2020

White paper series
Edition 9

CYBERSECURITY EDUCATION

Planning for the Future Through Workforce Development

OAS More rights for more people | aws

CYBERSECURITY **EDUCATION**

Planning for the Future Through Workforce Development

Prepared and published by the Cybersecurity Program of the Inter-American Committee against Terrorism (cybersecurity@oas.org).

The contents expressed in this document are presented exclusively for informational purposes and do not represent the official opinion or position of the Organization of American States, its General Secretariat or its Member States.

CREDITS

Luis Almagro
Secretary General
Organization of American States (OAS)

OAS Technical Team
Farah Diva Urrutia
Alison August Treppel
Belisario Contreras
Kerry-Ann Barrett
Gabriela Montes de Oca Fehr
Babara Marchiori de Assis
Rolando Ramirez

AWS Technical Team
Abby Daniell
Melanie Kaplan
Jordana Siegel

CYBERSECURITY
EDUCATION
Planning for the Future
Through Workforce Development

CONTENT

CYBERSECURITY EDUCATION

Planning for the Future
Through Workforce Development

What does this paper set out to do?

As the number of malicious activities in cyberspace continues to rise, the need for a workforce trained in cybersecurity is a necessity. The indispensable skills for such a workforce include the ability to optimally design and operate applications and systems with the capacity to identify and respond to cyber threats, as well as to design effective public policies to counter those threats. The future challenges of the cybersecurity workforce can only be addressed by encouraging careers in cybersecurity. The disparity between the supply of skilled cybersecurity professionals and the demand for them requires immediate action to train current practitioners while crafting policies to educate the next generation of cybersecurity professionals. Without policies to enhance the workforce's cybersecurity skills, a country will not fully reap the benefits of the digital economy. This paper outlines steps to build a Cybersecurity Education Action Plan (CEAP) that includes mechanisms to integrate cybersecurity education into policy development and school curricula to address the shortage of cybersecurity skills in Latin America and the Caribbean. It also offers a toolkit of initiatives and mechanisms at the national level to generate interest in cybersecurity careers.

CYBERSECURITY EDUCATION

Planning for the Future Through Workforce Development

Why is Education in Cybersecurity Important in Latin America?

The “Fourth Industrial Revolution” is powered by the world’s deeper interconnectivity (Schwab, 2016, p. 3). Latin America has been a fast adopter of digital services enabled by cloud computing, mobile devices, and broadband networks, allowing a deeper transformation of governments and businesses, including the incorporation of data processing for integrated and effective decision-making by policymakers. Despite the adoption of these technologies in Latin America, the new landscape has also transformed the nature and operations of crime. In Latin America and the Caribbean, the cost of cybercrime was estimated at between US$15 billion and US$30 billion in 2017: that is, between 0.28% and 0.57% of the region’s GDP (Lewis, 2018, p. 7). Countries in the region are not only a target of online attacks, but also an active source of them (Lewis, 2018, p. 20). The increase in cyber risks requires businesses and governments to embed cybersecurity into the fabric of their processes, technology acquisition, and personnel selection.

Despite these threats, there continues to be a global shortage of cybersecurity professionals, with the estimated shortfall amounting to some 4.07 million people. In the Latin American region alone, the cybersecurity workforce gap is roughly 600,000 people ((ISC)^2, 2019, p. 8). This figure represents a significant increase compared to 2018, when the shortage was estimated at around 136,000 professionals ((ISC)^2, 2018, p. 4). Both mid-sized and large companies have high demand for cybersecurity professionals, which requires a workforce prepared to design, build, and operate the latest technologies, primarily at the technical level (World Economic Forum ¬– WEF, 2015, p. 20).

CYBERSECURITY EDUCATION

Planning for the Future Through Workforce Development

Cybersecurity Education

In Latin America and the Caribbean, the gap in cybersecurity workforce demand has increased, especially in mid-sized companies ((ISC)2, 2019). According to the 2019 report by (ISC)2, "Cybersecurity professionals are likely to have at least a bachelor's degree—with a little more than one-third holding a master's or doctoral/post-doctoral degree. While most in the field get their degrees in computer and information sciences (40%), others get degrees that are not IT-focused, such as engineering (19%) and business (10%)." More specifically for the region, the report indicates that organizations are more likely to recruit from educational institutions and security vendors. The reality is that a vast majority of cybersecurity professionals did not start out in cybersecurity, but followed another career path, and many even started in non-IT fields. Policymakers must adopt a national approach to cybersecurity education to build a pipeline of cybersecurity professionals and think strategically about how to position cybersecurity education in the national cybersecurity framework.

The Education Pillar

Numerous tools have been created to help assess the state of a country's cybersecurity capacity. Two examples are the Cybersecurity Capacity Maturity Model for Nations (CMM) and the Global Cybersecurity Index. These tools emphasize the importance of cybersecurity education in a nation's cybersecurity capacity and include cybersecurity education as a key pillar in the national strategy.

The CMM, created by the Global Cyber Security Capacity Centre (GCSCC),[1] is a metric that assesses the national state of cybersecurity capacities in a country. The CMM includes a section dedicated to Cybersecurity Education, Training and Skills that highlights cybersecurity education as a key pillar for policymakers to consider in evaluating cybersecurity capacity through the ability, quality, and uptake of educational and training offerings for various groups, including government representatives, private sector, and the population as a whole (Cybersecurity Capacity Portal, 2020). This section is further divided into three main components: (1) awareness-raising for citizens, (2) framework for education, and (3) framework for professional training. While the first focuses on the existence of awareness-raising campaigns for a general audience, the second refers to accredited programs at the university level, research and development (R&D) initiatives, and a national cybersecurity curriculum. The third component then highlights the importance of cybersecurity certifications and training programs to support skill development over time.

[1] https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cybersecurity-capacity-maturity-model-nations-cmm-0

Likewise, the Global Cybersecurity Index 2018 (CGI), created by the International Telecommunication Union (ITU),[2] underscores the importance of combining different approaches, techniques, and tools to close the cybersecurity educational gap. Like the CMM, the CGI has similar indicators in the "Capacity Building" pillar, which include "public awareness campaigns, the framework for the certification and accreditation of cybersecurity professionals; professional training courses in cybersecurity, educational programs or academic curriculum in cybersecurity; investment in cybersecurity R&D programs, incentive mechanisms, and home-grown cybersecurity industry" (ITU, 2019, p. 8). Both models also highlight the importance of educational programs, which can influence social change and economic growth.

These cybersecurity maturity models and indexes demonstrate that education should also feature prominently in a country's national cybersecurity strategy. In Latin America, the governments of Argentina, Brazil, Chile, Colombia, Costa Rica, the Dominican Republic, Guatemala, Mexico, Panama, and Paraguay have all published or updated their national cybersecurity strategies. These strategies encompass a capacity-building framework and lines of action to strengthen cybersecurity education at the national level. For instance, the two first goals of Argentina's national strategy focus on cybersecurity awareness and education.[3] Four of the seven objectives of Brazil's National Information Security Policy relate to R&D, workforce capacity building, skill development, and an information security culture.[4] Similarly, the scope of the national cybersecurity frameworks of Chile and Colombia include education as a key feature to improve cybersecurity maturity, and they also identify specific actions to be carried out, setting a timeframe and determining the actors in charge of those tasks. Cybersecurity Education Action Plans can strengthen and guide cybersecurity policies in order to address the shortcomings of individual workforces and educational systems.

