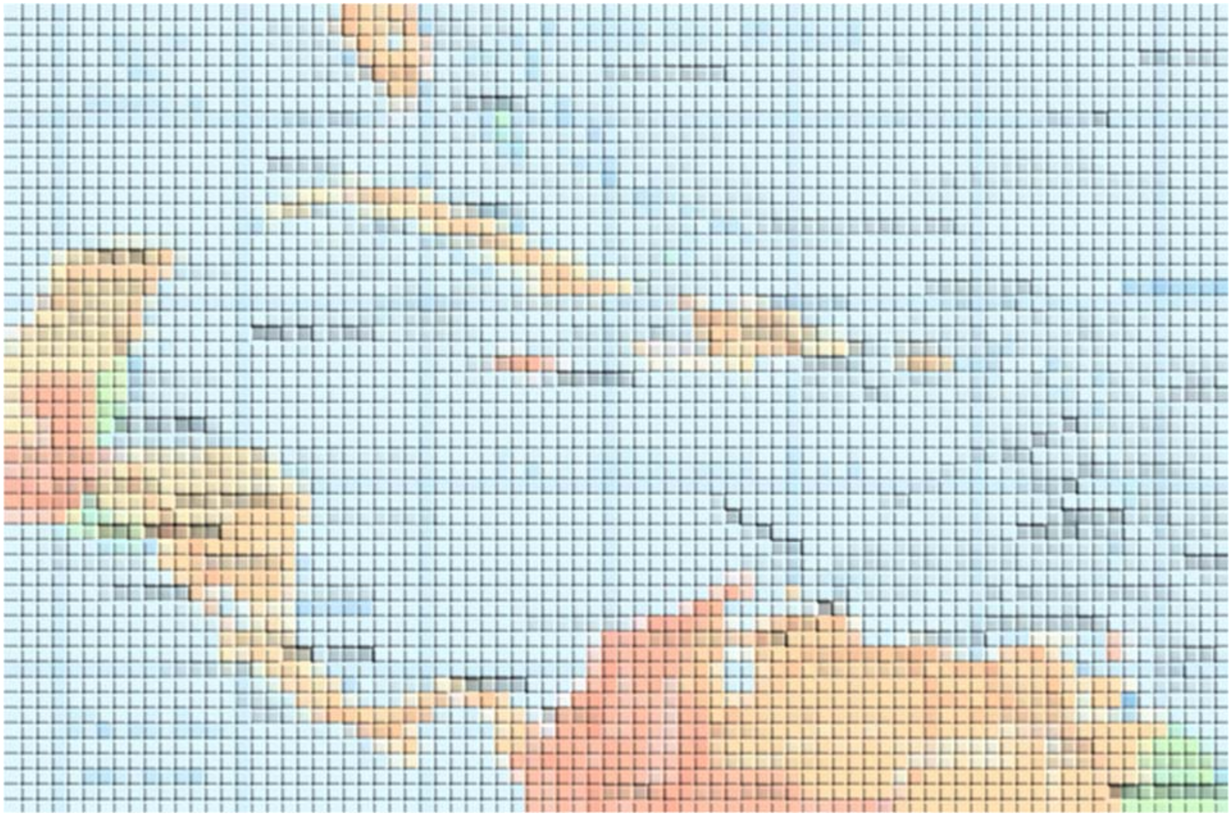
Caribbean Regional Cybersecurity Training Needs Analysis

2022



Public Version

Acknowledgements

The Caribbean Regional Cybersecurity Training Needs Analysis was done on behalf of the Government of Jamaica, through the Office of the National Security Advisor (ONSA) by the Protection Group International (PGI). The project was facilitated through the support of the United Kingdom's Foreign, Commonwealth and Development Office.

ONSA would like to thank the national and regional stakeholders who participated in the Skills Symposium and Validation workshops, and also the stakeholders who participated in the consultation.

ONSA Team
Brigadier Roderick Williams
Major Corlane Barclay
Ms Tameka Bowes

PGI Team
Reem Awad
Matthew Griffin
Lucas Kantariz-Diaz
Brian Lord
Sebastian Madden
Lara Pace
Sarah Puello Alfonso
Hanniyah Rahman Shepherd
Frederick Shepherd

Table of Contents

ACKNOWLEDGEMENTS 1

TABLE OF CONTENTS 2

INTRODUCTION 2

EXECUTIVE SUMMARY 4

CHAPTER 1 6

CHAPTER 2 21

CHAPTER 3 28

CHAPTER 4 36

APPENDIX A – CARIBBEAN CYBERSECURITY SKILLS SYMPOSIUM AGENDA 48

APPENDIX B – CARIBBEAN CYBERSECURITY SKILLS SYMPOSIUM SUMMARY 51

APPENDIX D – LITERATURE REVIEW SOURCE SUMMARY 55

APPENDIX E – INTERVIEW SUMMARY 56

APPENDIX F – CYBERSECURITY CAPACITY AND SKILLS MODELS 57

Introduction

This Training Needs Assessment report has been prepared for the Office of the National Security Advisor (ONSA) by Protection Group International (PGI) and funded by the Foreign, Commonwealth and Development Office of the United Kingdom. Some information has been redacted from the public version of this report.

Context

The outcome of the cybersecurity training needs assessment is to inform the development of a Cyber Academy under the auspices of the Jamaican Defence Force. The Academy's objective is to enable a robust, resilient and responsive cybersecurity cadre of expertise over the next three to five years by developing cyber security professionals for Jamaican Defence, public and private sector organisations. The Academy is also intended to serve as a resource for other countries in the English-speaking Caribbean to enable economies of scale and regional interoperability.

The ONSA asked PGI to propose a strategic training needs assessment to inform the development of the Academy's vision, goals, curriculum, course material and commercial model to ensure that the design is driven by Jamaica's strategic objectives and the type and volume of skills these are likely to require and, where possible, the training and education needs of other countries in the region.

Approach

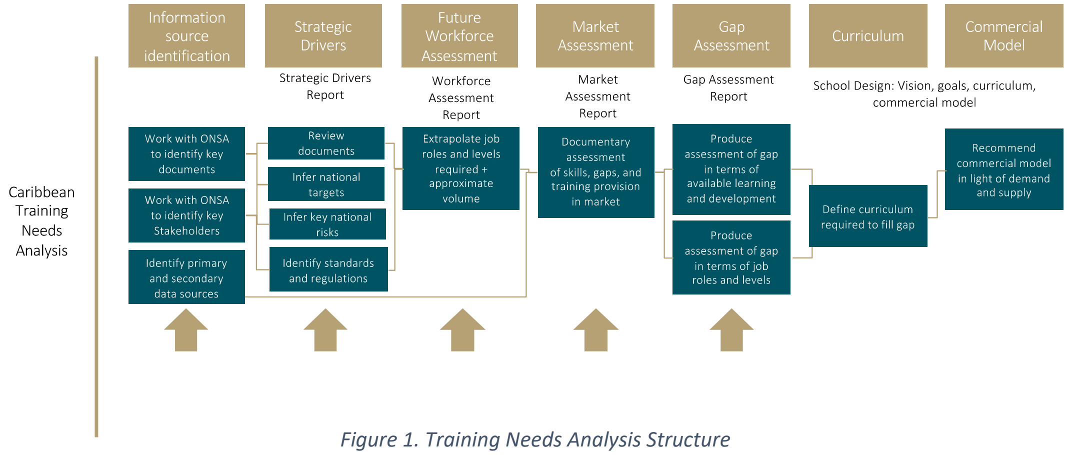

Information source identification
Strategic Drivers
Future Workforce Assessment
Market Assessment
Gap Assessment
Curriculum
Commercial Model
Strategic Drivers Report
Workforce Assessment Report
Market Assessment Report
Gap Assessment Report
School Design: Vision, goals, curriculum, commercial model
Caribbean Training Needs Analysis
Work with ONSA to identify key documents
Work with ONSA to identify key Stakeholders
Identify primary and secondary data sources
Review documents
Infer national targets
Infer key national risks
Identify standards and regulations
Extrapolate job roles and levels required + approximate volume
Documentary assessment of skills, gaps, and training provision in market
Produce assessment of gap in terms of available learning and development
Produce assessment of gap in terms of job roles and levels
Define curriculum required to fill gap
Recommend commercial model in light of demand and supply

Figure 1. Training Needs Analysis Structure

This report is broken down into five chapters:

- Executive Summary
- Chapter 1: Strategic Drivers
- Chapter 2: Future Workforce Assessment
- Chapter 3: Market Assessment
- Chapter 4: Gap Assessment

The report outlines a set of recommendations and next steps, which include a suggested Curriculum, Commercial Model and Implementation Plan for the Caribbean Military Academy’s Institute of Cyber Science.

Executive Summary

This study was undertaken at the request of the Office of the National Security Advisor, of Jamaica, to understand the cybersecurity training requirements and needs of Jamaica and the broader English-speaking Caribbean. Findings and recommendations would inform the curriculum design of the Caribbean Military Academy's Caribbean Institute of Cyber Science. The study was conducted over a period of four months, between August and November 2021.

