and will ultimately produce a more broadly cyber risk aware population.
- **Objective 9.3:** Government promotes cybersecurity awareness messages, has effective delivery mechanisms, and stimulates interest on the topic
  - *Hypothesis:* Governments that place a stronger emphasis on directly promoting awareness messaging or mechanisms of training for its population will likely reach a broader base of its citizens and residents, and create a more inclusively cybersecurity savvy population.
- **Objective 9.4**: Government conducts, promotes, and incentivizes continued cybersecurity awareness among underserved populations
  - *Hypothesis:* Those most at risk offline are usually also the most at risk online. Governments must be inclusive in its awareness campaigns and reach populations that are traditionally less likely to be aware of cybersecurity issues.

B.9.1. Objective 9.1 Geography provides equal opportunities for educational access across its population segments

Indicators to measure objective

- Indicator 9.1.1: Difference between Urban - Rural lower secondary completion rate
- Indicator 9.1.2: Difference between Urban - Rural upper secondary completion rate
- Indicator 9.1.3: Difference between Male - Female primary completion rate
- Indicator 9.1.4: Difference between Male - Female lower secondary completion rate
- Indicator 9.1.5: Difference between Male - Female upper secondary completion rate
  - *Source:* World Inequality Database on Education, (as of September 2020)

Reason for indicator selection

The World Inequality Database on Education brings together data from Demographic and Health Surveys, Multiple Indicator Cluster Surveys, other national household surveys and learning assessments from over 160 geographies.

There are several ways to consider educational inclusion. Due to the wide-ranging geographies covered, we chose to assess the differences in completion rates for both upper secondary and lower secondary school against rural – urban and male – female differences. Male – female completion rates were also assessed for primary level education, but rural – urban datasets were incomplete and thus intentionally left out of the assessment. These metrics provides a sense of education equality between urban and rural areas and whether there are differences in access to education based on gender.

We assumed that due to socioeconomic factors, on average, rural completion rates for education would be lower than urban completion rates, and female completion rates lower than male completion rates. In some geographies where data showed higher completion rates among rural residents than urban residents or among females over males, we assumed that the geography has achieved equal opportunity (i.e. a geography where both male and female completion rates are 80 percent is equivalent to a geography where male completion rate is 80 percent but female completion rate is 85 percent).

Weaknesses of indicators

The data has a few challenges we did not address. First, urban - rural definitions change over time, particularly in rapidly developing economies like China.

Second, we chose not to weight urban - rural populations when taking the difference between completion rates. Thus, it is possible that certain geographies with a wide gap in urban - rural education are artificially higher or lower as a result. For example, in the hypothetical extreme example of Geography A where the rural completion rate is 10 percent and urban completion rate is 90 percent, but where 99 percent of the population lives in an urban area, our indicator would show a wider disparity than the reality.

This same logic applies to male - female differences in completion. However, while births are naturally male-biased (at around 105 males per 100 female births)[51], gender imbalances overall should not materially affect results as they tend to become increasingly balanced across population over time.[52]

Additionally, we did not include an indicator to measure other such disparities as income level, which likely is correlated to the urban - rural divide. We additionally did not include differences by ethnicity or immigrants as these indicators were less likely to be globally comparable.

Finally, general weaknesses to sampling data apply to the original data sources.

Discussion of findings

Not surprisingly, we found that disparities among developed geographies tended to be lower than those of developing geographies. One exception is the Netherlands, which displayed a large discrepancy in upper secondary education rates for urban and rural areas. However, we also found that within developing geographies, government policies have helped to achieve high levels of gender equality in education (e.g., China) even if there remains a sizable urban - rural gap. In some developed geographies, our data showed that rural completion rates were higher than urban completion rates (which we considered the same as perfect equality). Similarly, in geographies like China and the United States, where female school completion rates are higher than those of male school completion rates, we considered this equivalent to perfect gender equality at the given education level.

B.9.2. Objective 9.2: Government provides funding for the development of national cyber risk literacy and education campaigns across different demographics

Note: Our research indicates that this objective did not have a measurable indicator or data and thus has a weight of 0 percent on this pillar.

Indicators to measure objective

- Indicator 9.2.1: N/A
  - *Source:* Oliver Wyman analysis of national cybersecurity plans (as of September 2020)

Reason for indicator selection

We reviewed government cybersecurity plans (and relevant implementation plans) for any indication of funding allocated toward national cyber risk literacy and education campaigns. With the notable exception of Australia, which provides a detailed budget breakdown for all cybersecurity programs and initiatives in its strategy, few other governments publish such information. Rather than significantly increase the scores of only a few geographies, we chose to exclude this objective from being weighted in the pillar until better data is available.

[51] (Ritchie 2019)
[52] (UN Department of Economic and Social Affairs 2019)

Weaknesses of indicator

Though we did not find publicly comparable data for this metric, government funding data may not always be directly comparable even once adjusted for population. For example, economies of scale can mean that larger geographies can spend comparatively less while still achieving the same overall effect.

Discussion of findings

Though governments generally did not release funding breakdowns, we maintain that this is an important objective. Governments must demonstrate transparent funding in their allocation of budgets to appropriately allocate funding towards cyber risk literacy and education. As a result, we recommend that geographies set more transparent standards in funding allocation for cyber risk literacy. We have kept this objective as a component of our Index in the hope of populating it with relevant data in the future.

B.9.3. Objective 9.3: Government promotes cybersecurity awareness messages, has effective delivery mechanisms, and stimulates interest on the topic

Indicator to measure objective

- Indicator 9.3.1: Awareness score of National Cybersecurity Strategy (Oliver Wyman Forum database assessment)
  - *Source:* Oliver Wyman analysis of national cybersecurity plans (as of September 2020)

Reason for indicator selection

Internal analysis was required as there are no known existing indicators that can measure or proxy the objective. We based our research on existing databases of cybersecurity plans, including ENISA National Cyber Security Strategies and the UNIDIR Cyber Policy Portal, supplemented with additional research to capture the most up-to-date documentation.

Government plans were assessed for content in three categories related to cyber risk literacy: education focus, from primary to graduate school; R&D, workforce, and industry development; and civilian awareness, with a focus on underserved populations such as seniors. This indicator assesses the plan for content related to public awareness campaigns and publicly available resources on cyber risk literacy. This indicator also captures whether the plan listed specific metrics, qualitative or quantitative, to assess success. The inclusion of metrics within these plans enable government accountability for their strategic visions and ensure governments can identify successful and lagging initiatives.

Weaknesses of indicator

Please see Weaknesses of Oliver Wyman Forum database assessments (Section C.3).

Discussion of findings

Every cybersecurity strategy assessed includes a goal around instituting (or maintaining, or supplementing) a public awareness campaign. More committed geographies operate a cybersecurity portal for the public with educational materials and updates. A few geographies offer unique and creative approaches to engaging and educating the public in cybersecurity. For example, Singapore's Neighborhood Police Centers frequently engage residents through Community Safety & Security Programs, and a Public Cyber-Outreach & Resilience Program that uses behavioral insights to nudge the general public to adopt good cyber hygiene practices. Singapore also maintains a Scam Alert website. Australia is introducing a 24/7 cyber security advice hotline for SMEs and families. Additionally, Australia offers support for victims of cybercrimes through programs such as IDCARE, a free specialist identity and cybercrime support service.

B.9.4. Objective 9.4: Government conducts, promotes, and incentivizes continued cybersecurity awareness among underserved populations

Indicator to measure objectives

- Indicator 9.4.1: Underserved score of National Cybersecurity Strategy (Oliver Wyman Forum database assessment)
  - *Source:* Oliver Wyman analysis of national cybersecurity plans (as of September 2020)

Reason for indicator selection

Internal analysis was required as there are no known existing indicators that can measure or proxy the objective. We based our research on existing databases of cybersecurity plans, including ENISA National Cyber Security Strategies and the UNIDIR Cyber Policy Portal, supplemented with additional research to capture the most up-to-date documentation.