As this paper was being finalized, COVID-19 became a global pandemic and changed education globally. Federal, state, and provincial education ministries and departments moved quickly to migrate their education content to the cloud to ensure millions of students and educators uninterrupted access to distance learning. Public and private universities, colleges, and K-12 schools did the same. Distance learning became more and more prevalent and, with that, so did the need to address cybersecurity issues in connectivity to enable learning. Online training exercises and support mechanisms for teachers and students on cybersecurity education are now more of a priority in the adaptation to virtual learning.

[2] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

[3] Argentina (2019). Estrategia Nacional de Ciberseguridad. Retrieved from
http://www.enre.gov.ar/web/bibliotd.nsf/203df3042bad9c40032578f6004ed613/1e2bd1ba24f72e9b03258408003abee3/$FILE/anexo%201.pdf.

[4] Brazil (2018). Política Nacional de Segurança da Informação. Retrieved from
http://www.planalto.gov.br/CCIVIL_03/_Ato2015-2018/2018/Decreto/D9637.htm.

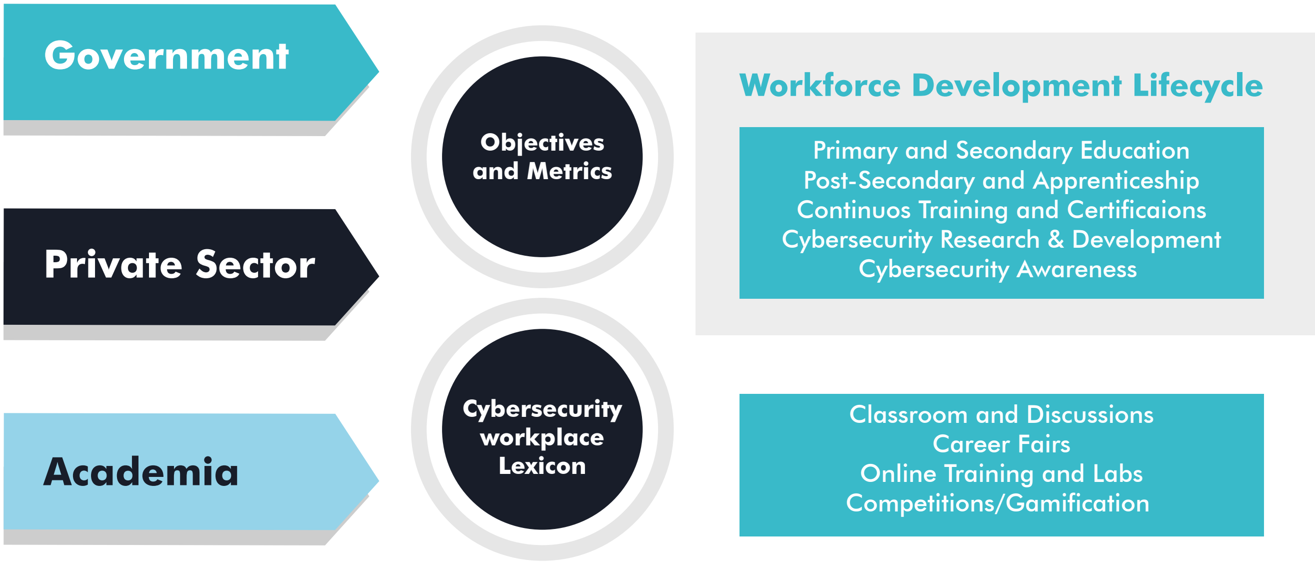
Building a Cybersecurity Education Action Plan

The Cybersecurity Education Action Plan (CEAP) is a blueprint for policymakers to design effective public policies intended to strengthen their national cybersecurity strategies and develop the cybersecurity workforce.

The diagram below demonstrates how a CEAP integrates with the national cybersecurity strategy's overarching goals as a specific action line to address the education pillar.

National Cybersecurity Strategy

Cybersecurity Education Action Plan



Government

Private Sector

Academia

Objectives and Metrics

Cybersecurity workplace Lexicon

Workforce Development Lifecycle

Primary and Secondary Education
Post-Secondary and Apprenticeship
Continuos Training and Certificaions
Cybersecurity Research & Development
Cybersecurity Awareness

Classroom and Discussions
Career Fairs
Online Training and Labs
Competitions/Gamification

The development of a CEAP should consider:

1. Establishing goals.

2. Integrating stakeholders into the CEAP.

3. Establishing objectives and metrics.

4. Creating a CEAP implementation plan.

5. Identifying the resources needed for CEAP implementation.

The National Initiative for Cybersecurity Education (NICE),[5] led by the National Institute of Standards and Technology (NIST) in the United States, is one example of a policy initiative that policymakers can emulate to develop a CEAP. NICE operates as a partnership between the government, the private sector, and civil society to address the workforce shortage by enhancing the country's ability to tackle current and future cybersecurity challenges. Considering cybersecurity's multidisciplinary nature and key recommendations received from academic, private, and government stakeholders, the NICE Framework clearly defines the roles and functions of stakeholders in the enhancement of cybersecurity capacities in the United States (NIST, 2017, pp. 1-2). As of August 2020, NIST is in the midst of a public consultation to update the NICE framework and expects to release the latest version in November 2020.[6]

NIST, through the NICE Framework, provides policymakers with examples about the importance of tailoring cybersecurity activities to each stage of the workforce development cycle. The framework can be used as a guide for organizations to develop cybersecurity training and educational programs that can be tailored by each country. Globally, NICE is the sole framework which seeks to standardize the roles required in the cybersecurity workforce, encompassing both technical and non-technical roles. Countries such as Australia, Singapore, and Japan have used NICE as a foundation for the creation of their own frameworks and have disseminated it across their public, private, and academic sectors. At present, no country in Latin America and the Caribbean has formally adopted the NICE framework.

The following sections describe the five critical steps for the creation of a CEAP following the NICE framework. The first section, ***Establishing Goals***, lays out specific goals that will define the long-term outcomes of the action plan. The second section, ***Integrating Stakeholders into the Cybersecurity Education Action Plan***, describes the importance of properly identifying the actors that will partake in the design and implementation of the action plan. The third section, ***Establishing Objectives and Metrics***, outlines the importance of selecting objectives that are both measurable and that are applicable to the context in which the action plan is to be applied. The fourth section, ***Implementing a Cybersecurity Education Plan***, identifies detailed actions that can be incorporated into each stage of education and the workforce development cycle. Lastly, the ***Actionable Recommendations*** section includes a comprehensive list of actionable recommendations to make the cybersecurity education plan a reality.

[5] See Annex for additional details.

[6] https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/nice-framework-draft-revision

Establishing Goals

At the initial stages of CEAP design, policymakers must select a limited number of goals and consider the country's social and economic context to structure a successful action plan. By selecting a few relevant and attainable goals, policymakers can better define the CEAP.

To be effective a CEAP should focus on: (a) addressing the shortage of cybersecurity education and skills, and (b) raising awareness about gaps in cybersecurity and about the importance of the field. As an example, the NICE framework outlines three goals to address the shortage of cybersecurity education and skills. These are non-exclusive although they are comprehensive and thorough, and they can be of use when they are adapted to the specific goals that the policymakers are seeking to achieve.