To establish the current and future training requirements of both Jamaica and the broader Caribbean region, a consultation with relevant stakeholders was initiated through the Region's first Caribbean Cybersecurity Skills Symposium which was convened on the 25th and 26th of August 2021 by the Office of the National Security Advisor. Stakeholders from across the region were invited to participate in the consultation and the symposium saw representation from 11 countries in the region.

Through a blended data collection approach, composed of a bespoke questionnaire, one-on-one interviews, and desktop research, eight strategic drivers were identified. These are:

1. Acceleration of Digital Transformation National and Regional Efforts.
2. Critical National Infrastructure Protection.
3. Enforcement and Compliance with National Cybersecurity legislative and regulatory agendas.
4. Capacity Building in National Security and the Criminal Justice System.
5. Strengthening Incident Response Capabilities.
6. Adoption of Security Standards and Controls.
7. Improving National and International Cooperation.
8. Responding to the Role of Research and Development.

The strategic priorities outlined above unlock the potential requirement of particular skillsets which are key to developing and building a workforce, as well as an enabling environment for Jamaica and the Caribbean region. Through the workforce assessment, the study outlines what type of job roles, units, teams, and departments will be required to support the strategic ambitions of the region. Coupled with a market assessment, which demonstrated that the training provision in region currently appears to be limited in scope and breadth, this study presents recommendations which are designed to build the necessary national and regional independent capability for the development of cybersecurity workforces.

For the Caribbean Institute of Cyber Science to meet the strategic goals for Jamaica and position itself as the driving force behind regional skills development, then the model upon which it is built must be designed with the following three objectives:

- Be as financially self-sustainable as possible; thus, mitigating the impact upon the wider Jamaican national (and military) budget;
- Reduce dependence upon internationally provided training provision and encourage and stimulate Jamaican and regional economic growth in both academia and private sector training provision to ensure value for money and enable national and regional self-sufficiency;
- Ensure the Caribbean Institute of Cyber Science 'owns' the evolution of national cyber workforce capability and places itself at the top end of national and regional skills and capability development.

A critical enabler to this will be the development of national and regulatory cyber security standards in delivering essential services in the public and private sectors. These standards will meet the primary aim of preserving the digital resilience of Jamaica and the region, and also provide a foundation for the Caribbean Institute of Cyber Science to meet the three objectives above.

Lastly, the study includes some practical next steps for consideration by the Government of Jamaica to ensure that the momentum built through the stakeholder consultation is not lost. They are designed to be tangible, consequential, and realistic in order to realize the recommendations outlined in this report.

This Training Needs Assessment provides the Government of Jamaica, and particularly the Caribbean Military Academy with the necessary analysis to comprehensively inform the design of the Caribbean Institute of Cyber Science. The different sections identify Strategic Drivers of the Region which in turn depict the demand for specific cybersecurity job roles, skills, and qualifications, coupled with market research to identify technical training provision in the region.

Chapter 1

Strategic Drivers

Introduction

This Strategic Drivers report identifies, defines, and describes key activities and capabilities that are either already in place, or are planned for action over the next three to five years, that are likely to drive a need for cybersecurity skills in the Caribbean region. This includes looking at a range of strategy and policy goals, legislative and regulatory priorities, the adoption of security standards and controls, and other activities and utilization of ICTs that will create requirements for developing the cybersecurity capacity and capability of national and regional governments, private sector, and civil society organizations.

A combination of complementary data collection exercises was completed to understand the various forces driving this need for cybersecurity skills in the Caribbean region with participation from across the region. This included:

1. a questionnaire distributed to government and non-government representatives to capture country and sectoral level activities and capabilities. Question set and response analysis summary detailed in *Appendix C*.

2. a literature review of key documents relating to national cybersecurity risks, formal and implied capacity maturity targets, and prevailing and planned legislation, regulation, and standards. Analysis summary provided in *Appendix D.*

3. a series of one-on-one interviews with senior-level national and regional stakeholders to address any research gaps. Interview details provided in *Appendix E.*

4. insights collected from the 2021 Caribbean Cybersecurity Skills Symposium. Summary provided in *Appendix B*.

Analysis of the research findings identified eight thematic areas that capture the key strategic forces that are likely to drive a need for cybersecurity skills in the Caribbean in the future including:

1. Acceleration of national and regional digital transformation efforts
2. Critical national infrastructure protection
3. Enforcement and compliance with national cybersecurity legislative and regulatory agendas
4. Capacity building in national security and the criminal justice system
5. Strengthening incident response capabilities
6. Adoption of security standards and controls
7. Improving national and regional collaboration
8. Responding to the role of research and development

Strategic Drivers: Thematic Areas

1. Acceleration of national and regional digital transformation efforts

Digital Transformation

The World Bank[1] defines digital transformation using an ecosystem approach consisting of five elements, including (i) Digital infrastructure (fixed and mobile broadband, fiber-optic cables, etc.); (ii) Digital financial services and digital identification; (iii) Digital innovation and entrepreneurship; (iv) Digital platforms, including e-commerce and e-government; and (v) Digital literacy and skills.

Caribbean Context

In response to the ongoing COVID-19 pandemic, Caribbean countries have witnessed a rapid acceleration of national and regional digital transformation activity as the pandemic forced work, education, and many public and private sector service offerings online. This has resulted in the increased adoption of ICTs across society while also highlighting gaps in areas such as internet connectivity, digital literacy, and the provision of e-commerce and e-government platforms across the regions.[2] The Caribbean Development Bank[3] in 2019 previously highlighted the importance of digital transformation efforts and the need for continued and increased investment in digital infrastructure as a key catalyst for accelerating economic growth and job creation in the region with such investments able to enhance public service delivery and build greater economic resilience.[4] Such digital transformation efforts are expected to continue over the next five years.

Examples of planned and ongoing digital transformation activity include:

Jamaica:

- The Jamaican government has recognized digital transformation as a catalyst of the Vision 2030 National Development Plan[5] with National Outcome #11 focused on developing a 'Technology Enabled Society'.
- Development and digitalization of a Government National Identification System (NIDS).[6]
- Jamaica Single Window for Trade (JSWIFT) providing a web-based portal for access to services in support of cross-border trade in Jamaica.[7]

Trinidad and Tobago:

- Establishment in 2021 of the standalone Ministry of Digital Transformation that will lead National Digital Transformation efforts.[8]
- Exploring the launch of e-identity and national health online services.

[1] https://www.worldbank.org/en/topic/digitaldevelopment/overview#2

[2] https://documents1.worldbank.org/curated/en/848701593136915061/pdf/Dominica-Grenada-St-Lucia-St-Vincent-and-the-Grenadines-and-the-Organization-of-Eastern-Caribbean-States-Caribbean-Digital-Transformation-Project-Digital-Caribbean.pdf

[3] https://www.caribank.org/sites/default/files/publication-resources/Keynote%20Address_President_Aldith%20Brown%20Memorial%20Lecture-ECCB_20191119.pdf

[4] https://documents1.worldbank.org/curated/en/848701593136915061/pdf/Dominica-Grenada-St-Lucia-St-Vincent-and-the-Grenadines-and-the-Organization-of-Eastern-Caribbean-States-Caribbean-Digital-Transformation-Project-Digital-Caribbean.pdf

[5] https://sustainabledevelopment.un.org/content/documents/1501jamaica.pdf

[6] https://opm.gov.jm/portfolios/national-identification-system/

[7] https://www.jswift.gov.jm/

[8] http://www.news.gov.tt/content/appointment-minister-digital-transformation

Guyana:

- Launch of the Digital Governance Roadmap for Guyana 2018.[9]

Regional

- World Bank Caribbean Digital Transformation Project 2020-2026[10]: $US94 million project to increase access to digital services, technologies, and skills by governments, businesses, and individuals in the participating Eastern Caribbean countries.
- CARICOM Strategic Plan 2015-2019[11]: 'Building Technological Resilience' as a strategic priority with a goal to develop a CARICOM Digital Economy within the framework of a CARICOM Digital Agenda 2025. This includes strategies to develop a single CARICOM ICT space, e-government and m-government services, and resource mobilization for ICT investments across member states.
- CTU Vision and Roadmap for a CARICOM Single ICT Space 2017[12]: Priority areas of focus in building the digital economy during the period 2014 to 2019 will include the establishment of a CARICOM Single ICT Space to provide the ICT-enabled foundation for enhancing both CARICOM's functional cooperation and fulfilling the social, cultural, and economic imperatives of the region.

Skills Requirement

While such digital transformation efforts bring a range of benefits they also come with risks, with more ICTs across the national ecosystem increasing the attack surface for malicious actors and cyber threats. As such, there will be increasing demand for a range of ICT and cybersecurity skills to facilitate, optimize, and secure the expansion of such digital transformation efforts.