Government plans were assessed for content in three categories related to cyber risk literacy: education focus, from primary to graduate school; R&D, workforce, and industry development; and civilian awareness. This indicator assesses the plan for content aimed at underserved populations such as seniors, non-native language speakers, or citizens in rural areas. This indicator also captures whether the plan listed specific metrics, qualitative or quantitative, to assess success. The inclusion of metrics within these plans enable government accountability for their strategic visions and ensure governments can identify successful and lagging initiatives.

Weaknesses of indicator(s)

Please see Weaknesses of Oliver Wyman Forum database assessments (Section C.3).

Discussion of findings

Our data suggest that governments should be doing more to address population inclusivity. Very few plans directly addressed the needs of seniors, and those that do are frequently vague and lack specificity. Almost no plans addressed concerns for developmentally challenged individuals. Beyond the previous examples, plans need to consider other often underserved groups such as women, immigrants, non-native language speakers, etc. Cyber risk literacy and education is still a relatively new topic, and governments, already struggling to deliver the importance of this message to traditionally well-served segments of their population, are all the more challenged to relay messages to underserved citizens. While the plans we reviewed showed that a number of governments acknowledge the need for tailored education, few have taken the necessary steps to provide it.

Appendix C. Weaknesses and future improvements

We explain key weaknesses of our Index methodology in this section. We invite policymakers, experts and the general public to provide us with feedback and suggestions for future improvements by emailing OWForum@oliverwyman.com.

C.1. General weaknesses

A set of general weaknesses apply to our Index:

- Economic and social indicators cannot reflect the full range of factors that affect cyber risk literacy, and no complete list of factors affecting cyber risk literacy can be created.
- Our expert committee have confirmed through majority vote that the indicators used in this Index correlate with our objectives, but other experts may have alternative opinions on what is and is not relevant, or whether second- or third-degree effects may impactfully alter the expected result.
- Finally, there is inherently some observer bias in our inaugural Index. While Oliver Wyman Forum is run with a global body of steering committee members, governance members, and interviewees, diverse in region, gender, and ethnicity, much of the research was done in (or translated) into English. Though we attempted to limit bias as much as possible, there remains the possibility that perspectives and indicator choices may be swayed.

C.2. Index design weaknesses

There are also some areas of subjectivity in the Index's design which include:

- Weighting is determined by our committee of experts, and while all efforts have been made to eliminate or reduce the influence of various biases, including geographic, racial, or ethnic, opinions of our experts naturally will differ among themselves.
- Cyber risk literacy is a new field and limited research has been conducted. We provided a logical argument for why we believe that the various indicators measure their respective objectives either directly or as a relevant proxy. In some cases, the measurement may be more straightforward than others. In future releases, we will continue to assess the appropriateness of these indicators and will likely supplement them with Oliver Wyman Forum surveys that aim to more closely measure each objective.
- As a result of the indicator selection process, individual objectives – or even pillars – can carry potential biases if a particular geography happens to perform exceptionally well on a given indicator. This bias is increasingly mitigated upon each of the aggregated levels of the Index (for example at the driver level, and the overall Index itself). Nonetheless, future versions will continue to assess the quality of indicators selected and either add or replace indicators that could be more representative of the objective.
- We recognize that summing the weighted scores of our five drivers implies that pillars are additive; that is, deficiency in government policy could be counteracted by high levels of public motivation, employment policy, education system, or population inclusivity. In particular, in the real world, population inclusivity, which measures for educational and technological inclusiveness, may not be independent of other indicators. We tested various scoring methodologies, such as multiplying the driver values to show interrelations, which generally showed only a few movements of no more than plus or minus three ranks. However, a select few geographies like India, South Africa, and Romania, showed greater movements if inclusivity is not included. In future versions, we will include additional considerations around this measurement.

C.3. Weaknesses of Oliver Wyman Forum database assessments

C.3.1. General weaknesses of Oliver Wyman Forum database assessments

We began by building upon on previously conducted research by other organizations that collected national cybersecurity strategy plans and national curricula and supplemented this work with our own in-house research. While we captured what we believe to be the most up-to-date version of each geography's cybersecurity strategy, national curriculum, and supporting documents, it is possible that certain updates have been overlooked or updated during our review. We invite governments and educators to submit to us any documents that may be relevant.

For national cybersecurity strategies, we did not have a method of assuring that nations followed through on their plans. Instead, we conducted our assessment based on whether various tenets our experts believed were important (e.g., developing students, inclusivity) were mentioned in each plan. We also assessed whether there were targeted actions listed to achieve the goals of each plan, as well as quantitative or qualitative measurements associated with those goals, which experts we spoke with felt more likely demonstrates an ability to achieve these end goals. Additionally, some nations may have more in-depth actions or measurements than others, but if they met what we considered to be a "baseline" set of measurements, they received the same score within our rubric.

Some nations may be less transparent in releasing various cybersecurity plans, even if they have been developed, given confidentiality and security concerns or interests.

When nations do not release plans, curricula, or other relevant documents in English, we searched in foreign languages. When the language was not native to the project team or other research staff, the search was conducted via Google Translate to arrive at various local language websites, and found documents were then translated using the Google Translate service. This may lead to situations where we have not captured relevant pieces of documents due to translation errors.

Reports that we pulled may be in the process of being updated but may not yet have been released, which could bring a nation's score higher in the rankings in a future iteration of the Index.

Our rubrics were constructed based on internal public policy and education expertise. However, other frameworks may aim to measure other details, or the same details in greater or less depth. For example, we gave points to national cybersecurity strategies that presented a reasonable method of both quantitative and qualitative measurement of implementation success, while another framework may assign points for including measurements for only one or the other.

Sources we reviewed are listed in Appendix E: National cybersecurity strategies and curricula sources. We invite any relevant feedback of any additional documents or websites we should review in future updates or versions.

C.3.2. Education plan specifics

As discussed in detail in Section A.1.4, education plans, curricula, and supplementary documents have two primary weaknesses:

- Not all nations release national education curricula (for example, the US). In these cases, we assessed how to proxy the curricula either by assessing general education guidelines/regulations or by reviewing the curricula of the nation's largest state, region or province.
- Education curricula are updated less frequently (often only every five to ten years or an even longer period), and unlike cybersecurity strategy plans, are generally meant solely for internal consumption. Additionally, national level education plans, requirements, and guidelines are sometimes intentionally left to the interpretation of various regional governments to implement in a customized fashion for their region, as is the case with China.[53] Thus, different levels of government would implement plans in a manner that they believe best fit their individual regional economies.

[53] (Pan, Vayssettes and Fordham 2016)

C.4. Data availability

Data availability is a significant challenge for any Index encompassing many indicators, for example:

- We wanted to select indicators for objectives that are considered unbiased, and available across all geographies. However, this means that certain unbiased indicators might have been omitted because the indicators did not cover enough geographies on our list. For example, while research has been done for a small set of geographies on how a national population understands cyberliteracy terms, this data was not comparable across our list of geographies.
- In some cases where data was generally available for all but a few geographies, we had to proxy the data, such as using a culturally and economically similar neighboring population (see Appendix F: Data imputation percent by geography).
- Certain data points may be discontinued in the future or become irrelevant, and we will likely need to replace them with alternative sources of the data if such events occur.