1. Accelerate learning and skill development: Describes the importance of creating awareness about the need for cybersecurity education among public and private actors. Specifically, it recommends the engagement of displaced workers who might be available to perform cybersecurity roles, as well as experimenting with the use of cooperative education programs where individuals can become part of the workforce and earn a salary while still learning the necessary skills.

2. Nurture a diverse learning community: Seeks to ensure that cybersecurity education emphasizes ongoing learning, remains measurable, and incorporates diversity. To promote diversity, NICE recommends actively encouraging members of under-represented minorities to take advantage of cybersecurity learning opportunities. This goal also encourages the private and public sectors to inspire cybersecurity career awareness, starting at the elementary school level, to facilitate the development of academic pathways.

3. Guide career development and workforce planning: Specifies the need to support employers in recruiting, retaining, and continually developing their workforce. It advocates measures such as assisting human resource professionals in developing tools to assist managers, and analyzing data sources to achieve targeted recruiting.

Policymakers should take into consideration the views of those directly and indirectly involved in the creation and implementation of the CEAP. By involving stakeholders in this process, policymakers can reinforce the effectiveness of the strategy and achieve the goals set. The following section offers an overview on how to better identify and engage stakeholders.

Integrating Stakeholders into the Cybersecurity Education Action Plan

Multi-stakeholder collaboration is essential during the formulation and implementation of a CEAP. During the formulation phase, the partnership between the government, private sector, and civil society helps assess the current workforce needs and identify relevant initiatives already in place in primary to post-secondary education.

Latin American and Caribbean governments could start by mapping key stakeholders from industry, academia, and civil society and inviting them to participate in the CEAP formulation process. To this end, it is essential to clearly communicate the following to the stakeholders: (1) the goals and scope of the national Cybersecurity Education Action Plan, (2) the timeframe, milestones, and deliverables of the formulation process, and (3) the decision-making mechanisms of the formulation process (e.g., how the action plan will be approved and how comments and inputs from different stakeholders will be considered, analyzed, and ultimately incorporated into it). Policymakers could engage stakeholders by creating committees, hosting workshops, and issuing public consultations, among other mechanisms. Countries that developed their National Cybersecurity Strategies through multi-stakeholder processes could apply that experience to the formulation of their CEAPs as well.[7]

Furthermore, to implement a national Cybersecurity Education Action Plan, policymakers should consider creating a committee or commission of government agencies to coordinate the implementation of educational policies, as well as working groups open to contributions and recommendations from various sectors. The NICE case offers a good example of coordination mechanisms including the NICE Interagency Coordinating Council (ICC) and the Working Group. While the former comprises the government agencies leading the implementation of the action plan, the latter aims to bring together representatives of different sectors. Both structures should be considered when implementing a national CEAP. It is noteworthy that many countries in Latin America and the Caribbean have developed a similar model for the implementation of their national cybersecurity strategies,[8] adopting a committee or commission composed of government agencies, as well as working groups that co-opt other sectors' representatives to participate voluntarily. This governance model could be replicated to support the national CEAP.

Private Sector

The private sector is a critical stakeholder and partner in implementing the national CEAP. With a leading role in driving technology development, the private sector is aware of industry needs and can also provide tools to train the workforce, as well as resources to improve the delivery of educational offerings.

[7] Documents that describe how the multi-stakeholder approach could be employed in the development of national cybersecurity strategies are a good start when formulating a national cybersecurity education framework. (See Global Partners Digital reports, such as "Framework for Multistakeholder Cyber Policy Development" and "Multistakeholder Approaches to National Cybersecurity Strategy Development.")

[8] For example, Chile has created the Cybersecurity Inter-Ministerial Committee, comprising various government agencies. The Committee can invite representatives of academia, civil society, and the private sector to participate in its sessions. Likewise, Paraguay has created a National Cybersecurity Commission with government members, and multi-stakeholder groups can be created to define specific topics.

In addition to governance structures, public-private-academic partnerships also play an important role in a CEAP. Public and private education institutions can leverage expertise from the private sector, including technology companies, to enhance content, efficiency, and ensure overall sustainability for cybersecurity education. Facilitating these partnerships can provide easier access to resources and opportunities and make them accessible to a greater number of students.

For example, Amazon Web Services (AWS)'s Educate Cloud Degree initiative helps "cloudify" the existing curricula of participating institutions, conferring degrees and credentials with a specialization or concentration in Cloud Computing. In Brazil and Colombia, both the National Service for Industrial Training (SENAI)[9] and the National Training Service (SENA)[10] have partnered with AWS to train students in artificial intelligence, the Internet of Things (IoT), and cloud computing, which includes tools and modules on cybersecurity. Through this partnership, SENAI and SENA trained 3,000 and 10,000 students in 2019, respectively. Similarly, the Government of Argentina has also partnered with AWS, offering its citizens the AWS Educate program on the Ministry of Modernization's portal in conjunction with a cloud computing curriculum with cybersecurity modules through AWS Educate to 28 educational institutions in the country.[11]

Similarly, CISCO and Trend Micro also provide resources to assist post-secondary students and institutions. The CISCO Networking Academy, for example, provides online and in-person learning on many tech topics, including cybersecurity, which is also available in Portuguese and Spanish.[12] Trend Micro, through the program "Cybersecurity Education for Universities,"[13] works with universities on training educators, aligning the cybersecurity curriculum, and providing technical seminars and webinars to students and faculty.

Academia

Through universities, think tanks, and other academic institutions, academia typically hosts multiple experts who, through their research, continue to advance the field of cybersecurity. The integration of academics into public-private-academic partnerships can provide objective, scientific, and peer-reviewed analysis for policy development. Academia can often be the source of innovation and advancement in technologies.

The University of Oxford, through the Global Cyber Security Capacity Centre (GCSCC), has established itself as a leading international research center on cybersecurity, promoting scale, pace, quality, and impact of cybersecurity. The university and the GSCC have partnered with organizations such as the OAS and the Inter-American Development Bank to provide models for an objective assessment on the state of cybersecurity in the region. The first of these partnerships took place in 2016 with the publication Cybersecurity: Are we ready in Latin America and the Caribbean? (2016).[14] This publication has allowed policymakers and private sector stakeholders to identify the progress in cybersecurity that each country has achieved, in addition to highlighting key areas of engagement and support needed to attain a higher level of maturity.

[9] https://noticias.portaldaindustria.com.br/noticias/educacao/senai-e-amazon-web-services-se-unem-para-incentivar-a-educacao-no-brasil/

[10] https://aws.amazon.com/blogs/publicsector/president-of-colombia-joins-aws-in-bogota-talks-innovation-across-the-region/

[11] https://aws.amazon.com/es/blogs/aws-spanish/aws-announces-amazon-cloudfront-edge-location-in-argentina/

[12] https://www.netacad.com/

[13] https://www.trendmicro.com/en_us/initiative-education/cybersecurity-education-universities.html

[14] https://publications.iadb.org/en/cybersecurity-are-we-ready-latin-america-and-caribbean

Integrating the academic sector should incentivize policymakers to use the advice and data available to construct effective policies that can assure the integration of cybersecurity principles into education. Most importantly, these are primary entities that must be financially supported to continue with their work in innovating and advancing the work of cybersecurity and education.