2. Critical national infrastructure protection

Critical National Infrastructure

Critical National infrastructure (CNI)[13] is defined as "those critical elements of infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in: a) Major detrimental impact on the availability, integrity or delivery of essential services – including those services whose integrity, if compromised, could result in significant loss of life or casualties – taking into account significant economic or social impacts; and/or b) Significant impact on national security, national defence, or the functioning of the state."

Caribbean Context

There are currently low levels of capacity maturity in the Caribbean when it comes to the identification and protection of CNI, with stakeholders in the community recognizing an urgent need for national risk assessments to define, identify, and develop strategies to protect such assets from increasing threat of cyber-attack.

[9] https://ndma.gov.gy/wp-content/uploads/2020/01/DigitalGovernanceRoadmap_20181025.pdf

[10] https://documents1.worldbank.org/curated/en/848701593136915061/pdf/Dominica-Grenada-St-Lucia-St-Vincent-and-the-Grenadines-and-the-Organization-of-Eastern-Caribbean-States-Caribbean-Digital-Transformation-Project-Digital-Caribbean.pdf

[11] https://caricom.org/documents/strategic-plan-caribbean-community-2015-2019/

[12] https://caricom.org/wp-content/uploads/vision_and_roadmap_for_a_single_ict_space_-_final_version_updated.pdf

[13] https://www.cpni.gov.uk/critical-national-infrastructure-0

A range of potential CNI assets and operators were identified by respondents to the questionnaire across a range of sectors including Banking and Finance, Defence and National Security, Emergency Services, Government, Public Health, Telecommunications, Transportation, and Utilities.

Examples of planned and ongoing CNI Protection activity include:

Jamaica

- A CNI Protection Plan is currently being drafted.
- Plans to establish formal monitoring mechanisms for CNI with clearly defined roles and channels of communication for all stakeholders
- Plans from the Government to strengthen the process of reviewing and monitoring of technical security standards being employed in the public sector and by private-sector entities that manage/operate CNI.
- Encourage software quality standards and functional requirements for the developers of applications and software in the public sector and for private-sector entities that are operators of CNI.
- Encourage the continued development and sharing of disaster recovery and business continuity plans for Government Ministries, Departments, and Agencies (MDAs) and private entities that manage critical infrastructure and critical information infrastructure.
- Baseline standards and mandatory certification for CNI system users.[14]

Trinidad and Tobago:

- In 2021 TnT CIRT is working with the UK FCDO to complete a national cybersecurity risk assessment to identify and reach out to CNI operators across the country.
- A National Critical Information Infrastructure Protection (CIIP) Policy is planned for development.

Skills Requirement

The formalization of CNI protection plans will bring a need for a range of cybersecurity skills to mitigate risks and defend against attacks of important sectors and assets across the government and private sectors.

3. Enforcement and compliance with national cybersecurity legislative and regulatory agendas

Cyber Legislation

Cybersecurity legislation and regulation includes a range of provisions related to cybersecurity and cybercrime. This can include a range of areas including but not limited to substantive law criminal offences to procedural laws, civil-and-criminal liabilities, breach notification and vulnerability disclosure, data protection, child protection online, consumer protection and intellectual property. [15]

[14] Consultant workshop for the development of the National Cybersecurity Strategy
[15] https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf

Convention on Cybercrime[16]

The Convention on Cybercrime, known as the 'Budapest Convention', is considered the leading international instrument focused on crimes committed via the Internet and other computer networks; dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception.

Caribbean Context

The past five years has seen a significant growth in cybercrime in the Caribbean, with examples including hacking of government websites, infiltration of child online exploitation materials and the increasing use of cryptocurrencies to fund criminal activities.[17] In response to this, Caribbean governments have been developing and updating a range of cybersecurity and cybercrime legislation and regulation to reflect the changing digital environment and outline requirements for public, private, and civil society sectors to protect their systems and operations from cyber-attacks.

Examples of planned and ongoing cybersecurity legislative agenda activity include:

Jamaica:

- Revising the national cybercrime act and other cybersecurity legislation and considering[18]:
  - New and emerging digitally-facilitated crimes and ensure legislation allows for vulnerability testing and collaborative investigation tools.
  - Improving legislation on ISPs related to data sharing and protecting CNI.
  - Reviewing the overall suite of legislation related to digital security.
  - Mandatory legislative requirements for reporting.
- Data Protection Act 2020 will be enacted in 2022 following a grace period to allow entities to prepare for its implementation.
- National identification and Registration Act in progress.
- The development of regulations for baseline cybersecurity services for Government.[19]

Antigua

- Plans to update the current cybersecurity legislature and expand the scope of cybercrimes.
- The Draft Antigua and Barbuda Information and Communication Technologies (ICTs) Policy[20] highlights plans to:
  - establish an Independent Regulatory Authority.
  - develop a regulatory framework that fosters the safe use of the Internet and protects intellectual property in a digital environment.

[16] https://www.coe.int/en/web/cybercrime/the-budapest-convention
[17] CARICOM Cyber Security and Cybercrime Action Plan (CCSCAP)
[18] Government of Jamaica 2021 Consultant workshop for the development of the National Cybersecurity Strategy
[19] Consultant workshop for the development of the National Cybersecurity Strategy
[20] https://docplayer.net/18832671-Antigua-and-barbuda-information-and-communication-technologies-icts-draft-policy.html

Barbados:

- Authorities in Barbados are currently pursuing updates of their domestic cybercrime legislation in line with the Budapest Convention and will then move to implementation of cybersecurity legislation and regulation.[21]
- Barbados' Data Protection Act 2019 was operationalized from March 2021.

Guyana

- Guyana Green State Development Strategy: Vision 2040 [22]details that the Ministry of Public Telecommunications strategic plan focuses on strengthening the legal, regulatory and policy environment in the sector.

Trinidad and Tobago

- Plans in place to strengthen Data Protection Act in 2021 through a Data Protection Amendment Bill.

Regional

- In 2017, CARICOM released their inaugural 'Cyber Security and Cybercrime Action Plan (CCSCAP)', which included the 'Legal Environment' as a key priority area of intervention for addressing cybersecurity and cybercrime issues in the Caribbean region. Focus points of the priority area include:
    - Enactment of appropriate Cyber legislation.
    - Establishment of effective data retention legislation, which balances public safety with human rights, privacy, and data protection regimes.
    - Developing a mechanism and infrastructure for dealing with online child pornography.
- World Bank Caribbean Digital Transformation Project 2020-2026[23] subcomponent 1.3 'Cybersecurity, Data Protection and Privacy: Legal and Regulatory Environment, Institutions, and Capacity' includes planned activities such as:
    - Reviewing and updating regional and national cybersecurity policies, legislation, regulation, and institutional and coordination structures.
    - Reviewing and updating regional and national data protection and privacy laws and data access and exchange policies.
- In 2019 the Council of Europe[24] held the 'Regional Conference on Cybercrime Strategies and Policies and features of the Budapest Convention for the Caribbean Community' which encouraged CARICOM member states to ratify the Budapest Convention.

[21] https://www.coe.int/en/web/cybercrime/-/octopus-project-authorities-in-barbados-are-pursuing-updates-of-their-domestic-cybercrime-legislation-in-line-with-the-budapest-convention

[22] https://observatorioplanificacion.cepal.org/en/plans/green-state-development-strategy-vision-2040-guyana

[23] https://documents1.worldbank.org/curated/en/848701593136915061/pdf/Dominica-Grenada-St-Lucia-St-Vincent-and-the-Grenadines-and-the-Organization-of-Eastern-Caribbean-States-Caribbean-Digital-Transformation-Project-Digital-Caribbean.pdf

[24] https://rm.coe.int/3148-1-1-3-final-report-dr-reg-conference-cy-policies-caribbean-comm-1/168098fb6c

Skills Requirement

The introduction of new—and amendment of existing—cybersecurity and cybercrime legislation brings with it a simultaneous need to build capacity and skills to both ensure compliance with such legislation, as well as developing the capability of actors in the criminal justice system to enforce such legislation.

4. Capacity building in national security and the criminal justice system

National Security and Criminal Justice[25]

Capacity to respond to cyber threats is important for countries to defend their national security and create a safe environment for the use of ICTs throughout society. National security actors include key government security agencies and defense-force entities tasked with protecting the cyber environment and interests of the country. Criminal justice sector actors include law enforcement, prosecutors, and courts involved in the investigation and prosecution of cybercrime cases, and play leading roles in the enforcement of capabilities of a country's cybercrime legislation.

Caribbean Context

Further to the development and revision of cybercrime legislation and strategies across the region, there has also been recognition of the need to build up national and regional capacity and capabilities to enforce and implement such activity as it comes in to force. From a national security perspective, cybersecurity has been identified as a key challenge by governments, with some in the region already taking steps to expand their defence capabilities to deal with the escalating cyber threat situation.