C.5. Data bias

Various data biases can occur in our indicators including:

- Some indicators may be biased toward a specific geography (e.g., more patents are filed by China and the United States simply due to larger populations). In these cases, we adjusted the data by using a relevant denominator (e.g., per 100,000 people) or a transformation (e.g. log transformation).
- The source's ability to collect equal data across all included geographies may show certain biases. For example, though CrunchBase is the world's leading[54] site for data on funding of startups, it largely skews toward companies receiving US investments and is less accurate in Europe and Asia. This may unfairly penalize some geographies. Again, in these limited cases we either chose not to use such an indicator to measure an objective, to amend its weighting to reflect its limitations, or to account for this bias using a relevant denominator or transformation.
- Some geographies on our list have larger digital access or education divides. Thus, some statistics may be skewed as we can only measure various cybersecurity indicators from the population that is online. We attempted to balance this by including "Population Inclusivity" as a separate and transparent pillar.
- More developed geographies may lend themselves to a greater volume of cyberattacks due to the higher reward of a successful breach, which may bias certain indicators.
- In limited cases, our indicators may be biased toward a specific geography (e.g., if a certification is issued by a US-based body, it is likely that there would be more uptake in the US for the certification). We limited use of such data and have called out where we had done so as well as any potential statistical adjustment for bias.
- Reporting bias may exist in government-released data, which in some cases could skew data to appear more favorable. As a result, certain statistics are more difficult to compare, even though we limited ourselves to official published sources or an established aggregator (e.g., OECD).

C.6. Survey weaknesses

Several indicators in this report leverage source data that rely on survey interviews. Although care has been taken in these instances to use highly reputable sources (such as multilateral or international organizations, or academic or corporation-commissioned studies), survey data tend to suffer inherent methodological weaknesses that may result in non-standardized data. These include:

- Sampling biases that skew responses toward particular answers by over-sampling certain demographics, communities or nature of individual.
- Survey design or question format irregularities that encourage responder bias toward particular answers (e.g. offering an ordinal ranking question with a large number of options may result in random responses).
- Survey responses are inevitably subject to human error – rather than reflecting objective reality, they may ultimately reflect a certain community's perception or opinion.

[54] (Archer 2019)

Appendix D. Summary of Index indicator data and sources

This Index uses a mixture of both publicly available data and independent Oliver Wyman Forum analysis of government policies and curricula from the Oliver Wyman Forum. Public sources are identified below. Some indicator names may include "detailed phrasing" that provides more context of the indicator's intended interpretation. Indicators marked with an asterisk (*) were log-normalized to account for data skew. In some limited situations, we used more than one indicator for an objective and the indicator may have unequal weights to account for indicator quality.

Table 8: Pillars, and indicators and indicator sources for the Cyber Risk Literacy and Education Index

Pillar	Indicator number	Indicator	Unit (*log-normalized)	Dates used of indicator	Source	Source release date
PILLAR 1: Cyber risk awareness and motivation	1.1.1	Average percentage of machines running Microsoft that encountered malware	#	2019	Microsoft Security Intelligence Report	2020
	1.1.2	Local infections on computers with Kaspersky security software	#	July 2020	Kaspersky Cyber map	2020
	1.2.1	Percentage of individuals who report avoiding opening emails from unknown addresses *(Detailed phrasing: Due to security concerns, percentage of population answering that they have begun avoiding opening emails from unknown addresses in past year)*	%	2019	Special Eurobarometer 499: Europeans' attitudes towards cyber security Supplement: CIGI-Ipsos Global Survey on Internet Security and Trust	2019
	1.2.2	Percentage of individuals who report changing passwords regularly *(Detailed phrasing: Due to security concerns, percentage of population that has begun changing passwords regularly in past year)*	%	2019	Special Eurobarometer 499: Europeans' attitudes towards cyber security Supplement: CIGI-Ipsos Global Survey on Internet Security and Trust	2019
	1.2.3	Market share of all non-Internet Explorer and 25 percent of non-legacy Edge browsers	%	2019	Statcounter: Browser version market share	Sep 2020
PILLAR 2: Cultural proclivity towards security risk reduction	2.1.1	Duckduckgo.com search engine market share	%	2020	Statcounter: Search Engine Market Share	July 2020
	2.2.1	Discloses less personal information online *(Detailed phrasing: Due to security concerns, percentage of population that has begun disclosing less personal information online in past year)*	%	2019	Special Eurobarometer 499: Europeans' attitudes towards cyber security Supplement: CIGI-Ipsos Global Survey on Internet Security and Trust	2019

Pillar	Indicator number	Indicator	Unit (*log-normalized)	Dates used of indicator	Source	Source release date
	2.3.1	Average total years of schooling of adult population	#	2018	United Nations Development Programme, Human Development Report (2019 Statistical Update)	2019
	2.4.1	Percentage of population that has confidence in the national government	%	2018; 2019	Welcome Global Monitor Supplement: Edelman Trust Barometer 2020	2019; 2020
	2.5.1	Percentage of population that feel physically safe in their geography *(Detailed phrasing: Percentage of population that feels safe walking alone at night)*	%	2019	Gallup Global Law and Order Report	2019
PILLAR 3: Long-term vision and commitment	3.1.1	Overall score of National Cybersecurity Strategy (Oliver Wyman Forum database assessment)	0-10	Latest available	See Appendix E: National cybersecurity strategies and curricula sources for full list of national cybersecurity strategies consulted	As of September 2020,
	3.2.1	Measurable score of National Cybersecurity Strategy (Oliver Wyman Forum database assessment)	0-4	Latest available	See Appendix E: National cybersecurity strategies and curricula sources for full list of national cybersecurity strategies consulted	As of September, 2020
	3.3.1	Adoption of cybercrime and e-commerce legislation	0-4	2020	UNCTAD Global Cyberlaw Tracker	February 2020
	3.4.1	Net migration for jobs with cybersecurity skills from global LinkedIn profiles	Per 10,000 people	2019	World Bank—LinkedIn Digital Data	2019
PILLAR 4: Formal education	4.1.1	Program for International Student Assessment (PISA) math score;	#	2018	OECD	2018
	4.1.2	Program for International Student Assessment (PISA) science score	#	2018	OECD	2018
	4.2.1	Use of Internet in schools for learning purposes	0-7	2016-2017 weighted average	World Economic Forum Executive Opinion Survey	2017-2018
	4.3.1	Primary school education curriculum analysis (Oliver Wyman Forum database assessment)	0-13	Latest available	See Appendix E: National cybersecurity strategies and curricula sources for full list of national curricula consulted	As of September, 2020
	4.4.1	Secondary school education curriculum analysis (Oliver Wyman Forum database assessment)	0-13	Latest available	See Appendix E: National cybersecurity strategies and curricula sources for full list of national curricula consulted	As of September, 2020

Pillar	Indicator number	Indicator	Unit (*log-normalized)	Dates used of indicator	Source	Source release date
	4.5.1	Coursera Technology Skill ranking	%	Latest available	Coursera Global Skills Index	As of September, 2020
PILLAR 5: Labor upskilling	5.1.1	Workforce score of National Cybersecurity Strategy	0-3	Latest available	See Appendix E: National cybersecurity strategies and curricula sources for full list of national cybersecurity strategies consulted	As of September, 2020
	5.2.1	Percent growth in computer and network security employment	%	2019	World Bank—LinkedIn Digital Data	2019
	5.2.2	Percent growth in computer networking employment	%	2019	World Bank—LinkedIn Digital Data	2019
	5.3.1	Number of (ISC)² members holding the CISSP certification per 100,000 of population	*#	2020	(ISC)²	2020
Pillar 6: Skill demand from employer expectations	6.1.1	Relative ranking of "cybersecurity" as a risk in WEF Executive Opinion Survey of Risks Facing Employer	0-5 (translated to %)	2019	WEF Regional Risks of Doing Business Report	2019
	6.2.1	Extent to which population possesses sufficient digital skills (computer skills, basic coding, digital reading)	1-7	2018-2019 weighted	World Economic Forum Executive Opinion Survey	2019
	6.3.1	Percentage of people moving to a position in computer and network security	%	2019	World Bank—LinkedIn Digital Data	2019
PILLAR 7: Innovation-driven demand for skills	7.1.1	PCT Patents per 100,000 of population (in telecommunications, digital communication, computer technology, IT methods for management, and basic communication processes);	*#	2019	WIPO	2019
	7.1.2	Number of publications/citations per publication (H-Index) in artificial intelligence, computer networks and communications, computer science applications, information systems, and software	*H-Index	2019	Scimago Journal and Geography Rank	2019
	7.2.1	Cybersecurity related companies founded inclusively between 2015 - 2019 per 100,000 of population	#	2015-2020	Crunchbase	2020
	7.3.1	Private public partnership score of National Cybersecurity Strategy (Oliver Wyman Forum database assessment)	0-3	Latest available	See Appendix E: National cybersecurity strategies and curricula sources for full list of national cybersecurity strategies consulted	As of September, 2020