Civil Society

Civil society and many information security associations (e.g., (ISC)2, CompTIA, ISACA, and SANS) have developed cybersecurity education programs that can assist governments in leveraging cybersecurity skills across different institutions and regions of the country. Furthermore, in projects geared towards improving youth education and employability, public-private partnerships tend to be neutral and of defined durations and they often engage with civil society (IDB, 2018, p. 4). Non-profits assist governments and private actors in the monitoring and accountability of these projects and ensuring that the objectives are met. In addition, "NGOs, communities and academic institutions also necessarily fit into this equation by contributing their own comparative advantage, voice and positioning" (WEF, 2014, p. 11). Additionally, in Latin America organizations are more likely to recruit cybersecurity professionals from academic institutions ((ISC)2, 2019, p. 27), which highlights the importance of public-private-civil society partnerships in enhancing the skills and knowledge of the region's cybersecurity professionals.

All stakeholders should take part in supporting the development of a skilled cybersecurity workforce, as those different actors play unique roles at different instances of the educational cycle. The following sections provide some examples through which both the public and the private sector, as well as civil society, can participate in advancing the understanding of cybersecurity and educate the workforce needed to bridge the gap.

Establishing Objectives and Metrics

Having measurable objectives and appropriate metrics to continually evaluate progress and provide feedback for their improvement directly assists in the delivery of effective and targeted CEAPs. For them to function correctly, however, objectives should be SMART: specific, measurable, accurate, reliable, and timely.

Governments could also consider using input indicators (i.e., related to the resources needed, such as teacher training and classroom pedagogy), outcome indicators (i.e., referring to the impact of the activity undertaken, e.g. student knowledge and skills), national educational and socio-economic indicators, such as educational enrollment rates and cost indicators (i.e., comparison of an initiative's outcomes with its costs through a cost-benefit analysis, for example) (Wagner et al., 2005, pp. 21-30).

Policymakers could also consider adapting Information and Communications Technology (ICT) indicators to measure the impact of cybersecurity education. For instance, the "Partnership on Measuring ICT for Development"[15] of the International Telecommunication Union consists of a list of indicators agreed upon through a multi-stakeholder consultation process and includes a number of indicators for ICT in education that could be adjusted and then used to assess the overall implementation of the CEAP at the national level. Some national indicators include, as examples:

- Proportion of primary and secondary schools with cybersecurity educational programs.
- Proportion of post-secondary students enrolled in cybersecurity-related courses.
- Proportion of cybersecurity-qualified educators in schools.[16]

Governments and other stakeholders should consider not only relying on traditional tools—such as dedicated surveys—to measure impact, but should also explore other data sources (OECD, 2019, p. 18). For instance, thanks to technological advancement, policymakers can combine different sources of data, identify correlations, and even conduct predictive analyses.

[15] https://www.itu.int/en/ITU-D/Statistics/Pages/intlcoop/partnership/default.aspx

[16] Indicators prepared based on the core list of ICT indicators of the Partnership on Measuring ICT for Development, available at https://www.itu.int/en/ITU-D/Statistics/Pages/coreindicators/default.aspx.

Implementing a Cybersecurity Education Plan

This section provides information on critical aspects to be considered in the implementation of a CEAP in each phase of the workforce development lifecycle, as well as best practices that have been considered around the globe.

Primary and Secondary Education – Educating the Next Generation

The NICE Strategic Plan is a good example of how to outline a primary to secondary education plan. The "National K-12 Cybersecurity Education Implementation Plan"[17] aims to: (1) encourage students to engage in cybersecurity-related activities, (2) assist educators in incorporating cybersecurity concepts into classes, and finally, (3) help students from primary and secondary education identify career opportunities in the cybersecurity field. Additionally, this K-12 Cybersecurity Education Implementation Plan also fosters community engagement in establishing a cybersecurity career awareness campaign, targeting "educators, students, parents, administrators, and counselors." These goals are an excellent example of what governments could aim for when educating the next generation of cybersecurity professionals.

To help students at the K-12 level, the National Integrated Cyber Education Research Center (NICERC)[18] in the United States offers free curricula for educators to integrate cybersecurity concepts into classroom instruction as well as professional development opportunities for teachers.

To educate the next generation workforce, policymakers should consider creating a specific action plan with activities for educators and students. For educators, training should provide resources and innovative tools that teachers could add to their classes to capture students' attention. For primary and secondary students, it is essential to consider safety concerns, potential career paths, and how to leverage games and competitions. Governments should also consider partnering with the private sector, non-profits, and universities when formulating and implementing educational initiatives. Many tools could be used to educate children on cybersecurity, ranging from adapting curricula—or developing new ones—to competitions offered by the private sector.

Case Study

AWS has partnered with Code.org, a non-profit organization dedicated to expanding computer science access in schools and increasing participation by women and under-represented minorities. Powered by AWS, Code.org's vision is for every student in every school to have the opportunity to learn computer science, just like biology, chemistry, or algebra. Specifically, AWS supports Code.org's website throughout the year by enhancing its ability to scale to handle millions of teachers and students in over 180 countries during Hour of Code, an annual campaign that engages 15% of students worldwide in one-hour-long introductory coding activities. Additionally, Code.org protects millions of student records and guards against cyber-attacks using AWS Infrastructure Event Management, AWS Shield Advanced, AWS WAF – Web Application Firewall, and AWS GuardDuty. Over the past three years, thousands of Amazon employees have volunteered during Hour of Code in local classrooms from San Miguel, Chile, to Cape Town, South Africa, and in 2019, Amazon employees led 280 events across more than 20 countries and 160 cities.

[17] https://www.nist.gov/sites/default/files/documents/2017/04/26/nice_k12_implementation_plan.pdf

[18] https://nicerc.org/student/

Post-Secondary and Apprenticeship

During this phase of their schooling, students often take the first major step towards a career in cybersecurity. At the post-secondary level, cybersecurity education could be included both for students pursuing technical jobs and those seeking careers in non-technical fields, such as law, public policy, business, defense, and the military. Many of today's cybersecurity professionals have a non-IT background, with 30% of them coming from fields such as business, marketing, finance, accounting, and the military. In Latin America, 18% of cybersecurity professionals began in non-technical careers ((ICS)2, 2017, p. 5).

Many computer sciences and engineering programs have not been updated to address changes brought about by the Fourth Industrial Revolution and a call for their modernization could be one of the first steps in this process. Similarly, cybersecurity courses should become an integral part of computer science and software engineering programs to ensure that developers incorporate security by design in the development process.

Educational responses should consider including more interdisciplinary courses, as well as dynamic and responsive curricula, to keep pace with technological advances (Gleason, 2018, p. 223). For example, there is a need for professionals with both knowledge of the healthcare sector and cybersecurity. As a result, some universities have started offering educational programs combining both health policy and cybersecurity.[19]

After undergraduate programs, students have the option to specialize in cybersecurity at the graduate level. There are a number of cybersecurity graduate programs, including Professional Masters' Degrees and Master of Research in fields from computer science to policy and management. Indeed, a few countries in Latin America offer cybersecurity graduate studies, such as the Instituto Tecnológico y de Estudios Superiores de Monterrey (Monterrey Institute of Technology and Higher Education) in Mexico[20] and the Escuela Superior de Guerra (Superior School of War) in Colombia.[21]

The European Union Agency for Cybersecurity (ENISA) created an education map of relevant cybersecurity degrees in its member states, including undergraduate and graduate programs.[22] Aside from helping students make informed decisions about their cybersecurity programs, by creating a cybersecurity education map governments can obtain a better idea of the availability of cybersecurity programs in higher education.