Examples of planned and ongoing activity include:

Jamaica

- Cyber recently added as a new frontier for the Jamaican Defence Force with the establishment of the Maritime, Air and Cyber Command (MACC) multi-domain force. [26]
- Discussions underway to establish a cyber forensic lab and to acquire equipment and training to enhance the competency across law enforcement agencies. This initiative is being funded by the British High Commission and should be implemented by April 2022.
- There is a proposal to provide cybersecurity as a service to law enforcement and of security entities aligned with the Ministry of National Security to improve and protect these entities and allow for information garnered by law enforcement to remain protected.

Barbados

- Plans to establish an Interpol branch.
- Participating in training and collaboration with CARICOM IMPACS and Council of Europe.

Antigua

- Police Force Cyber lab has been established.

[25] https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf
[26] https://www.jdfweb.com/maritime-air-and-cyber-command/

Regional

- In 2019, the Council of Europe[27] held the 'Regional Conference on Cybercrime Strategies and Policies and features of the Budapest Convention for the Caribbean Community' during which discussions were held regarding the possibility of creating a joint cyber forensics' lab that could be used by several countries and territories.
- The CARICOM Cyber Security and Cybercrime Action Plan (CCSCAP) identified 'Building Sustainable Capacity' and 'Technical Standards and Infrastructure' as two priority areas. Activities within these priority areas include support for member countries to:
    - Enhance training for judges and prosecutors in electronic evidence and cybercrime.
    - Training for law enforcement first responders, investigators, and prosecutors.
    - Increase the number of cyber forensic labs available.
- CARICOM Strategic Plan 2015-2019[28] outlined plans to explore the resources needed to develop equipment and infrastructure for the establishment of a CARICOM Cyber Crime Centre.

Skills Requirement

Such investments and targets for national security and criminal justice cybersecurity capacity development will require a range of upskilling and specialized training to ensure such actors can support and defend national interests and enforce and prosecute cybercrimes.

5. Strengthening incident response capabilities

Incident Response[29]

Incident response relates to governments and organizations' capacity to identify and resolve cyber-attacks and limit potential harms and consequences of such attacks. Computer Security Incident Response Teams (CSIRT) at the sectoral, national, and regional level typically take leadership roles in organizing, coordinating, and operationalizing such incident-response capabilities.

Caribbean Context

The importance of incident-response capabilities has been recognized across the Caribbean, with several countries already establishing their own CSIRTs, including Jamaica (JA-CIRT)[30], Guyana (CIRTGY)[31], and Trinidad and Tobago (TTCSIRT)[32]. However, there are a range of views on the respective roles of national CSIRTS, from a focus on awareness and training, to government incident management, private sector collaboration, data collection and reporting, and proactive defence and threat mitigation.

[27] https://rm.coe.int/3148-1-1-3-final-report-dr-reg-conference-cy-policies-caribbean-comm-1/168098fb6c
[28] https://caricom.org/documents/strategic-plan-caribbean-community-2015-2019/
[29] https://gcscc.ox.ac.uk/cmm-2021-edition
[30] https://www.cirt.gov.jm/
[31] https://cirt.gy/
[32] https://ttcsirt.gov.tt/

Examples of planned and ongoing activity include:

Jamaica

- Recommendations from the recent Consultant workshop for the development of the National Cybersecurity Strategy suggested:
    - o developing sectoral CIRTs to treat the incidents that do not meet the national incident threshold, while sharing the data with the National CIRT.
    - o that the government consider offering data storage facilities to store data from incidents that will be investigated later, requiring a dedicated budget and a policy mechanism to warehouse and provide data analytics.

Trinidad and Tobago

- The National Cyber Security Strategy identifies incident management as one of five key areas of focus to meet the country's objectives.

Regional

- CARICOM Strategic Plan 2015-2019[33], outlined plans to explore the establishment of a central CARICOM Emergency Response Team to provide support to CARICOM Member States in the investigation and prosecution of cybercrimes and support the establishment of National CSIRTs.
- World Bank Caribbean Digital Transformation Project 2020-2026[34] subcomponent 1.3 'Cybersecurity, Data Protection and Privacy: Legal and Regulatory Environment, Institutions, and Capacity' includes planned activities such as:
    - o Establishing a Computer Emergency Response Team (CERT) or a cybersecurity agency at the national level in line with a regionally agreed model and support for regional threat intelligence sharing, incident escalation, and support protocols (regional, DOM, GRE, SLU, SVG).

Skills Requirement

The dynamic cyber-threat landscape and planned national and regional investments and activities in strengthening incident-response capabilities will drive demand for skills to support threat identification and management, and the sharing of intelligence to protect organizations and governments from harm.

6. Adoption of security standards and controls

Security Standards and Controls[35]

Cybersecurity standards include international, national, and industry specific techniques and baseline requirements for cybersecurity good practices that can be implemented across public, private, and civil

[33] https://caricom.org/documents/strategic-plan-caribbean-community-2015-2019/

[34] https://documents1.worldbank.org/curated/en/848701593136915061/pdf/Dominica-Grenada-St-Lucia-St-Vincent-and-the-Grenadines-and-the-Organization-of-Eastern-Caribbean-States-Caribbean-Digital-Transformation-Project-Digital-Caribbean.pdf

[35] https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf

society sector organizations, including ICT Security Standards, Standards in Procurements, and Standards for the provision of Products and Services.

Security controls include physical, technological, and cryptographic security safeguards to assist organizations to mitigate the risks of cybersecurity threats with a range of internationally established cybersecurity frameworks which provide good practice guidance, such as NIST and COBIT.

Caribbean Context

The adoption and monitoring for compliance of security standards and controls across the Caribbean is still in its early stages. Some countries, including Jamaica and Barbados, are holding discussions and commencing planning regarding the development and adoption of security standards and controls across public sector organizations.

Examples of planned and ongoing activity include:

Jamaica[36]

- Operationalizing the National ICT Authority.
- Finalization of the ICT Policies, Standards and Guidelines (PSG) Manual for Public Sector Entities.
- Promotions of compliance with the NIST framework and in the long-term ISO 27001.
- Encourage ISPs to strengthen policies for the deployment of technical controls as a part of their services, particularly to Micro, Small and Medium Sized Enterprises (MSMEs).
- Facilitate the tailoring of technical standards by collaborating with the relevant sectoral stakeholders, particularly from a resourcing and investment standpoint.
- Promotion of the use of Cryptographic controls to encourage entities to put in place measures that ensure data is protect in transit and at rest.
- Recent formation of the Public Procurement Commission and developments in the standardization of procurement in general.
- Promotion of domestic providers of cybersecurity products and mitigating dependency on foreign cybersecurity technologies.

Barbados

- Review of policies and operational practices currently being conducted.
- Discussions with Barbados' National Standards Institute to develop home grown equivalent to UK's Cyber Essentials and Cyber Essentials Plus.

Regional

- The CARICOM Cyber Security and Cybercrime Action Plan (CCSCAP) identified ‘Technical Standards and Infrastructure’ as one of five priority areas. Activities within this focus area include support for member countries to:
    - Implement international standards in the configuration of networks.
    - Adopt and comply with ISO Standards (including training).
    - Adopt a top-down approach to policy development and include civil society and the internet society in setting standards.

[36] Review of the 2015 National Cyber Security Strategy of the Government of Jamaica

Skills Requirement

As countries in the Caribbean adopt, develop, and promote the use of security standards and controls there will be a skills requirement to implement such standards and controls as well as developing the capacity and capability to monitor compliance.

7. Improving national and regional collaboration

National and Regional Collaboration[37]

The multi-faceted and transnational nature of cybersecurity and cybercrime threats requires countries to foster both internal and external collaborative approaches and mechanisms. This can include domestic based cooperation between government, CNI operators, and the private sector, as well as supporting strong international networks and relationships with foreign law enforcement and national security counterparts.

Caribbean Context

Domestic collaboration in response to cybersecurity and cybercrime issues in the Caribbean is currently characterized by informal domestic initiatives either led by government or within critical sectors such as banking and finance. At the regional level, CARICOM IMPACS provides a forum for regional cybersecurity collaboration alongside several other regional and international organizations, such as the Organization of American States, Council of Europe, UK FCDO, ITU, and World Bank, which have initiated regional dialogues and collaboration on cybersecurity issues.

Examples of planned and ongoing activity include:

Jamaica

- Plans to strengthen government partnerships with Telecommunication Providers to improve the resilience of the infrastructure and the reliability of the service provided.

Guyana

- The National Green State Development Strategy: Vision 2040[38] identifies Policy Recommendations for Knowledge Management and ICT that include the need for investment in modern data systems and encouragement of inter-agency/sectoral collaboration and planning around information sharing.

Trinidad and Tobago

- The National Cyber Security Strategy[39] defines Collaboration as one of five key areas of focus which includes the establishment of public-private/civil society partnership in securing Trinidad and Tobago's cyber infrastructure, as well as the promotion of cooperation with international organizations.