Pillar	Indicator number	Indicator	Unit (*log-normalized)	Dates used of indicator	Source	Source release date
	7.4.1	Security by design score of National Cybersecurity Strategy (Oliver Wyman Forum database assessment)	0-3	Latest available	See Appendix E: National cybersecurity strategies and curricula sources for full list of national cybersecurity strategies consulted	As of September, 2020
PILLAR 8: Technological inclusivity	8.1.1	Percent of households with computer access	%	2017	ITU	2018
	8.1.2	Percent of individuals using the Internet	%	2017 and 2018	ITU	2018 (available data as of Sep 2020)
	8.2.1	Fixed broadband subscriptions per 100 inhabitants	Per every 100 people in geography	2017 and 2018	ITU, World Telecommunication/ICT Development Report and database (accessed via World Bank)	2018 (available data as of Sep 2020)
PILLAR 9: Educational inclusivity	9.1.1	Difference between Urban – Rural lower secondary completion rate	%	Latest available	UNESCO World Inequality Database on Education; World Bank	As of September, 2020
	9.1.2	Difference between Urban—Rural upper secondary completion rate	%	Latest available	UNESCO World Inequality Database on Education; World Bank	As of September, 2020
	9.1.3	Difference between Male – Female primary completion rate	%	Latest available	UNESCO World Inequality Database on Education; World Bank	As of September, 2020
	9.1.4	Difference between Male—Female lower secondary completion rate	%	Latest available (as of Sep 2020)	UNESCO World Inequality Database on Education	2020
	9.1.5	Difference between Male—Female upper secondary completion rate	%	Latest available (as of Sep 2020)	UNESCO World Inequality Database on Education; World Bank	2020
	9.2.1	N/A – *Note: Our research indicates that this objective did not have a measurable indicator or data and thus has a weight of 0 percent on this pillar.*	N/A	N/A	N/A	N/A
	9.3.1	Awareness score of National Cybersecurity Strategy (Oliver Wyman Forum database assessment)	0-3	Latest available	See Appendix E: National cybersecurity strategies and curricula sources for full list of national cybersecurity strategies consulted	As of September, 2020
	9.4.1	Underserved score of National Cybersecurity Strategy (Oliver Wyman Forum database assessment)	0-3	Latest available	See Appendix E: National cybersecurity strategies and curricula sources for full list of national cybersecurity strategies consulted	As of September, 2020

Appendix E. National cybersecurity strategies and curricula sources

Please refer to Section C.3 for a discussion of the weaknesses of our database assessments.

As with qualitative analysis and coding exercises of this kind, we gathered the documents and completed our analysis on a best-efforts basis across all geographies. We invite governments to reach out directly to us at OWForum@oliverwyman.com if there are additional documents you believe would be relevant for your geography to be considered in a future update. We will continue to maintain a repository of documents for consideration by Oliver Wyman Forum or other external researchers and stakeholders.

Table 9: National cybersecurity strategy and curriculum sources for the Cyber Risk Literacy and Education Index

Geography	National cybersecurity strategy (link)	National curricula website (link)
Argentina	ARG_NCS	ARG_Curricula_es
Australia	AUS_NCS	AUS_Curricula_en
Austria	AUT_NCS	AUT_Curricula_de
Belgium	BEL_NCS	BEL_Curricula_fr BEL_Curricula_nl
Brazil	BRA_NCS	BRA_Curricula_pt
Bulgaria	BGR_NCS	BGR_Curricula_bg
Canada	CAN_NCS CAN_Action Plan	CAN_Curricula_Ontario CAN_Curricula_BC CAN_Curricula_Quebec
China	CHN_NCS	CHN_Five_Year_Plan_en CHN_Education_Snapshot_en CHN_Education_Reform_Plan_en
Croatia	HRV_NCS	HRV_Curricula_hr
Cyprus	CYP_NCS	CYP_Curricula_el
Czech Republic	CZE_NCS CZE_Action Plan	CZE_Curricula_cs
Denmark	DNK_NCS	DNK_Curricula_da
Estonia	EST_NCS	EST_Curricula_en
Finland	FIN_NCS FIN_Action Plan	FIN_Curricula_en
France	FRA_NCS	FRA_Curricula_fr
Germany	DEU_NCS	DEU_Curricula_NRW_de
Greece	GRC_NCS	GRC_Curricula_en
Hungary	HUN_NCS	HUN_Curricula_hu
India	IND_NCS	IND_Curricula_en
Indonesia	IDN_NCS	IDN_Curricula_id
Ireland	IRL_NCS	IRL_Curricula_en

Geography	National cybersecurity strategy (link)	National curricula website (link)
Israel	ISR_NCS Resolution 2443 Resolution 2444 Resolution 3611	ISR_Curricula_he
Italy	ITA_NCS ITA_Action Plan	ITA_Curricula_it
Japan	JPN_NCS	JPN_Curricula_en JPN_Curricula_jp
Kuwait	KWT_NCS	KWT_Curricula_ar
Latvia	LVA_NCS	LVA_Curricula_lv
Lithuania	LTU_NCS	LTU_Curricula_lt
Mexico	MEX_NCS	MEX_Curricula_es
Netherlands	NLD_NCS	NLD_Curricula_nl
New Zealand	NZL_NCS	NZL_Curricula_en
Norway	NOR_NCS	NOR_Curricula_no
Poland	POL_NCS	POL_Primary_Education_Law_pl POL_Secondary_Education_Law_pl
Portugal	PRT_NCS	PRT_Curricula_pt
Qatar	QAT_NCS	QAT_National_Vision_2030
Romania	ROU_NCS	ROU_Curricula_ro
Russia	RUS_NCS	RUS_Curricula_ru
Saudi Arabia	SAU_NCS	SAU_National_Vision_2030
Singapore	SGP_NCS	SGP_Curricula_en
Slovakia	SVK_NCS	SVK_Curricula_sk
Slovenia	SVN_NCS	SVN_Curricula_sl
South Africa	ZAF_NCS	ZAF_Curricula_en
South Korea	KOR_NCS	KOR_Curricula_ko
Spain	ESP_NCS	ESP_Education_Law_2013 ESP_Education_Law_2006 ESP_Digital_Competence_Framework
Sweden	SWE_NCS	SWE_Curricula_en
Switzerland	CHE_NCS CHE_Action Plan	CHE_Curricula_de
Turkey	TUR_NCS	TUR_Education_Law_Primary TUR_Education_Law_Secondary
United Arab Emirates	ARE_NCS	ARE_Curricula_ar
United Kingdom	GBR_NCS	GBR_Curricula_Scotland GBR_Curricula_England GBR_Curricula_Wales
United States	USA_NCS	USA_Curricula_CA USA_Curricula_TX

Appendix F. Data imputation percent by geography

Data availability is a significant constraint for an Index that uses different variables. The table below shows the percent of indicators for each geography that required imputation. The European Union is omitted from this analysis as it is assessed a population-weighted aggregation of the European geographies in the Index even when some of the underlying EU country's original data was itself subject to data imputation. This assessment is against all indicators utilized, including limited cases where sub-indicators built up into a single overarching indicator (e.g., different types of cyber-related publications building up to a single indicator of publications) that we otherwise listed as a single indicator in other summary tables.