Governments can play an essential role in promoting the availability and quality of higher education cybersecurity programs by setting a standard for good cybersecurity education at the national level. For instance, the NCSC in the United Kingdom certifies bachelors' and masters' degrees in cybersecurity in the country.[23] This helps students make informed decisions about their chosen post-secondary education and employers are able to recruit more qualified individuals.

[19] For example, the University of Sydney is offering a Master of Health Security. See https://sydney.edu.au/courses/courses/pc/master-of-health-security.html.

[20] https://maestriasydiplomados.tec.mx/posgrados/maestria-en-ciberseguridad

[21] https://ciber.esdegue.edu.co/course/index.php?categoryid=6

[22] https://www.enisa.europa.eu/topics/cybersecurity-education/nis-in-education/universities

[23] https://www.ncsc.gov.uk/information/ncsc-certified-degrees

Cybersecurity Apprenticeship Programs

Students can get involved in cybersecurity after high school via apprenticeship programs. Specifically, apprenticeship programs focused on emerging techniques such as machine learning and artificial intelligence (AI) are critical to the future of the workforce, as these technologies will be present in almost every new software product and have become a top investment priority for Chief Information Officers (CIOs).[24] A survey conducted among 800 high-tech experts and executives predicted that by 2025 there would be an extensive integration of AI technology and, as such, AI roles and jobs in different parts of organizations. At the same time, many high-tech security companies are interested in developing apprenticeship programs that combine cybersecurity and artificial intelligence.[25]

Many apprenticeship programs in Latin America have already started training students in cybersecurity, such as the programs already referred to above from SENAI in Brazil and SENA in Colombia. Similarly, the National Research Foundation (NRF) in Singapore, for example, created a national AI program, AI Singapore, which includes an AI Apprenticeship Program (AIAP)[26] to groom local AI talent. In Germany[27] and South Korea,[28] governments have been applying a dual-education apprenticeship model, which combines hands-on training through partnerships with employers in parallel with traditional education (Deloitte, 2018b, p. 23). This dual-learning apprenticeship system can be a great mechanism to facilitate hiring by tech companies with high levels of demand for skilled workers.

Continuous Training and Certifications

Technological advances and the changing landscape of the cybersecurity threats require continuous upskilling and reskilling. No longer an option, it is now a necessity for 21st-century workers to continue their education. Short-term training and online courses help fill knowledge and skill gaps quickly. In Latin America, there are some opportunities for in-person and online short-term training. There are also many scholarship opportunities funded by governments, the private sector, and international organizations, such as the OAS.

For instance, the Spanish National Cybersecurity Institute (INCIBE) and the OAS organize the Cybersecurity Summer Bootcamp every year in León, Spain. This is a two-week program taught in Spanish for technicians, law enforcement professionals, and those interested in the development of national cybersecurity strategies.[29] The OAS provides scholarships for professionals from Latin America and the Caribbean to attend the Summer Bootcamp, which help them meet the costs of their participation. This program is becoming a leading initiative in cybersecurity with more than 100 professionals from Latin America participating in 2019 through scholarships provided by the OAS. Similarly, Florida International University (FIU) organizes a two-day cybersecurity executive certificate in cybersecurity leadership, supported by the OAS.[30] In 2020 the Cybersecurity Summer Bootcamp transformed into a virtual event in which more than 800 students from eighty countries participated.

[24] Gartner (July 2017). Gartner says AI technology will be in almost every new software product by 2020. Available at https://www.gartner.com/en/newsroom/press-releases/2017-07-18-gartner-says-ai-technologies-will-be-in-almost-every-new-software-product-by-2020.

[25] American Association of Community Colleges (January 2019). Developing Apprenticeships for cybersecurity. Available at http://www.ccdaily.com/2019/01/developing-apprenticeships-cybersecurity/.

[26] More information available at https://www.aisingapore.org/industryinnovation/aiap/.

[27] https://www.make-it-in-germany.com/en/study-training/training/vocational/system/

[28] http://ncee.org/what-we-do/center-on-international-education-benchmarking/top-performing-countries/south-korea-overview/south-korea-school-to-work-transition/

[29] https://www.incibe.es/en/summer-bootcamp

[30] https://gordoninstitute.fiu.edu/executive-education/cls/

Many private organizations also provide training and certification opportunities with cybersecurity modules, such as AWS,[31] Microsoft,[32] and CISCO.[33] Although a higher education degree is an indication of increased cybersecurity knowledge, employers may consider a certification as a better way to acquire cybersecurity skills (McAfee, 2017, p. 4). Indeed, cybersecurity training and certification can provide hands-on experience in practical areas of cybersecurity (Catota; Morgan; Sicker, 2019). Moreover, certifications can have a direct impact on salary expectations. The average salary of cybersecurity professionals holding security certificates is higher than the average of those without. While the former earn about US$21,000, the latter make an average of approximately US$16,000 in Latin America ((ISC)2, 2019, p. 17).

Continuous training and certification are such an important mechanism for promoting the adaptability of a cybersecurity workforce that the NICE initiative in the United States created a sub-working group on this topic. The Training and Certification Sub-Working Group developed a mapping matrix that links existing certifications to the NICE Framework of cybersecurity work roles within an organization.[34] Recognized cybersecurity certifications include:

- The Certified Ethical Hacker (CEH), offered by the International Council of E-Commerce Consultants (EC-Council).[35]
- The Certified Information Security Manager (CISM), offered by ISACA.[36]
- CompTIA Security+.[37]
- The Certified Information Systems Security Professionals (CISSP), offered by (ISC)^2.[38]
- The Sans GIAC Security Essentials (GSEC).[39]
- NIST Cybersecurity Framework (NCSF), Foundation and Practitioner.[40]
- Certified Computer Security Incident Handler (CERT), offered by Carnegie Mellon University.[41]

Ongoing opportunities for training and certifications allow professionals to stay up to date and to fill any knowledge gaps quickly.

Cybersecurity Research and Development (R&D)

Research expertise can assist governments and industry in the formulation of innovative solutions when addressing ongoing and future cybersecurity challenges and in identifying skills needed to streamline training plans. Research can take different forms, including: (1) Ph.D. programs focused on cybersecurity studies, (2) Centers of Excellence in Cybersecurity Research, and (3) specific R&D programs through agreements between academia and industry/government, among others.