[37] https://gcscc.ox.ac.uk/cmm-2021-edition
[38] https://observatorioplanificacion.cepal.org/en/plans/green-state-development-strategy-vision-2040-guyana
[39] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/TrinidadandTobagoNationalCyberSecurityStategyEnglish.pdf

Regional

- The CARICOM Cyber Security and Cybercrime Action Plan (CCSCAP) identified 'Regional and International Cooperation' as one of five priority areas. Activities within this focus area include:
  - Expanding the role of CARICOM IMPACS Regional Intelligence Fusion Centre (RIFC) to improve cybersecurity and cybercrime monitoring and intelligence analysis.
  - Establishing a Regional Cyber Committee (RCC) to support the RIFC and bring together National Cyber Points of Contact (RCPOC) from each participating territory and provide an effective mechanism that will aid in the coordination of projects.
  - Supporting improved informal international cooperation between law enforcement agencies.

Skills Requirement

To support domestic, regional, and international cyber collaboration efforts there will be a skills requirement to safely facilitate information sharing between various actors, as well as needs for cyber diplomacy, and understanding of the interoperability of technologies and systems to be effective within and across organizations, sectors, countries, and regions.

8. Responding to the role of research and development

Research and Development[40]

Research and development include the exploration of cybersecurity ideas, products, and services to address emerging technological and societal challenges in order to advance the development of cybersecurity knowledge and capabilities that meet national requirements.

Emerging Technologies

In presenting its 2020 report on top emerging technologies, the World Economic Forum (WEF)[41] noted that:

> *"during the last two decades, the world has witnessed an unprecedented pace of technological innovation in all fields, from computing and artificial intelligence to biotechnology and nanotechnology. These technologies come with a potential to help us solve some of our most pressing global challenges, but also pose significant risks, if misused and mismanaged."*

Caribbean Context

When government and industry leaders from the Caribbean were asked which emerging technologies were expected to play important roles within key sectors and wider society, the top five responses include:

1. Cryptocurrencies (86%)
2. Internet of Things (76%)
3. Artificial Intelligence (72%)
4. Blockchain (62%)
5. 5G (59%)

[40] https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf
[41] https://www.weforum.org/reports/top-10-emerging-technologies-2020

There has been some acknowledgement in the region that the associated emerging security issues that come with such technologies will need to be addressed in a way that does not exacerbate existing digital divides across the region.[42]

This need for investment in research and development to leverage these emerging technologies to serve the needs of the Caribbean specifically appears to still be in the early stages.

Examples of planned and ongoing activity include:

Jamaica

- The Jamaican government has recognized the role of emerging technologies as part of the Vision 2030 National Development Plan[43] including utilizing emerging technologies to reduce dependency on fossil fuels and contribute to the development of a green economy.

- A review of the national cybersecurity strategy[44] identified research and development opportunities as part of future national capacity building efforts, including the provision of funding and research opportunities from national stakeholders and international partners, to develop this area of expertise.

- A Central Bank Digital Currency Pilot.[45]

Barbados

- Fish farmers are using 3D printing to make feeding devices and other prototypes. In this instance, technology is enabling the operation to become more sustainable. [46]

Trinidad and Tobago

- A pilot system using blockchain to trace the quality of cocoa is being explored.[47]

- The National Cyber Security Strategy details that Research and Development (R&D) in cybersecurity will be encouraged in order to build capacity and maintain a resilient knowledge base.

Regional

- In 2018, the Caribbean-Central American Action in partnership with Mastercard and the Inter-American Bank hosted the 'Caribbean Smart Islands' Forum[48] to discuss how public and private entities can partner in the digital payments ecosystem to generate economic growth in the Caribbean.

- CARICOM Strategic Plan 2015-2019[49] includes 'Enabling Resilience: Coordinated Foreign and External Relations and Research and Development and Innovation' as one of seven strategic priorities. Activities related to this priority include:

[42] https://publications.iadb.org/publications/english/document/2020-Cybersecurity-Report-Risks-Progress-and-the-Way-Forward-in-Latin-America-and-the-Caribbean.pdf
[43] https://sustainabledevelopment.un.org/content/documents/1501jamaica.pdf
[44] Consultant workshop for the development of the National Cybersecurity Strategy
[45] https://boj.org.jm/boj-mints-first-batch-of-jamaicas-central-bank-digital-currency/
[46] https://www.caribank.org/sites/default/files/publication-resources/Keynote%20Address_President_Aldith%20Brown%20Memorial%20Lecture-ECCB_20191119.pdf
[47] https://www.caribank.org/sites/default/files/publication-resources/Keynote%20Address_President_Aldith%20Brown%20Memorial%20Lecture-ECCB_20191119.pdf
[48] https://blogs.iadb.org/caribbean-dev-trends/en/8721/
[49] https://caricom.org/documents/strategic-plan-caribbean-community-2015-2019/

- Advocating for resources (state and private sector) to finance R&D in business development.
- Facilitating an enabling legislative environment for R&D and Innovation e.g., protection of intellectual property, incentives for the private sector, incentives for innovation which capitalize on indigenous knowledge and resources.
- Identifying and promoting opportunities for functional cooperation in R&D and Innovation.
- Advocating for national school-based programmes (primary, secondary, and tertiary) that drive, enable and reward R&D and Innovation.

Skills Requirement

To enable the fast adoption of new technologies to ensure they can play a positive economic role for the region, there will be a need to invest in and develop national Research and Development capabilities to best understand how such technologies can be leveraged to suit the requirements of the Caribbean region. This will create a need for cybersecurity skills to help understand and manage the associated risks to harness and protect the value of these new innovations.

Conclusion

The thematic areas identified as strategic drivers provide an insight into the strategic forces in the Caribbean region that are driving needs for certain skills requirements to ensure that such activities and capabilities can be deployed securely.

Such strategic drivers were analyzed to inform the Future Workforce Assessment so that the design of future-skills provision in Jamaica and the Caribbean region will be focused on areas that will best facilitate the delivery of capacity building targets, mitigate risks, and support the enforcement and compliance of related legislation and regulation.

Chapter 2

Future Workforce Assessment

Introduction

This Future Workforce Assessment report provides an analysis of the eight strategic drivers identified in Chapter 1 in order to extrapolate the technical cybersecurity job roles and additional cybersecurityskills that Jamaica and the Caribbean region will require in order to facilitate the delivery of capacity building targets and mitigation of risks, and support the enforcement and compliance of related legislation and regulation. This includes extrapolating requirements for:

- interventions to build national capacity maturity.
- establishment of cybersecurity workforce teams/units/functions.
- identifying required technical cybersecurity job roles.
- identifying additional cybersecurity skills required for the non-specialist workforce.

This process is illustrated in Figure 2 below. Figure 2 also details how the Future Workforce Assessmentwill be utilized in forthcoming chapters to identify the cybersecurity courses and certifications to address the training needs of the region.

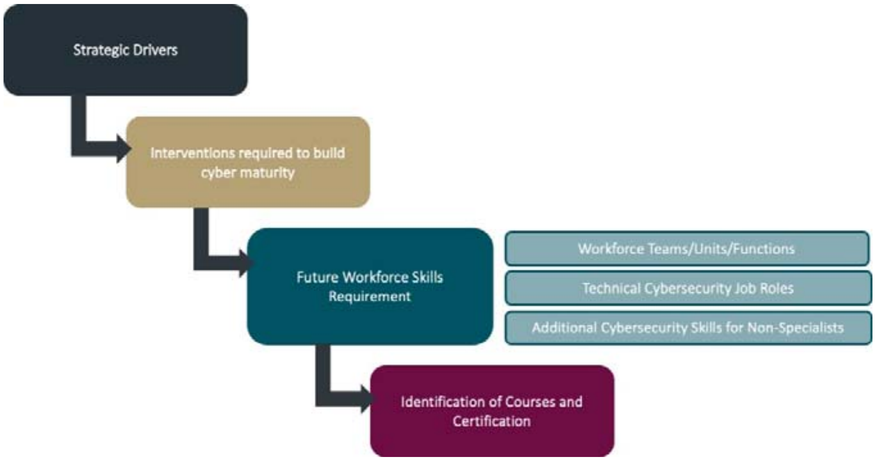

Strategic Drivers
Interventions required to build cyber maturity
Future Workforce Skills Requirement
Workforce Teams/Units/Functions
Technical Cybersecurity Job Roles
Additional Cybersecurity Skills for Non-Specialists
Identification of Courses and Certification

Figure 2

In order to assist with identifying interventions that will likely be required to increase national and regional cybersecurity capacity maturity and reduce the risk in responses to the eight strategic drivers,the dimensions of Oxford Cybersecurity Capacity Maturity Model for Nations (CMM)[1] are utilized to guide what capacity and capability will need to look like at these higher levels of maturity.

- CMM: “helps nations understand what works, what does not work and why, across all areas of cybersecurity capacity. This is important so that governments and enterprises can adopt policies and make investments that have the potential to significantly enhance safety and security in

[1] https://gcscc.ox.ac.uk/cmm-2021-edition

cyberspace, while also respecting human rights, such as privacy and freedom of expression." Further details on the CMM provided in *Appendix F*.