Table 10: Percent of hot-deck imputed data vs. total indicators assessed across Index

	Public motivation		Government policy	Educational system		Labor market		Population inclusivity	
	Pillar 1	Pillar 2	Pillar 3	Pillar 4	Pillar 5	Pillar 6	Pillar 7	Pillar 8	Pillar 9
Geography	Cyber risk awareness and motivation	Cultural proclivity towards security risk reduction	Long-term vision and commitment	Formal education	Labor upskilling	Skill demand from employer expectations	Innovation-driven demand for skills	Technological inclusivity	Educational inclusivity
Argentina	4%	2%	0%	0%	0%	0%	0%	0%	4%
Australia	0%	0%	0%	0%	0%	0%	0%	0%	6%
Austria	0%	0%	0%	0%	0%	0%	0%	0%	0%
Belgium	0%	0%	0%	0%	0%	0%	0%	0%	2%
Brazil	0%	0%	0%	0%	0%	0%	0%	0%	0%
Bulgaria	0%	0%	0%	0%	0%	0%	0%	0%	0%
Canada	0%	0%	0%	0%	0%	0%	0%	0%	2%
China	0%	2%	0%	0%	0%	0%	0%	0%	0%
Croatia	0%	0%	0%	0%	2%	0%	0%	0%	0%
Cyprus	0%	0%	0%	0%	2%	0%	0%	0%	0%
Czech Republic	0%	0%	0%	0%	0%	0%	0%	0%	0%
Denmark	0%	0%	0%	0%	0%	0%	0%	0%	0%
Estonia	0%	0%	0%	0%	4%	0%	0%	0%	0%
Finland	0%	0%	0%	0%	0%	0%	0%	0%	0%
France	0%	0%	0%	0%	0%	0%	0%	0%	2%
Germany	0%	0%	0%	0%	0%	0%	0%	0%	0%
Greece	0%	0%	0%	0%	0%	0%	0%	0%	0%
Hungary	0%	0%	0%	0%	0%	0%	0%	0%	0%
India	0%	0%	0%	0%	0%	0%	0%	0%	0%
Indonesia	0%	0%	0%	0%	0%	0%	0%	0%	0%
Ireland	0%	0%	0%	0%	0%	0%	0%	0%	2%

	Public motivation		Government policy	Educational system		Labor market		Population inclusivity	
	Pillar 1	Pillar 2	Pillar 3	Pillar 4	Pillar 5	Pillar 6	Pillar 7	Pillar 8	Pillar 9
Geography	Cyber risk awareness and motivation	Cultural proclivity towards security risk reduction	Long-term vision and commitment	Formal education	Labor upskilling	Skill demand from employer expectations	Innovation-driven demand for skills	Technological inclusivity	Educational inclusivity
Israel	4%	2%	0%	0%	0%	0%	0%	0%	0%
Italy	0%	0%	0%	0%	0%	0%	0%	0%	0%
Japan	0%	0%	0%	0%	0%	0%	0%	0%	9%
Kuwait	4%	6%	0%	0%	2%	0%	0%	0%	4%
Latvia	0%	0%	0%	0%	4%	0%	0%	0%	0%
Lithuania	0%	0%	0%	0%	2%	0%	0%	0%	0%
Mexico	0%	0%	0%	0%	0%	0%	0%	0%	0%
Netherlands	0%	0%	0%	0%	0%	0%	0%	0%	6%
New Zealand	4%	2%	0%	0%	0%	0%	0%	0%	6%
Norway	4%	2%	0%	0%	0%	0%	0%	0%	0%
Poland	0%	0%	0%	0%	0%	0%	0%	0%	0%
Portugal	0%	0%	0%	0%	0%	0%	0%	0%	2%
Qatar	4%	6%	0%	0%	0%	0%	0%	0%	4%
Romania	0%	0%	0%	0%	0%	0%	0%	0%	0%
Russia	0%	0%	2%	0%	4%	2%	0%	0%	0%
Saudi Arabia	4%	2%	0%	0%	0%	0%	0%	0%	4%
Singapore	4%	2%	0%	0%	0%	0%	0%	0%	4%
Slovakia	0%	0%	0%	2%	0%	2%	0%	0%	0%
Slovenia	0%	0%	0%	2%	0%	0%	0%	0%	4%
South Africa	0%	0%	0%	0%	0%	0%	0%	0%	0%
South Korea	0%	0%	0%	0%	0%	0%	0%	0%	4%
Spain	0%	0%	0%	0%	0%	0%	0%	0%	0%
Sweden	0%	0%	0%	0%	0%	0%	0%	0%	0%
Switzerland	4%	2%	0%	0%	0%	0%	0%	0%	0%
Turkey	0%	2%	0%	0%	0%	0%	0%	0%	0%
United Arab Emirates	4%	2%	0%	0%	0%	0%	0%	0%	4%
United Kingdom	0%	0%	0%	0%	0%	0%	0%	0%	0%
United States	0%	0%	0%	0%	0%	0%	0%	0%	2%

Table 11: Percent of hot-deck imputed data vs. total indicators assessed in respective pillar

	Public motivation		Government policy	Educational system		Labor market		Population inclusivity	
	Pillar 1	Pillar 2	Pillar 3	Pillar 4	Pillar 5	Pillar 6	Pillar 7	Pillar 8	Pillar 9
Geography	Cyber risk awareness and motivation	Cultural proclivity towards security risk reduction	Long-term vision and commitment	Formal education	Labor upskilling	Skill demand from employer expectations	Innovation-driven demand for skills	Technological inclusivity	Educational inclusivity
Argentina	40%	20%	0%	0%	0%	0%	0%	0%	25%
Australia	0%	0%	0%	0%	0%	0%	0%	0%	38%
Austria	0%	0%	0%	0%	0%	0%	0%	0%	0%
Belgium	0%	0%	0%	0%	0%	0%	0%	0%	13%
Brazil	0%	0%	0%	0%	0%	0%	0%	0%	0%
Bulgaria	0%	0%	0%	0%	0%	0%	0%	0%	0%
Canada	0%	0%	0%	0%	0%	0%	0%	0%	13%
China	0%	20%	0%	0%	0%	0%	0%	0%	0%
Croatia	0%	0%	0%	0%	25%	0%	0%	0%	0%
Cyprus	0%	0%	0%	0%	25%	0%	0%	0%	0%
Czech Republic	0%	0%	0%	0%	0%	0%	0%	0%	0%
Denmark	0%	0%	0%	0%	0%	0%	0%	0%	0%
Estonia	0%	0%	0%	0%	50%	0%	0%	0%	0%
Finland	0%	0%	0%	0%	0%	0%	0%	0%	0%
France	0%	0%	0%	0%	0%	0%	0%	0%	13%
Germany	0%	0%	0%	0%	0%	0%	0%	0%	0%
Greece	0%	0%	0%	0%	0%	0%	0%	0%	0%
Hungary	0%	0%	0%	0%	0%	0%	0%	0%	0%
India	0%	0%	0%	0%	0%	0%	0%	0%	0%
Indonesia	0%	0%	0%	0%	0%	0%	0%	0%	0%
Ireland	0%	0%	0%	0%	0%	0%	0%	0%	13%
Israel	40%	20%	0%	0%	0%	0%	0%	0%	0%
Italy	0%	0%	0%	0%	0%	0%	0%	0%	0%
Japan	0%	0%	0%	0%	0%	0%	0%	0%	63%
Kuwait	40%	60%	0%	0%	25%	0%	0%	0%	25%
Latvia	0%	0%	0%	0%	50%	0%	0%	0%	0%
Lithuania	0%	0%	0%	0%	25%	0%	0%	0%	0%
Mexico	0%	0%	0%	0%	0%	0%	0%	0%	0%
Netherlands	0%	0%	0%	0%	0%	0%	0%	0%	38%