[31] https://www.aws.training/

[32] https://www.microsoft.com/en-us/learning/default.aspx

[33] https://www.cisco.com/c/en/us/training-events/training-certifications.html

[34] https://www.nist.gov/itl/applied-cybersecurity/nice/illustrative-mapping-certifications-nice-framework

[35] https://cert.eccouncil.org/application-process-eligibility.html

[36] http://www.isaca.org/certification/cism-certified-information-security-manager/pages/default.aspx

[37] https://certification.comptia.org/certifications/security

[38] https://www.isc2.org/Certifications/CISSP

[39] https://www.giac.org/certification/security-essentials-gsec

[40] https://niccs.us-cert.gov/training/search/itsm-solutions-llc/nist-cybersecurity-framework-boot-camp-foundation-practitioner

[41] https://www.sei.cmu.edu/education-outreach/credentials/credential.cfm?customel_datapageid_14047=14324

For instance, the Prime Minister's Office of Singapore launched the National Cybersecurity R&D Program, which seeks to strengthen the resilience and preparedness of critical cyber infrastructure. Its initiatives include the National Cybersecurity R&D Laboratory (NCL), the Cybersecurity Consortium, Research Grants, as well as scholarships for graduate studies. To illustrate how these programs encourage cybersecurity education, the NCL recently partnered with the Singapore University of Technology and Design's iTrust Labs to "offer integrated experimentations and services to support government agencies, academia, and industry in their enterprise IT and operations technology cybersecurity research, technology evaluations and training."[42]

Another example is the National Cybersecurity Center of Excellence (NCCoE) in the United States. The NCCoE is part of NIST and consists of "a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity issues. This public-private partnership enables the creation of practical cybersecurity solutions for specific industries, as well as for broad, cross-sector technology challenges."[43] The NCCoE is undertaking many projects, such as Transport Layer Security (TLS), Server Certificate Management, Mobile Device Security, Data Security Projects, among others.[44]

Led by governments with a national vision for cybersecurity R&D, stakeholders such as universities, industry, civil society, and government can come together to collaborate in the development of research and tools to solve countries' most pressing cybersecurity needs. R&D hubs can be created when stakeholders from different sectors combine their efforts.

Building a Culture of Cybersecurity

Today, much of our personal and professional lives is conducted online. All citizens—even those not pursuing a career in the cybersecurity field—need a level of security proficiency to protect their personal data and that of any organization in which they work. According to a McKinsey report, human error is identified as one of the major causes of data breaches in organizations: 50% of data breaches between 2012 and 2017 had an insider threat component (McKinsey, 2018, p. 3). Professionals from all career paths can and should learn cybersecurity best practices.

The **OAS Cybersecurity Awareness Campaign Toolkit** recommends that cybersecurity awareness campaigns be simple and easy, avoiding technical specifics.[45] Cybersecurity awareness messages should be positively framed to empower the public to take action to protect themselves (OAS, 2016, p. 14). Governments should consider conducting surveys on how young people use technology and what they know about online security and privacy. There are a number of tools that could be applied to raise cybersecurity awareness, such as school assemblies, competitions, classroom lessons, informative material available from websites, social media campaigns, and others.

Partnerships between government, industry, and civil society can also contribute to raising cybersecurity awareness. The **STOP.THINK.CONNECT**[46] campaign was created by the National Cybersecurity Alliance (NCSA) and the Anti-Phishing Working Group (APWG) in collaboration with private

[42] https://www.nrf.gov.sg/programmes/national-cybersecurity-r-d-programme

[43] https://www.nccoe.nist.gov/about-the-center

[44] https://www.nccoe.nist.gov/projects

[45] https://www.thegfce.com/documents/publications/2015/10/01/cybersecurity-awareness-campaign-toolkit

[46] https://www.stopthinkconnect.org/

companies, non-profits, and government organizations. In 2014, the OAS recognized October as Cybersecurity Awareness Month and has celebrated every year since. The OAS has also encouraged its member states to increase their efforts on national cybersecurity policies and to join the STOP. THINK.CONNECT initiative "in establishing a coordinated and unified worldwide drive to create public awareness on cybersecurity."[47]

In Latin America, the Government of Chile launched a national cybersecurity awareness campaign, which includes several recommendations for the general public and office workers.[48] Likewise, Colombia's National Cybersecurity Awareness Campaign, entitled EnTIConfío, provides information and resources to a broad audience, particularly children.[49] Countries such as Argentina, Mexico, Panama, and Uruguay to name a few have created their own awareness campaigns to support the efforts of constructing more cyber resilient societies.

Actionable Recommendations

This section provides an outline of different tools and programs that could be develop by policymakers and educators in Latin America and the Caribbean to enhance the knowledge and skills of the region's current workforce and action the goals and objectives of the Cybersecurity Education Plan.

Classroom Lectures and Discussions

Innovative and dynamic classes on cybersecurity that encourage the discussion of basic concepts and introduce more complex concepts during the education cycle will help prepare students for the workforce. Educators could introduce cybersecurity concepts into existing classes or organize specific workshops about the topic. For example, the OAS, in partnership with Citi Foundation, developed the project "Creating a Career Path in Digital Security, Pathways2Progress," which provides a 48-hour digital security technical course for college students from 17 to 25 years of age. Spain's National Cybersecurity Institute (INCIBE) also organizes the "Cybersecurity Spaces," which consist of a three-hour practical technical course for between 20 and 30 students aged from 16 to 18. These are some examples of courses that help encourage young people to pursue a cybersecurity career.

Career Fairs

Career fairs and informative campaigns about a career path in cybersecurity should be encouraged, as most secondary students do not have access to cybersecurity-related courses, nor do they have an understanding of the opportunities in the field in many Latin American countries (Catota; Morgan; Sicker, 2019). Career fairs should engage not only students but also parents, as they can help their children in choosing career paths. For instance, the NICE initiative in the United States organizes the "NICE K-12 Cybersecurity Education Conference,"[52] which brings together educators, professionals, researchers, non-profits, and students to discuss potential strategies for raising awareness of cybersecurity career pathways among students and parents.

[47] OAS (October 2014). OAS Joins in Recognizing October as "Cybersecurity Awareness Month." Available at https://www.oas.org/en/media_center/press_release.asp?sCodigo=E-474/14.

[48] https://www.concienciadigital.gob.cl/

[49] https://www.enticconfio.gov.co/

Online Training and Labs

There are a number of online programs and webinars that offer a range of cybersecurity classes for various audiences and at various levels. In many Latin American countries, people get online through public innovation labs, and online training could be made available in these labs. Governments should combine their ICT-access projects with cybersecurity online training.

Platforms like AWS Educate and CISCO Academy, mentioned above, are good examples of training available online. Microsoft also offers a Professional Program for Cybersecurity that runs for three months every quarter. Massive Online Open Courses (MOOCs) have also become an essential tool for cybersecurity capacity building. Platforms such as Coursera, edX, Udacity, and Pluralsight offer many courses and even masters' degrees from recognized universities available in Spanish. To sum up, online training and labs are an exciting option for students from countries where cybersecurity training is not widely available or has prohibitive costs. Through public-private partnerships, national and local governments should seize the opportunity to use these online platforms to train their workforce on cybersecurity issues. The industry developed many of these platforms based on what they are looking for in an employee.

Competitions/Gamification

Competitions can contribute to raise awareness, encourage teamwork, and enable participants to tackle a real-world cyber incident in a controlled environment under the supervision of experts. These simulations can be structured to best approximate real-world attacks faced by organizations. Additionally, this is an opportunity for competitors to network and share information and even for encouraging diversity in the cybersecurity field.

The National Cybersecurity Centre (NCSC) in the United Kingdom, for example, is organizing the CyberFirst Girls Competition for young girls in the country, which aims to encourage the next generation of women to pursue a career in the cybersecurity field. Likewise, in Latin America, the OAS organizes the CyberWomen Challenge in partnership with Trend Micro, which establishes female-only teams to effectively mitigate cyber-attacks. Online games and quizzes are also an interactive way of capturing the attention of the general public to learn about good cybersecurity practices.