There are a number of established cybersecurity workforce and skills frameworks that provide valuableguidance on the range of cybersecurity knowledge areas, team functions, job roles and competencies required to establish a robust and resilient cybersecurity capability. Three such frameworks include:

- The Cyber Security Body of Knowledge (CyBOK)[2]: "aims to codify the foundational and generally recognised knowledge on cyber security...and is meant to be a guide to the body of knowledge; the knowledge that it codifies already exists in literature such as textbooks, academic research articles, technical reports, white papers, and standards. Its focus is on mapping established knowledge and not fully replicating everything that has ever been written on the subject. Educational programmes ranging from secondary and undergraduate education to postgraduate and continuing professional development programmes can then be developed on the basis of CyBOK." Further details on CyBOK provided in *Appendix F*.

- Saudi Cybersecurity Workforce Framework (SCyWF)[3]: provides an updated (2020) version of the NICE framework using a similar taxonomy to NICE. It has updated NICE job roles that reflect new challenges such as cloud and artificial intelligence and a simpler structure that emphasizes those roles that are most frequently required across government and critical infrastructure. The full list of SCyWF job roles is provided in *Appendix F*.

- Workforce Framework for Cybersecurity (NICE Framework)[4]: "provides a set of building blocks fordescribing the tasks, knowledge, and skills that are needed to perform cybersecurity work performed by individuals and teams. Through these building blocks, the NICE Framework enables organizations to develop their workforces to perform cybersecurity work, and it helps learners to explore cybersecurity work and to engage in appropriate learning activities to develop their knowledge and skills."

The analysis of strategic drivers in this report draws upon and adapts these frameworks in order to identify future workforce requirement. It classifies the requirement using the SCyWF job role categories.

Future Workforce Analysis of Strategic Drivers

The analysis table detailed below provides a high-level view of how the eight strategic driver thematic areas link to future capacity maturity and risk reduction activity, and the associated cybersecurity job roles required to support such activity. A summary of the skills requirement information from this this analysis is provided below.

[2] https://www.cybok.org/

[3] https://nca.gov.sa/files/scywf_en.pdf

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

Cybersecurity Workforce Units, Teams or Functions

In order for Jamaica and the Caribbean region to reach its digital transformation and cybersecuritycapacity development ambitions, it will require a range of cybersecurity workforce units, teams or functions to facilitate and secure such activity. Based on the analysis of the strategic drivers, the following such workforce units, teams and functions have been identified to fulfil such requirements:

Strategic Driver	Workforce Units/Teams/Functions
1. Acceleration of nationaland regional digital transformation efforts	• eGovernment Providers • eCommerce Providers • ISPs • Internet Infrastructure Operators. • Government agency responsible for addressing disinformation.
2. Critical national infrastructure protection	• CNI Operators/assets • ISPs • Government agency responsible for monitoring and compliance of CNIoperators/assets. • National CIRTs • Sectoral CIRTs
3. Enforcement and compliance with national cybersecurity legislative and regulatory agendas	• National Telecommunications/ICT Regulator • Sector Specific Regulators • Government agency responsible for overseeing cybersecurity compliance. • Government agency responsible for data protection. • CNI operators and other regulated entities.
4. Capacity building in national security and thecriminal justice system	• Police Force • Prosecutors • Courts and Judges • Defence Force / Cyber Command
5. Strengthening incidentresponse capabilities	• National CIRTs • Sectoral CIRTS • CNI Operators • ISPs • Units responsible for cybersecurity/SOC within: o Government Ministries/Departments o Private Sector Organisations o Civil Society Organisations
6. Adoption of securitystandards and controls	• ISPs • CNI Operators • Defence Force / Cyber Command • National Standards Agencies • Units responsible for cybersecurity/SOC within: o Government Ministries/Departments o Private Sector Organisations o Civil Society Organisations

Strategic Driver	Workforce Units/Teams/Functions
7. Improving national and regional collaboration	• National CIRTs • Sectoral CIRTs • Regional CIRTs • Transnational Crime and Law Enforcement Units • Defence Force / Cyber Command • Units responsible for cybersecurity/SOC within: o Government Ministries/Departments o Private Sector Organisations • Civil Society Organisations
8. Responding to the role of research and development	• National Telecommunications/ICT Regulator • National Research and Innovation Institutes • Units responsible for cybersecurity/SOC within: o Government Ministries/Departments

Additional Cyber Security Workforce Requirements

In addition, the increasing cybersecurity threats faced by all these organisations as well as the growth in their cybersecurity role and responsibilities implied by the strategic drivers, suggests that each organization or type of organization on this list should also develop cybersecurity awareness across its whole workforce, ensure all managers understand basic cybersecurity principles and how to apply policies, and enable all senior executives to develop and apply cybersecurity strategies and embed an organizational cybersecurity culture. In addition, all are likely to need to add knowledge ofnetwork security, information security management principles, common threats and how they seek to exploit system, network and human vulnerabilities, as well as basic response and investigation techniques to their IT departments' skillsets.

All sectors and organisations listed above	• Senior Executives who can develop organisational cybersecurity strategies and culture; • Managers who understand security principles and apply security policies; • IT staff with knowledge of: o Information security management principles o Hacker techniques o Incident response and investigation o Network security • All staff have a general understanding of how to keep themselves, organisational assets and their families safe in cyberspace.

Conclusion

The future workforce needs identified in this report provide an understanding of the technical cybersecurity workforce job roles and associated skills required across all involved organisations for Jamaica and the Caribbean region to fulfil their digital transformation and cybersecurity capacity development ambitions and respond to and mitigate the risk from the growing cyber threat landscape. Through establishing this demand-side element of the cybersecurity workforce ecosystem, it is now possible to determine the education and training supply-side elements that will be required to service such demand.

The next stage of the Training Needs Assessment includes a market assessment of reports covering the current cybersecurity skills base and training capability and capacity in Jamaica and the Caribbean region.

Combining the findings of the future workforce assessment and market assessment will then informthe gap assessment to understand how the proposed Cyber Academy can best address any cybersecurity workforce supply and demand deficits.

Chapter 3

Market Assessment

Summary

The Market Assessment report examines the existing cybersecurity skills development market in Jamaica and the wider Caribbean region. The report assesses a range of public and private sector businesses and initiatives, as well as educational institutions, and international service providers that provide cybersecurity training and certifications in the region.

The Market Assessment found that Trinidad and Tobago possess the most developed cybersecurity strategy in the region, followed by Jamaica and Barbados when reviewed against the Cybersecurity Capacity Maturity Model for Nations Dimension 1. However, the majority of private sector entities and educational institutions offering cybersecurity training services are located in Jamaica.

Most cybersecurity training providers did not offer sector specific training, and the majority of them fall under the private sector. These companies appear primarily to be selling external courses and facilitating the supply of training course resources, though they do also provide access to a wide range of cybersecurity certifications.

The governments of Jamaica, Guyana, and Trinidad and Tobago have established cybersecurity initiatives which primarily offer cybersecurity response services. While, the public sector entities do not offer specific training services, they possess initiatives aimed at promoting cyber skills education and raising awareness of cyber threats amongst the local populations.

Alongside the private and public sectors, there are several educational institutions which offer cybersecurity training courses. These include short courses, as well as more formal university degrees.

Finally, there are a number of established international consultancies which offer cybersecurity training in the Caribbean which have been operating for several years. These companies provide support to both government and private companies. However, limited information regarding their strategy and costs were made available.

Further information regarding cost and length of courses and certifications is needed to assess best options in terms of cybersecurity capability development in Jamaica.

Methodology

- Research was carried out using open-source resources and data gathered through PGI's market research report which was carried out in the earlier stages of the project.

- Open-source resources included company websites, academic journals focused on cybersecurity in the region, government websites, and news reports of cyber academy openings.

- Keywords/ phrases were used to find resources such as:
  - Cybersecurity training
  - Caribbean cybersecurity market
  - Cyber threats in the Caribbean

- Key sources included but were not limited to, publications by the Inter-American Development Bank, Organization of American States, and the Global Cyber Security Centre at the University of Oxford.

Market Assessment

Background

Region

While some Caribbean governments and companies have begun to recognise the importance of investing in cybersecurity strategies that would protect against cyber threats and foster economic and social prosperity, there are still few relevant laws and limited capacity to respond to these threats.[50] Government services, banking and financial services, and private sector operations still require updated testing systems and essential infrastructure.

It should be a strategic priority for Caribbean governments to invest in cybersecurity. LATAM and the Caribbean is the fourth largest mobile phone market, where half of the population uses the internet and includes countries with citizens who make 100 per cent of purchases via telephone.[51] In 2016, the cost of cybercrimes was estimated at USD90bn for the Latin America and the Caribbean regions.[52] In 2019, the cybersecurity market in Latin America and the Caribbean was valued at almost USD13bn. It is estimated that between 2020 and 2025, the overall market will grow at an annual rate of around 14 per cent and be worth over USD26bn by 2025.[53] The high cost of cyber threats, coupled with the potential market value, highlight the importance of investing in cybersecurity strategies and capabilities.