	Public motivation		Government policy	Educational system		Labor market		Population inclusivity	
	Pillar 1	Pillar 2	Pillar 3	Pillar 4	Pillar 5	Pillar 6	Pillar 7	Pillar 8	Pillar 9
Geography	Cyber risk awareness and motivation	Cultural proclivity towards security risk reduction	Long-term vision and commitment	Formal education	Labor upskilling	Skill demand from employer expectations	Innovation-driven demand for skills	Technological inclusivity	Educational inclusivity
New Zealand	40%	20%	0%	0%	0%	0%	0%	0%	38%
Norway	40%	20%	0%	0%	0%	0%	0%	0%	0%
Poland	0%	0%	0%	0%	0%	0%	0%	0%	0%
Portugal	0%	0%	0%	0%	0%	0%	0%	0%	13%
Qatar	40%	60%	0%	0%	0%	0%	0%	0%	25%
Romania	0%	0%	0%	0%	0%	0%	0%	0%	0%
Russia	0%	0%	25%	0%	50%	33%	0%	0%	0%
Saudi Arabia	40%	20%	0%	0%	0%	0%	0%	0%	25%
Singapore	40%	20%	0%	0%	0%	0%	0%	0%	25%
Slovakia	0%	0%	0%	17%	0%	33%	0%	0%	0%
Slovenia	0%	0%	0%	17%	0%	0%	0%	0%	25%
South Africa	0%	0%	0%	0%	0%	0%	0%	0%	0%
South Korea	0%	0%	0%	0%	0%	0%	0%	0%	25%
Spain	0%	0%	0%	0%	0%	0%	0%	0%	0%
Sweden	0%	0%	0%	0%	0%	0%	0%	0%	0%
Switzerland	40%	20%	0%	0%	0%	0%	0%	0%	0%
Turkey	0%	20%	0%	0%	0%	0%	0%	0%	0%
United Arab Emirates	40%	20%	0%	0%	0%	0%	0%	0%	25%
United Kingdom	0%	0%	0%	0%	0%	0%	0%	0%	0%
United States	0%	0%	0%	0%	0%	0%	0%	0%	13%

Appendix G. Impact of alternative normalization and weighting methods on rankings

We assessed the overall Index rankings under various methodologies and compared how the rankings would perform under the same weightings but different methodologies. The results are in the table below. The initial column lists the final Index rankings per the final methodology used: that is, using the average IGC weighting applied to the distance to frontier approach and adjusted for indicator quality. The remaining columns compare how the rankings would have changed under alternative methodologies.

Table abbreviation notes: DF = Distance to frontier approach; Z-score = Z-score approach; IQA = Indicator quality adjustment

Table 12: Ranking changes under alternative normalization and weighting methodologies, better/(worse) compared to October 2020 released rankings

Alternative test conducted	Average IGC weighting (DF, IQA) – Chosen Index approach	Geography	Average IGC weighting (DF)	Average IGC weighting (Z-Score)	Average IGC weighting (Z-score, IQA)
Rankings and ranking changes – Better/(Worse)	1	Switzerland	0	0	0
	2	Singapore	0	0	0
	3	United Kingdom	0	(2)	0
	4	Australia	0	1	0
	5	Netherlands	0	1	0
	6	Canada	0	0	0
	7	Estonia	0	0	0
	8	Israel	(1)	(2)	0
	9	Ireland	(1)	1	0
	10	United States	2	1	0
	11	Germany	0	(1)	(1)
	12	Denmark	0	1	1
	13	Sweden	(1)	(2)	(1)
	14	Finland	1	0	(1)
	15	France	(2)	(3)	(2)
	16	New Zealand	1	3	3
	17	Czech Republic	(2)	(3)	1
	18	United Arab Emirates	2	2	(2)
	19	Austria	1	2	1
	20	Latvia	(1)	(1)	(1)
	21	Norway	1	2	2
	22	Poland	0	(2)	0
	23	European Union	0	0	(1)

Alternative test conducted	Average IGC weighting (DF, IQA) – Chosen Index approach	Geography	Average IGC weighting (DF)	Average IGC weighting (Z-Score)	Average IGC weighting (Z-score, IQA)
Rankings and ranking changes – Better/(Worse)	24	Qatar	0	2	1
	25	Portugal	0	0	(1)
	26	Spain	0	0	1
	27	Belgium	0	0	0
	28	Japan	0	(2)	(1)
	29	Slovakia	(1)	1	1
	30	Saudi Arabia	1	1	0
	31	Italy	0	(3)	(1)
	32	South Korea	(1)	(5)	(4)
	33	Russia	1	2	2
	34	Lithuania	(1)	(2)	(1)
	35	Slovenia	1	3	2
	36	Cyprus	0	3	2
	37	Kuwait	0	2	0
	38	Croatia	0	0	0
	39	Hungary	0	(1)	(1)
	40	Bulgaria	0	1	1
	41	Greece	0	0	0
	42	Brazil	(1)	(2)	(2)
	43	Romania	(1)	0	0
	44	Mexico	2	2	2
	45	India	(1)	0	0
	46	Indonesia	1	0	(1)
	47	Argentina	0	(1)	(1)
	48	Turkey	0	1	2
	49	China	0	0	(1)
	50	South Africa	0	0	1

Acknowledgements

PROJECT TEAM

Paul Mee
Cyber Risk Lead, Oliver Wyman Forum;
Partner, Oliver Wyman, New York

Rico Brandenburg
Cyber Risk Co-Lead, Oliver Wyman Forum;
Partner, Oliver Wyman, New York

Wenhan "John" Lin
Engagement Manager, Oliver Wyman, New York

Marisa Flignor
Senior Consultant, Oliver Wyman, Boston

Meghna Basu
Consultant, Oliver Wyman, Singapore

This publication reflects the ideas and contributions of many individuals, across interviews, workshops, events, and external publications. The project team would like to offer its gratitude to the members of the project steering committee, experts interviewed across public and private sectors, and the governance committee who graciously shared their time and insights. We would like to thank the support of those who helped with review and logistics behind the launch of this report and Index.

The diverse range of views enabled a broad spectrum of perspectives to be captured. The views expressed in this report are those of Oliver Wyman Forum and do not necessarily reflect any individual views of listed contributors.

INDEX GOVERNANCE COMMITTEE (VOTING)

Paul Mee, Committee Chair
Partner and Cyber Platform Lead, Oliver Wyman, New York

Rico Brandenburg, Committee Vice-Chair
Partner, Oliver Wyman, New York

Dr. David Farber
Distinguished Professor, Keio University;
Co-Director, Cyber Civilization Research Center, Keio University

Dr. Greg Rattray
Co-Founder, Next Peak;
Adjunct Professor, Columbia University;
Senior Advisor, Oliver Wyman, New York

Dr. Herb Lin
Senior Research Scholar, Center for International Security and Cooperation, Stanford University;
Fellow in Cyber Policy and Security, Hoover Institution, Stanford University

Dr. Ana Carla Abrão Costa
Partner and Market Leader of Oliver Wyman Latin America, Oliver Wyman, São Paulo

Chip Greene
Partner and Co-head of Oliver Wyman's Global Education Practice, Oliver Wyman, Boston

Claudia Wang
Partner, Oliver Wyman, Shanghai

INDEX GOVERNANCE COMMITTEE ADVISORS

Dustin Irwin
Senior Manager, Oliver Wyman Forum, New York

Matt Ellison
Cyber Research Associate, Hoover Institution, Stanford University

Dr. Tobias Burgers
Project Assistant Professor, Keio University

STEERING COMMITTEE

Dr. Ana Carla Abrão Costa
Partner & Market Leader of Oliver Wyman Latin America, Oliver Wyman, São Paulo

Ana Kreacic
Chief Operating Officer, Oliver Wyman Forum;
Partner, Oliver Wyman, New York

Chip Greene
Partner & Co-head of Oliver Wyman's Global Education Practice, Oliver Wyman, Boston

Claudia Wang
Partner, Oliver Wyman, Shanghai

Dr. Greg Rattray
Co-Founder, Next Peak;
Adjunct Professor, Columbia University;
Senior Advisor, Oliver Wyman, New York

Paul Mee
Partner and Cyber Platform Lead, Oliver Wyman, New York

Rico Brandenburg
Partner, Oliver Wyman, New York

Rodrigo Gouvea
Principal, Oliver Wyman, São Paulo

Wolfram Hedrich
Partner, Oliver Wyman, Singapore

ADDITIONAL METHODOLOGY REVIEW

Dr. Ugur Koyluoglu
Partner and Vice Chairman of Financial Services Americas, Oliver Wyman, New York

SPECIAL THANKS

To members of various Oliver Wyman Forum internal teams who made the launch possible with notable call outs to the individuals below.