There is no shortage of policies that could further the integration of cybersecurity into education. The effective implementation of cybersecurity education policies can result in a larger prioritization of cybersecurity overall. As this white paper has highlighted, the first step for policymakers is to identify the need for the integration of cybersecurity into education. Following this, it is important to build a Cybersecurity Education Action Plan that will streamline the process of setting goals, objectives, and metrics. Once established, policymakers can opt for the integration of actors such as the private sector, academia, and even civil society through public-private-academic partnerships. These actors will lead different efforts under the overarching goal of educating the public on cybersecurity and ensuring a more cyber-aware population. Some examples include educating those at the primary and secondary level, encouraging students to pursue post-secondary studies in cybersecurity or pursuing apprenticeships, continuous training and certifications. Policies at a micro level, such as classroom lectures, discussions, career fairs, and training labs, must also be taken into consideration for a rapid integration.

Conclusion

To formulate and implement a Cybersecurity Education Action Plan, Latin American and Caribbean governments must coordinate their efforts with the private sector, civil society, and academia. The shortage of skilled cybersecurity professionals requires immediate action to train current cybersecurity professionals and educate the next generation of the workforce. To close the workforce gap—which in Latin America is 600,000 people, rising to 4 million people worldwide—governments need to take a strategic approach and collaborate with the private sector and academia to formulate and implement a Cybersecurity Education Action Plan or CEAP. A CEAP is a blueprint for policymakers to design effective public policies intended to strengthen their national cybersecurity strategies and develop the cybersecurity workforce and can contribute to a more prepared cybersecurity workforce and a more cyber-aware population. The key components of a CEAP include:

(1) clear and defined goals to prioritize and integrate cybersecurity education at all levels that guide the actions of policymakers

(2) a multi-stakeholder approach

(3) monitoring mechanisms and indicators that evaluate progress towards the goals of the action plan.

Policymakers have a variety of tools at their disposal to implement the CEAP and can create age appropriate programming to boost cybersecurity awareness and education from primary school to professionals interested in continuing education. The programming ranges from online labs to competitions, gamification, career fairs, and classroom lectures and discussions. As students mature, there are opportunities for cybersecurity apprenticeships, graduate programs, additional training and certifications.

The NICE Strategic Plan is a good example of how to outline a primary to secondary education plan. The "National K-12 Cybersecurity Education Implementation Plan" aims to: (1) encourage students to engage in cybersecurity-related activities, (2) assist educators in incorporating cybersecurity concepts into classes, and finally, (3) help primary and secondary students identify career opportunities in the cybersecurity field. Education and workforce development has many stages, and the expansion of any cybersecurity education plan should keep that in mind. Education from the primary to post-secondary levels, continuing educational programs, and R&D play a significant role in enhancing the cybersecurity workforce. Several tools could be developed to foster cybersecurity education in each stage of the workforce development lifecycle. Capacity building can be enhanced at the national level at all stages of education and workforce development by including specific components of cyber education during each instance. From K-12 education to Research and Development these can all benefit from the promotion of tangible and soft cyber-education skills.

Countries in Latin America will be able to reap the benefits of the Fourth Industrial Revolution if they invest in both technology and their people. Innovation through new business opportunities and social interactions can only be achieved at the point where technology meets skilled workers. Latin America, like every region of the world, requires a workforce that has the knowledge and skills to build and operate emerging and future technologies, as well as the capability to secure them.

References

Catota, F. E.; Morgan, M.G.; and Sicker, D.C. (2019). Cybersecurity education in a developing nation: the Ecuadorian environment, Journal of Cybersecurity, Volume 5, Issue 1. Retrieved from https://doi.org/10.1093/cybsec/tyz001

Cybersecurity Ventures (2019). 2019 Official Annual Cybercrime Report. Retrieved from https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf

Deloitte (2019). Tech Trends 2019. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/br/Documents/technology/DI_TechTrends2019.pdf

Deloitte (2018a). The jobs are here, but where are the people? Retrieved from https://www2.deloitte.com/us/en/pages/manufacturing/articles/future-of-manufacturing-skills-gap-study.html

Deloitte (2018b). Preparing tomorrow's workforce for the Fourth Industrial Revolution. Retrieved from: https://www2.deloitte.com/content/dam/Deloitte/global/Documents/About-Deloitte/gx-preparing-tomorrow-workforce-for-4IR.pdf.

ENISA (2019). Cybersecurity Culture Guidelines: Behavioral Aspects of Cybersecurity. Retrieved from https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity

ENISA (2015). Status of Privacy and NIS course curricula in Member States. Retrieved from https://www.enisa.europa.eu/publications/status-of-privacy-and-nis-course-curricula-in-eu-member-states

Gleason, N. W. (Ed.). (2018). Higher education in the era of the fourth industrial revolution. Singapore: Palgrave Macmillan.

Global Cyber Security Capacity Centre (2016). Cybersecurity Capacity Maturity Model for Nations (CMM) – Revised Edition. Retrieved from https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20revised%20edition_09022017_1.pdf.

IBM (2018). IBM X-Force Threat Intelligence Index 2018. Retrieved from https://www.ibm.com/downloads/cas/MKJOL3DG

Inter-American Development Bank – IDB (2016). The Road toward Smart Cities: Migrating from Traditional City Management to the Smart City. Retrieved from https://publications.iadb.org/en/road-toward-smart-cities-migrating-traditional-city-management-smart-city

IDB (2018). Factores de éxito y aprendizajes obtenidos de la formación de alianzas público-privadas. Retrieved from https://publications.iadb.org/es/factores-de-exito-y-aprendizajes-obtenidos-de-la-formacion-de-alianzas-publico-privadas

(ISC)2 (2019). Strategies for Building and Growing Strong Cybersecurity Teams. (ISC)2 Cybersecurity Workforce Study, 2019. Retrieved from https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx?la=en&hash=D087F6468B4991E0BEFFC017BC1ADF59CD5A2EF7

(ISC)2 (2018). Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens. (ISC)2 Cybersecurity Study, 2018. Retrieved from https://www.isc2.org/-/media/ISC2/Research/2018-ISC2-Cybersecurity-Workforce-Study.ashx?la=en&hash=4E09681D0FB51698D9BA6BF13EEABFA48BD17DB0

(ISC)2 (2017). Global Information Security Workforce Study. Retrieved from https://www.isc2.org/-/media/B7E003F79E1D4043A0E74A57D5B6F33E.ashx

International Telecommunication Union – ITU (2019). Global Cybersecurity Index (GCI) 2018. Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf

Lewis, J. (2018). Economic Impact of Cybercrime – No Slowing Down. Retrieved from https://csis-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf?kab1HywrewRzH17N9wuE24soo1IdhuHd&utm_source=Press&utm_campaign=bb9303ae70-EMAIL_CAMPAIGN_2018_02_21&utm_medium=email&utm_term=0_7623d157be-bb9303ae70-1940938

Kelly, K. (2016). The inevitable: understanding the 12 technological forces that will shape your future. New York, NY: Penguin Books.

McAfee (2017). Hacking the Skills Shortage: A study of the international shortage in cybersecurity skills. Retrieved from https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hacking-skills-shortage.pdf

McKinsey & Company (2018). Insider Threat: The human element of cyberrisk. Retrieved from https://www.mckinsey.com/business-functions/risk/our-insights/insider-threat-the-human-element-of-cyberrisk.