PGI's assessment of the cybersecurity market in the Caribbean concluded that Trinidad and Tobago was by far ahead in terms of capabilities and understanding of cybersecurity.[54] Notably, in 2017, Trinidad and Tobago launched a cybersecurity capacity building workshop for secondary and tertiary students and professionals to learn cybersecurity basics.[55] Close behind Trinidad and Tobago, in terms of their cybersecurity strategies, are Jamaica and Barbados.[56] While Antigua, The Bahamas, Dominica, Haiti, and Suriname are in the process of drawing up strategies, there is no indication of when these will be developed.

In an attempt to increase their ability to detect and respond to cyber-attacks, Jamaica, Barbados, and Trinidad and Tobago partnered with the International Telecommunication Union (ITU) in 2013 and introduced a National Computer Incident Response Team (CIRTs).[57] This is important as it ensures cooperation between the private and public sector in regards to sharing information and responses to

[50] https://www.caribbean-council.org/action-needed-address-caribbean-cyber-security/
[51] https://www.caribbean-council.org/action-needed-address-caribbean-cyber-security/
[52] https://www.researchgate.net/publication/326414375_The_Development_of_Cybersecurity_Policy_and_Legislative_Landscape_in_Latin_America_and_Caribbean_States
[53] https://www.statista.com/statistics/1180184/value-cybersecurity-market-latin-america/
[54] https://www.caribbean-council.org/action-needed-address-caribbean-cyber-security/
[55] https://metron.services/f/cybersecurity-capacity-building-initiative-for-trinidad-tobago
[56] https://www.researchgate.net/publication/326414375_The_Development_of_Cybersecurity_Policy_and_Legislative_Landscape_in_Latin_America_and_Caribbean_States
[57] https://www.researchgate.net/publication/326414375_The_Development_of_Cybersecurity_Policy_and_Legislative_Landscape_in_Latin_America_and_Caribbean_States

breaches.[58] Regional cooperation is key to enhancing cybersecurity capabilities and strategies across the region.

Jamaica

The growth of a 'technology-enabled society' and a population with high levels of digital skills is central to the Jamaican government's digital services strategy. Here, the government aims to significantly increase the number of employees in the digital services sector from around 40,000 to 70,000 by 2025.[59]

The government's ambitious vision for its cybersecurity workforce will be supported by a growing cybersecurity skills development market. The publication of the country's first National Cyber Strategy in 2015 marked the start of this process. The strategy set the foundations for the establishment of a national framework built around four key areas: Technical Measures; Human Resource and Capacity Building; Legal and Regulatory; and Public Education and Awareness.[60]

The strategy invited a wide range of companies and initiatives to provide cybersecurity skills development training in Jamaica. These include both private sector and public sector entities, as well as educational institutions such as universities and colleges.

As a result, Jamaica's cybersecurity capabilities have improved in recent years. The UN's International Telecommunication Union ranked the island 15th out 35 countries in the Americas and gave Jamaica an overall score of 32.53 out of 100 in its 2020 Global Cybersecurity Index. The report states that Jamaica's area of relative strength is its Legal Measures, and its area of potential growth is its Technical Measures.[61]

Existing Companies and Initiatives in the Rest of the Caribbean

Barbados

Advantage Caribbean Institute

The Advantage Caribbean Institute offers corporations, small businesses and individual students training in areas of information technology, management and general career development. It is headquartered in Barbados.[62]

In regard to cyber security training, the institute uses certification courses carried out by Mile2 based in the US. The courses teach the fundamental and advanced principles of cybersecurity, including penetration testing, disaster recovery, incident handling and network forensics.[63]

[58] https://assets.kpmg/content/dam/kpmg/bb/pdf/2019/11/cybersecurity_and_trust_in_the_caribbean.pdf
[59] https://jis.gov.jm/ministry-moving-ahead-to-implement-five-year-global-digital-services-strategy/
[60] https://www.mset.gov.jm/wp-content/uploads/2019/09/Jamaica-National-Cyber-Security-Strategy-2015.pdf
[61] https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf
[62] https://advantagecaribbean.com/contact-us/
[63] https://advantagecaribbean.com/cyber-security/

They also offer a range of other security courses such as C)DRE Certified Disaster Recovery Engineer, C)ISSM Certified Information Systems Security Manager, C)ISSO Certified Information Systems Security Officer, C)PEH Certified Professional Ethical Hacker, C)PTE Certified Penetration Testing Engineer, C)SS Certified Security Sentinel, C)VA Vulnerability Assessor, Certified Information Systems Security Professional (CISSP) and CompTIA Security+. Users can register interest on the website but details regarding costs are not made available. All the course lengths range from 2 to 5 days.[64]

Guyana

CIRT.GY

CIRT.GY is the public arm of the Guyana National Computer Incident Response Team (GNCIRT) The team was formed by the Government of Guyana in January 2013 and now operates under the purview of the National Data Management Authority (NDMA) within the office of the Prime Minister.[65]

CIRT.GY provides computer incident management and is the national point of contact on cybersecurity issues for international agencies in Guyana and the Government of Guyana.[66]

They do not offer any cybersecurity courses to the public but host a range of resources on their website including a four-week awareness curriculum for cybersecurity issues as part of Cybersecurity Awareness Month.[67]

Zara Cyber Security Centre

The Zara Cyber Security Centre is a joint collaboration between the Guyana Police Force (GPF) and the Zara Group that was launched in 2017. The center was established to boost the police force's ability to tackle cybercrimes as well as provide free training of community members in information technology.[68] The center does not have its own website, and details of how the training operates does not seem to be available.

Trinidad & Tobago

Trinidad and Tobago Cyber Security Incident Response Team

The Government of Trinidad and Tobago, through the Ministry of National Security, established the Cyber Security Incident Response Team (TTCSIRT) in November 2015 with the assistance of the Organization of American States (OAS) and the International Telecommunications Union (ITU). The establishment of the response team is an objective of Trinidad and Tobago's 2015 National Cyber Security Strategy.[69]

[64] https://advantagecaribbean.com/course-catalogue/region-BR/cat-4-security/
[65] https://cirt.gy/about
[66] https://cirt.gy/about
[67] https://cirt.gy/node/660
[68] https://guyanatimesgy.com/zara-cybersecurity-centre-launched-at-police-college/
[69] https://ttcsirt.gov.tt/background/

The mission of the response team is to provide technical assistance to the Government and other stakeholders within the national framework and build capabilities in managing cyber threats and enhance cyber security capabilities.[70]

The core services they offer include education and training, but their website does not detail how the training is carried out or if this is available to the public.[71]

Cyber Security & Anti-Crime Services (CSACS)

CSACS is a cyber security and anti-crime training and investigations agency that provides law enforcement training and consultancy services throughout Trinidad and Tobago. They offer training in cyber security and cybercrime investigations. CSACS' trainers are all former members of the protective services of Trinidad and Tobago, including the Trinidad and Tobago Police Service and Defence Force.[72] Their website does not provide any details regarding course length or cost.

The University of Trinidad and Tobago

The University of Trinidad and Tobago is a state-owned university established in 2004. It started as a university focused on providing programs in engineering and technology.[73]

The university offers a Master of Science in Cybersecurity, which aims to provide students with the skills to prevent, counter, and recover from cybercrimes and attacks. Students are given two options to focus on: (1) Hacking and Cybercrime Investigation, (2) Cybersecurity Management, Law and Policy.[74]

The course is only available as evening classes and takes 1.5 years to complete full time and 2.5 years to complete part time.

Tuition fees for the 2020-2021 academic year for the course were TT16,800 full time for Trinidad and Tobago nationals, USD3,200 full time for CARICOM/ OECS nationals and USD6,400 for international students.[75]

University of West Indies, (St Augustine Campus) Trinidad and Tobago

Starting as a university college of Jamaica in 1948, UWI has evolved into a modern, future driven activist, top ranked academy with over 50,000 students with campuses in Jamaica, Trinidad and Tobago, Barbados, Antigua and Barbuda, and also accommodates regional provision of training online. While they do not offer specific cybersecurity programmes at graduate or undergraduate level the University offers several undergraduate and graduate computer science programmes across most of its campuses[76]. The campus in Trinidad and Tobago, provides a training workshop for students in

[70] https://ttcsirt.gov.tt/mission-vision-core-values/
[71] https://ttcsirt.gov.tt/core-functions/
[72] https://www.csacstt.com/home.html
[73] https://utt.edu.tt/index.php?page_key=7&main=1
[74] https://utt.edu.tt/?wk=1&programmes=1&utt_programme_key=157
[75] https://my.utt.edu.tt/uploads/rev_fees_booklet.pdf
[76] https://www.mona.uwi.edu/programmes/search?name=Computer+Science

Cybersecurity Fundamentals[77] and a Cybersecurity Concepts Bootcamp for students in secondary school and those entering undergraduate programmes[78].