DESIGN

Campbell Reid
Creative Head, Oliver Wyman Design, London

Neil Campbell
Art Director, Oliver Wyman Design, New York

Caroline Sun
Solutions Manager, Oliver Wyman IT, New York

Adrien Slimani
Art Director, Oliver Wyman Design, Paris

Ayo Roque
Designer, Oliver Wyman Design, Mexico City

Mike Tveskov
Designer, Oliver Wyman Design, Boston

EDITORIAL

Emily Thornton
Director, Oliver Wyman Marketing,
New York

Jilian Mincer
Managing Editor, Oliver Wyman Forum, New York

Tom Buerkle
Editor, Oliver Wyman Forum, New York

MARKETING

John Manning
Senior Marketing Manager,
Oliver Wyman Marketing, New York

Francine Minadeo
Global Head of PR,
Oliver Wyman Marketing, New York

OLIVER WYMAN FORUM –
URBAN MOBILITY READINESS INDEX

Laura Reid
Associate, Oliver Wyman, Dubai

About the Oliver Wyman Forum

The Oliver Wyman Forum is committed to bringing together business, public policy, and social enterprise leaders to help solve the world's toughest problems. The Oliver Wyman Forum strives to discover and develop innovative solutions by conducting research, convening leading thinkers, analyzing options, and inspiring action on three fronts: Reframing Industry, Business in Society, and Global Economic and Political Change. Together with our growing and diverse community of experts in business, public policy, social enterprises, and academia, we think we can make a difference. For more information, visit www.oliverwymanforum.com

References

Agrafiotis, Ioannis, Maria Bada, Paul Cornish, Sadie Creese, Michael Goldsmith, Eva Ignatuschtschenko, Taylor Roberts, and David M. Upton. 2016. "Cyber Harm: Concepts, Taxonomy and Measurement." *Said Business School WP 2016-23*. August 1. http://dx.doi.org/10.2139/ssrn.2828646.

Archer, Seth. 2019. "Markets Insider launches private-company data pages with help from Crunchbase." *Markets Insider*. April 17. https://markets.businessinsider.com/news/stocks/private-company-data-pages-on-markets-insider-from-crunchbase-2019-4-1028117732#.

Australian Government eSafety Commissioner. 2018. *Supervising preschoolers online*. July. Accessed September 9, 2020. https://www.esafety.gov.au/about-us/research/digital-parenting/supervising-preschoolers-online.

Blank, Grant, William Dutton, and Julia Lefkowitz. 2020. "OxIS 2019: Digital Divides in Britain are Narrowing but Deepening." *Oxford Internet Institute. University of Oxford*. January 19. http://dx.doi.org/10.2139/ssrn.3522083.

Bott, Ed. 2015. "Who's still using Internet Explorer? And why won't they upgrade?" *ZD Net*. December 11. https://www.zdnet.com/article/whos-still-using-internet-explorer-and-why-wont-they-upgrade/.

Committe on Information Technology Literacy, National Research Council. 1999. *Being Fluent with Information Technology*. Washington, D.C.: National Academy Press. http://www.nap.edu/catalog/6482.html.

Dutton, William, Sadie Creese, Ruth Shillair, Maria Bada, and Taylor Roberts. 2017. "Cyber Security Capacity: Does it Matter?" *Quello Center Working Paper No. 2938078*. March 20. http://dx.doi.org/10.2139/ssrn.2938078.

2020. "Edelman Trust Barometer." *Edelman*. https://www.edelman.com/trustbarometer.

ETS. 2019. "A Snapshot of the Individuals Who Took the GRE General Test JULY 2013–JUNE 2018." *GRE*. https://www.ets.org/s/gre/pdf/snapshot_test_taker_data_2018.pdf.

Evangelho, Jason. 2018. "Why You Should Ditch Google Search And Use DuckDuckGo." *Forbes*. October 3. https://www.forbes.com/sites/jasonevangelho/2018/10/03/when-does-googles-convenience-turn-creepy-let-me-duckduckgo-that-for-you/#226ca29d235e.

Fahs, Ginny, Anil Dewan, Steven Buccini, and Ora Tanner. 2019. "Protecting Older Users Online." *Aspen Institute*. https://www.aspentechpolicyhub.org/project/protecting-older-users-online/.

Fiserv. 2019. *Cybersecurity Awareness Insights Study*. https://www.firstdata.com/images/fd-facelift/images/FDC_Cybersecurity_and_Awareness_eBook.pdf.

Gartner Research. 2018. *Forecast Analysis: Information Security, Worldwide, 2Q18 Update*. Septermber 14. https://www.gartner.com/en/documents/3889055.

2020. "Global Cyber Education: An Assessment of National Primary and Secondary Curricula." *Oliver Wyman Forum*.

2018. "Global Cybersecurity Index." *International Telecommunication Union*. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

2019. "Global Law and Order Report." *Gallup*. https://www.gallup.com/analytics/267896/2019-global-law-order-report.aspx?utm_source=Law_and_Order_Nurture_Campaign&utm_medium=email&utm_campaign=Law_and_Order_Nuture_Campaign_Email_8&utm_content=Download_Report_CTA_1&elqTrackId=df4c49d9102a47e4b7ec1779a7.

2020. "Global Skills Index." *Coursera*. https://www.coursera.org/gsi.

2020. "Governmental Commitments to Cyber Literacy and Education: A Comparison of National Cybersecurity Strategies." *Oliver Wyman Forum*.

Hoffman, Chris. 2020. "How-To Geek." June 4. https://www.howtogeek.com/659857/what-you-need-to-know-about-the-new-microsoft-edge-browser/.

IBM. 2014. "IBM Security Services 2014 Cyber Security Intelligence Index." May. https://i.crn.com/sites/default/files/ckfinderimages/userfiles/images/crn/custom/IBMSecurityServices2014.PDF.

2019. "Insight Report: Regional Risk for Doing Business." *World Economic Forum*. http://www3.weforum.org/docs/WEF_Regional_Risks_Doing_Business_report_2019.pdf.

Institute, DQ. 2019. "DQ Global Standards Report 2019." https://www.dropbox.com/s/a6grb11ultqdzad/DQGlobalStandardsReport2019.pdf?dl=0.

Jacobs, Harrison. 2018. "One photo shows that China is already in a cashless future." *Business Insider*. May 29. https://www.businessinsider.com/alipay-wechat-pay-china-mobile-payments-street-vendors-musicians-2018-5.

Julie Inman Grant (eSafety Commissioner, Australian Government). 2020. "Feedback for Oliver Wyman on the Future of Cyber Risk Literacy and Education."

Kaspersky Labs. 2015. "Are You Cyber Savvy?" https://media.kasperskycontenthub.com/wp-

content/uploads/sites/45/2018/03/08234157/Cyber_savvy_quiz_report.pdf.

Keizer, Gregg. 2014. "Microsoft nixes EU browser ballot screen." *Computerworld*. December 18. https://www.computerworld.com/article/2860886/microsoft-nixes-eu-browser-ballot-screen.html.