National Cybersecurity Alliance – NCSA (2017). Securing our Future: Cybersecurity and the Millennial Workforce. Retrieved from: https://www.raytheon.com/sites/default/files/2017-12/2017_cyber_report_rev1.pdf

National Initiative for Cybersecurity Education – NICE (2017). National K-12 Cybersecurity Education Implementation Plan. Retrieved from https://www.nist.gov/sites/default/files/documents/2017/04/26/nice_k12_implementation_plan.pdf

National Institute of Standards and Technology – NIST (2017). NIST Special Publication 800-181, National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf

Open Web Application Security Project – OWASP (2016). Security by Design Principles. Retrieved from https://www.owasp.org/index.php/Security_by_Design_Principles

Organization of American States – OAS (2016). Cybersecurity Awareness Campaign Toolkit. Retrieved from https://www.thegfce.com/documents/publications/2015/10/01/cybersecurity-awareness-campaign-toolkit

Organization for Economic Cooperation and Development – OECD (2012). The Protection of Children Online: Recommendations of the OECD Council. Retrieved from:

Organization for Economic Cooperation and Development – OECD (2016). Start-up Latin America 2016: building an innovative future. Retrieved from: https://www.oecd.org/dev/americas/Startups2016-Assessment-and-Recommendations.pdf

Organization for Economic Cooperation and Development – OECD (2017). Latin America Economic Outlook 2017 – Youth, Skills and Entrepreneurship. Retrieved from: https://www.oecd.org/dev/americas/Overview_LEO2017.pdf

Organization for Economic Cooperation and Development – OECD (2019). Measuring Innovation in Education 2019: What has changed in the classroom? Retrieved from:

Ponemon Institute (2018). 2018 Cost of a Data Breach Study: Global Overview. Retrieved from: https://www.ibm.com/downloads/cas/861MNWN2

Ponemon Institute (2019). Ninth Annual Cost of Cybercrime Study: Unlocking the Value of Improved Cybersecurity Protection. Retrieved from https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50

Schwab, K. (2016). The Fourth Industrial Revolution. New York, NY: Crown Business

Symantec (2018). Internet Security Threat Report. Retrieved from http://images.mktgassets.symantec.com/Web/Symantec/%7B3a70beb8-c55d-4516-98ed-1d0818a42661%7D_ISTR23_Main-FINAL-APR10.pdf?aid=elq_

Symantec (2019). Internet Security Threat Report. Retrieved from https://img03.en25.com/Web/Symantec/%7Bdfc1cc41-2049-4a71-8bd8-12141bea65fd%7D_ISTR_24_2019_en.pdf

Wagner, D. A., et al. (2005). Monitoring and evaluation of ICT in education projects: a handbook for developing countries. Washington, DC: InfoDev.

World Economic Forum – WEF (2014). Creating New Models: Innovative Public-Private Partnerships for Inclusive Development in Latin America. Retrieved from http://www3.weforum.org/docs/GAC/2014/WEF_GAC_LatinAmerica_InnovativePublicPrivatePartnerships_Report_2014.pdf

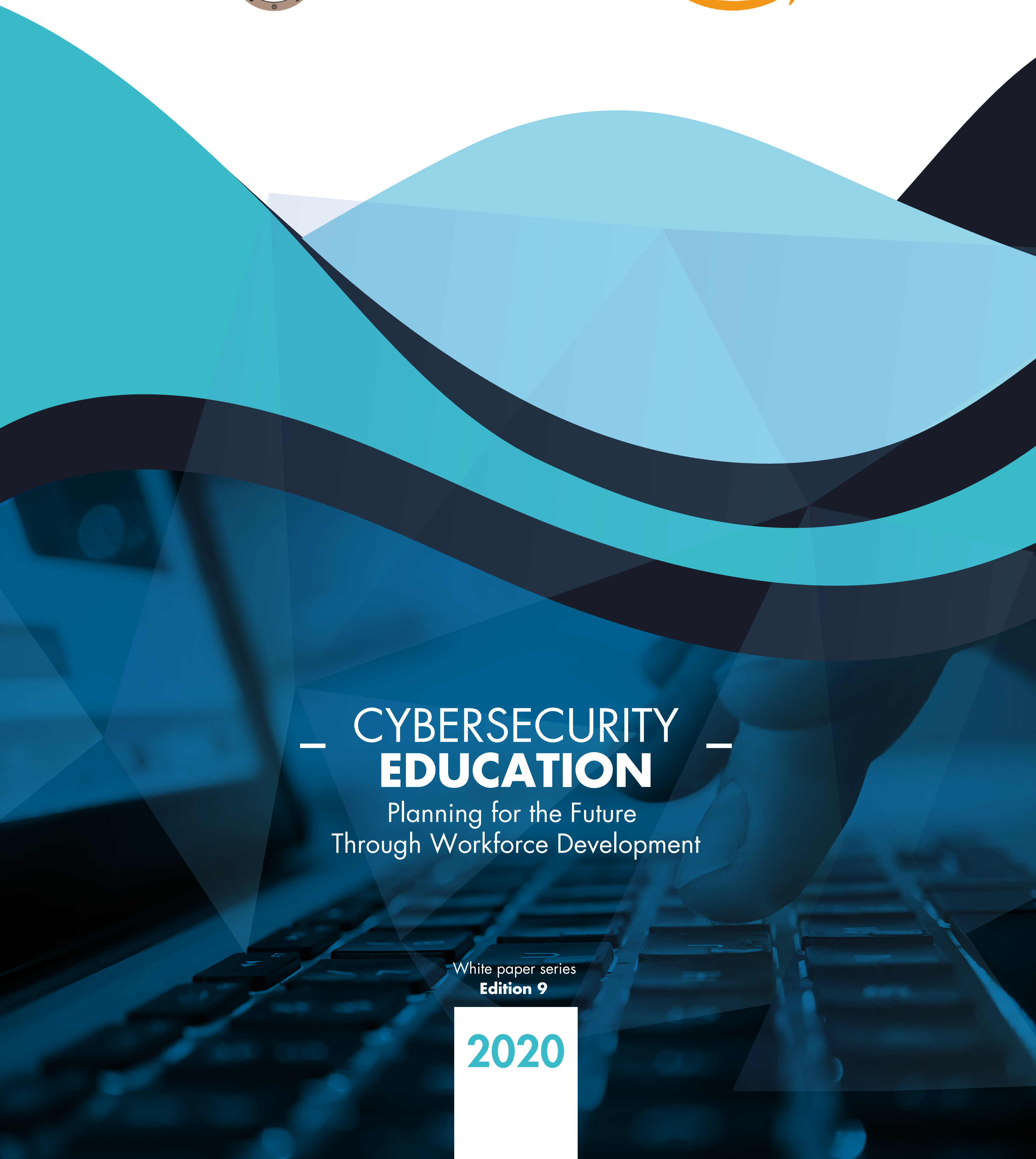
World Economic Forum – WEF (2015a). Bridging the Skills and Innovation Gap to Boost Productivity in Latin America. Retrieved from: https://www2.deloitte.com/content/dam/Deloitte/cr/Documents/finance/201501-Competitiveness_Lab_Latin_America_final.pdf

World Economic Forum – WEF (2015b). Deep Shift: technology tipping points and societal impact. Retrieved from: http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf

CYBERSECURITY EDUCATION

Planning for the Future Through Workforce Development

CICTE01316E05



_ CYBERSECURITY EDUCATION _

Planning for the Future Through Workforce Development

White paper series
Edition 9

2020