Legatum Institute. 2019. "Methodology." *Legatum Prosperity Index*. https://prosperitysite.s3-accelerate.amazonaws.com/7515/8634/9002/Methodology_for_Legatum_Prosperity_Index_2019.pdf.

Lessenski, Marin. 2019. "Findings of the Media Literacy Index 2019." *Open Society Institute Sofia*. November. https://osis.bg/wp-content/uploads/2019/11/MediaLiteracyIndex2019_-ENG.pdf.

Lunden, Ingrid. 2017. "Russia says 'nyet,' continues LinkedIn block after it refuses to store data in Russia." *Tech Crunch*, March 7. https://techcrunch.com/2017/03/07/russia-says-nyet-continues-linkedin-block-after-it-refuses-to-store-data-in-russia/.

Madnick, Stuart. 2018. "How Companies Can Create a Cybersafe Culture at Work." *The Wall Street Journal*, May 29. https://www.wsj.com/articles/how-companies-can-create-a-cybersafe-culture-at-work-152764.

Makridis, Christos Andreas, and Max Smeets. 2018. "Determinants of Cyber Readiness." doi:http://dx.doi.org/10.2139/ssrn.3216231.

Marsh Microsoft. 2019. "Marsh Microsoft Global Cyber Risk Perception Survey." https://www.microsoft.com/security/blog/wp-content/uploads/2019/09/Marsh-Microsoft-2019-Global-Cyber-Risk-Perception-Survey.pdf.

Microsoft 365 Blog. 2020. *Microsoft 365 apps say farewell to Internet Explorer 11 and Windows 10 sunsets Microsoft Edge Legacy*. August 17. https://techcommunity.microsoft.com/t5/microsoft-365-blog/microsoft-365-apps-say-farewell-to-internet-explorer-11-and/ba-p/1591666.

Microsoft News Center India. 2020. "Malware, ransomware and drive-by download attacks pose biggest cyberthreat challenge in India: Microsoft Security Endpoint Threat Report 2019." *Microsoft*. July 29. https://news.microsoft.com/en-in/microsoft-security-endpoint-threat-report-2019-india/.

Microsoft Support. 2020. *Use Internet Explorer in Windows 10*. June 6. https://support.microsoft.com/en-us/help/4026136/windows-10-use-internet-explorer#:~:text=Internet%20Explorer%2011%20is%20a,enter%20Internet%20Explorer%20in%20Search%20.

Ministry of Commerce People's Republic of China. 1986. "Compulsory Education Law." April 12. http://english.mofcom.gov.cn/aarticle/lawsdata/chineselaw/200211/20021100050302.html.

Nasu, Hitoshi, and Helen Trezise. 2015. "Cyber Security in the Asia-Pacific." *ANU College of Law Research Paper 2015* (Series 2). https://ssrn.com/abstract=2700388.

National Cyber Security Authority of Israel. 2017. "Cyber Defense Methodology for an Organization." https://www.gov.il/BlobFolder/policy/cyber_security_methodology_for_organizations/he/Cyber1.0_english_617_A4.pdf.

2020. "National Cyber Security Index." *e-Governance Academy*. https://ncsi.ega.ee/methodology/.

2019. "Network Readiness Index." *Portulans Institute*. https://networkreadinessindex.org/.

OECD. 2008. "Handbook on constructing composite indicators: Methodology and user guide." *OECD*. https://www.oecd.org/sdd/42495745.pdf.

Pan, Yuanyuan, Sophie Vayssettes, and Elizabeth Fordham. 2016. "Education in China: A Snapshot." *OECD*. https://www.oecd.org/china/Education-in-China-a-snapshot.pdf.

Pena, Juan, and Luis A. Garcia-Segura. 2014. "The Critical Role of Education in Every Cyber Defense Strategy." *Northern Kentucky Law Review* 41 (3).

2016. "Policy Review: Building Digital Citizenship in Asia-Pacific through Safe, Effective and Responsible Use of ICT." *UNESCO Bangkok: Asia and Pacific Regional Bureau for Education*. https://bangkok.unesco.org/content/policy-review-building-digital-citizenship-asia-pacific-through-safe-effective-and.

Rains, Tim. 2014. "Which Countries/Regions Encountered the Most Malware in 2013?" *Microsoft*. May 21. https://www.microsoft.com/security/blog/2014/05/21/which-countriesregions-encountered-the-most-malware-in-2013/.

Ritchie, Hannah. 2019. "Gender Ratio." *OurWorldInData.org*. https://ourworldindata.org/gender-ratio.

2019. "Scores bolster case for Shanghai math in British schools." *The Star*. December 10. https://www.thestar.com.my/news/regional/2019/12/10/scores-bolster-case-for-shanghai-math-in-british-schools.

Shackelford, Scott, and Amanda Craig. 2014. "Beyond the New 'Digital Divide': Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cybersecurity." *Stanford Journal of International Law* 50 (Winter): 119-185. https://ssrn.com/abstract=2446666.

Shen, Xinmei. 2020. "WeChat users renting out accounts for quick bucks could wind up as criminal accomplices." *Abacus*. August 5.

https://www.scmp.com/abacus/tech/article/3095994/wechat-users-renting-out-accounts-quick-bucks-could-wind-criminal.

Shillair, Ruth, and William Dutton. 2016. "Supporting a Cybersecurity Mindset: Getting Internet Users into the Cat and Mouse Game." March 30. http://dx.doi.org/10.2139/ssrn.2756736.

Solt, Fredeck. 2020. *Harvard Dataverse*. https://dataverse.harvard.edu/dataset.xhtml?persistentId=doi:10.7910/DVN/LM4OWF.

Sowers, Rob. 2020. "64% of Americans Don't Know What to Do After a Data Breach -- Do You? (Survey)." *Varonis*. March 29. https://www.varonis.com/blog/data-breach-literacy-survey/.

Schwab, Klaus, ed. 2019. "The Global Competitiveness Report." *World Economic Forum*. http://www3.weforum.org/docs/WEF_TheGlobalCompetitivenessReport2019.pdf.

Turner, Camilla. 2019. "Britain jumps up international maths rankings following Chinese-style teaching." *The Telegraph*, December 2019. https://www.telegraph.co.uk/news/2019/12/03/britain-jumps-international-maths-rankings-following-chinese/.

UN Department of Economic and Social Affairs. 2019. *World Population Prospects*. Accessed July 2020. https://population.un.org/wpp/Download/Standard/Population/.

UNESCO. 2018. "A Global Framework of Reference on Digital Literacy Skills for Indicator 4.4.2." http://uis.unesco.org/sites/default/files/documents/ip51-global-framework-reference-digital-literacy-skills-2018-en.pdf.

Varonis. 2020. *64% of Americans Don't Know What to Do After a Data Breach — Do You?* March 3. https://www.varonis.com/blog/data-breach-literacy-survey/.

Warren, Tom. 2019. "Microsoft really doesn't want you to use Internet Explorer anymore." *The Verge*. February 8. https://www.theverge.com/2019/2/8/18216767/microsoft-internet-explorer-warning-compatibility-solution.

Windows IT Pro Blog. 2019. *The perils of using Internet Explorer as your default browser*. June 2. https://techcommunity.microsoft.com/t5/windows-it-pro-blog/the-perils-of-using-internet-explorer-as-your-default-browser/ba-p/331732.

Yip, Wai Yee. 2020. "Need to close digital divide widened by Covid-19: NMP." *The Straits Times*, May 27. https://www.straitstimes.com/singapore/need-to-close-digital-divide-widened-by-covid-19-nmp.

Zhu, Tingting Juni, Alan Fritzler, and Jan Orlowski. 2018. "Data Insights: Jobs, Skills and Migration Trends Methodology and Validation Results." *World Bank Group and LinkedIn*. November. https://development-data-hub-s3-public.s3.amazonaws.com/ddhfiles/144635/wbg-linkedin-methodology-report_1.pdf.