Conclusion

The cybersecurity skills development market in Jamaica and the Caribbean is made up of primarily private sector entities, as well as educational institutions. PGI identified just one public sector institution that offers cybersecurity skills development services: the Jamaica Cyber Incident Response Team. Though the JaCIRT does not offer cybersecurity training, rather it focuses its cybersecurity skills development on spreading awareness of the importance of cybersecurity skills across the island.

Existing private sector entities that provide cybersecurity training are mainly IT consultancies, which offer training as part of a wider IT solutions offering. These companies appear to be primarily selling external courses and facilitating the supply of training course resources, allowing students to undertake self-study. However, these private sector entities do provide access to a wide range of cybersecurity certifications.

There are also several educational institutions that provide cybersecurity training in Jamaica. These institutions offer a range of short cybersecurity courses and longer university degrees. Both types of courses offer a comprehensive training in a range of cybersecurity skills.

International companies such as PwC and KPMG have a considerable presence in the Caribbean and offer a wide range of support to cyber businesses. Limited information is available regarding cost and length of courses or certifications, but their standing as well-known companies increases the likelihood that they have a wide array of resources available.

[77] https://sta.uwi.edu/fst/dcit/content/csx-cyber-security-fundamentals-training-workshop
[78] https://sta.uwi.edu/fst/dcit/bootcamp

Chapter 4

Gap Assessment

Introduction

This Gap Assessment report considers the combined findings presented in the previous chapters from the Future Workforce Assessment (Chapter 3) and Market assessment (Chapter 4) in order to understand the gap between the anticipated skill requirements and current skills and training capability and capacity in Jamaica and the Caribbean region. This gap assessment is an important step that will inform the design of the curriculum and commercial model for the proposed Cyber Institute and will help to minimize duplication of effort and address current and expected future cybersecurity education and training gaps in Jamaica and the Caribbean.

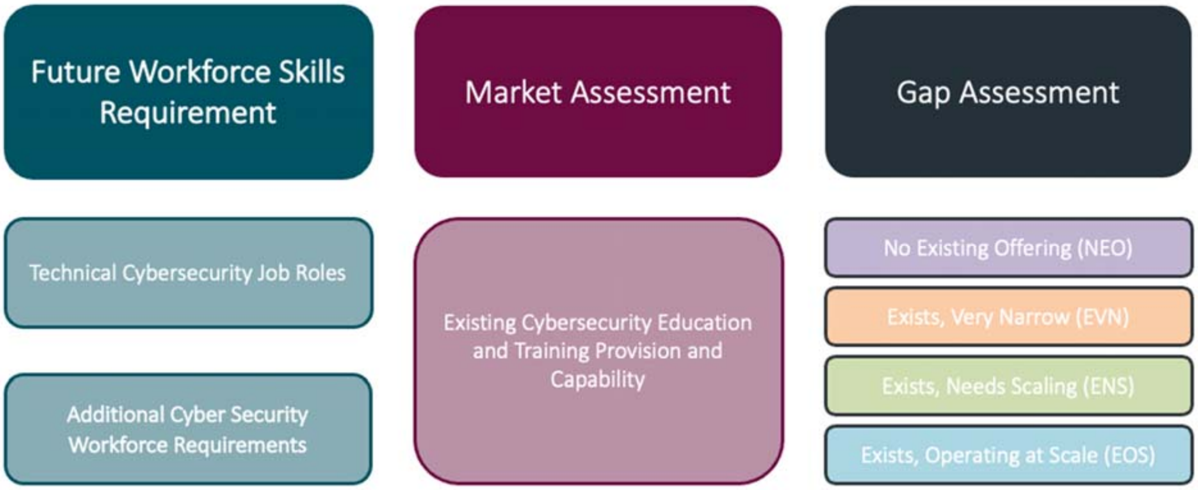
The gap assessment was completed by firstly isolating the overlapping Technical Cybersecurity Job Roles and additional Cyber Security Workforce Requirements identified in the Future Workforce Assessment. This resulted in 36 different technical cybersecurity job roles being identified.

Secondly, the range existing education and training offerings and capabilities identified in the Market Assessment (both regional and international provisions where applicable) were mapped against each of the different technical cybersecurity job roles and additional cyber security workforce requirements.

Lastly, a gap assessment was completed for each of the different Technical Cybersecurity Job Roles and additional Cyber Security Workforce Requirement areas to determine the extent to which cybersecurity education and training provisions and capabilities existed in the Jamaican and Caribbean Market. Table 1 below details the rating system used in the gap assessment.

Table 1 - Gap Assessment Rating Criteria

Gap Assessment Rating	Description
No Existing Offering (NEO)	The market assessment was unable to identify any existing cybersecurity education and training provisions or capabilities to support skills development in this area.
Exists, Very Narrow (EVN)	The market assessment identified existing cybersecurity education and training provisions or capabilities to support skills development in this area. However, such offerings and capabilities are very narrow and would unlikely be sufficient to support the expected future workforce and skills requirement.
Exists, Needs Scaling and External Validation (ENS)	The market assessment identified existing cybersecurity education and training provisions or capabilities to support skills development in this area. Such offerings and capabilities are suitable to support expected future workforce and skills requirement, however, increase scale and independent external validation is required to support future demand and interoperability
Exists, Operating at Scale (EOS)	The market assessment identified existing cybersecurity education and training provisions or capabilities to support skills development in this area. Such offerings and capabilities are suitable, and externally validated to support expected future workforce and skills requirement and additional education and training provisions are not required.



Future Workforce Skills Requirement

Technical Cybersecurity Job Roles

Additional Cyber Security Workforce Requirements

Market Assessment

Existing Cybersecurity Education and Training Provision and Capability

Gap Assessment

No Existing Offering (NEO)

Exists, Very Narrow (EVN)

Exists, Needs Scaling (ENS)

Exists, Operating at Scale (EOS)

Figure 3

Gap Assessment

Technical Cybersecurity Job Roles

Table 2 below details the mapping of market offerings to identified job roles, with an assessment of the provision taking into consideration external validation of the training provision. The exercise evidences the limited provision of cybersecurity technical training regionally with access to international and remote provision where applicable.

Table 2.1 - Mapping and Gap Assessment of Technical Cybersecurity Roles with Market Offerings According to the Gap Assessment Rating

Gap assessment	Specialty area	Job role	Market offering
ENS	Governance, Risk and Compliance (GRC)	Compliance Officer	PM Solutions Jamaica • CompTIA Security • COBIT 5 Advantage Caribbean Institute • CompTIA Security+ Caribbean Cyber Security and Privacy Association (The Caribbean CSPA) • CompTIA Security+ SY0-601 Unichrone • COBIT5
	Governance, Risk and Compliance (GRC)	Cybersecurity Auditor	PM Solutions Jamaica • CompTIA Security Advantage Caribbean Institute • CompTIA Security+ Caribbean Cyber Security and Privacy Association (The Caribbean CSPA) • Caribbean Certified Data Protection Auditor • CompTIA Security+ SY0-601

Gap assessment	Specialty area	Job role	Market offering
	Cybersecurity Architecture (CA)	Cybersecurity Architect	Advantage Caribbean Institute • Certified Information Systems Security Professional (CISSP)
	Incident Response (IR)	Incident Responder	PM Solutions Jamaica • CompTIA Security Advantage Caribbean Institute • Certified Disaster Recovery Engineer • Vulnerability Assessor • CompTIA Security+ Caribbean Cyber Security and Privacy Association (The Caribbean CSPA) • CompTIA Security+ SY0-601
EVN	Governance, Risk and Compliance (GRC)	Risk Officer	PM Solutions Jamaica • COBIT 5 Unichrone • PMI Risk Management Professional • COBIT5
	Laws and Data Protection (LDP)	Cybersecurity Legal Specialist	Cyber Security & Anti-Crime Services (CSACS) • Cybersecurity and cybercrime investigations training Caribbean Cyber Security and Privacy Association (The Caribbean CSPA) • Caribbean Certified Cyber Crime Professional
	Laws and Data Protection (LDP)	Data Protection Officer	Caribbean Cyber Security and Privacy Association (The Caribbean CSPA) • Caribbean Certified Data Protection Professional • Certified Data Protection Officer • Caribbean Certified Data Protection Auditor Symptai Consulting • Information and Privacy
	Cybersecurity Architecture (CA)	Secure Cloud Specialist	PM Solutions Jamaica • Cloud computing security

Gap assessment	Specialty area	Job role	Market offering
	Cybersecurity Research and Development (CRD)	Secure Software Assessor	Advantage Caribbean Institute • Certified Information Systems Security Professional (CISSP)
	Cybersecurity Research and Development (CRD)	Systems Security Development	PM Solutions Jamaica • Information Systems Security
	Defense (D)	Cyber Defence Analyst	Advantage Caribbean Institute • Vulnerability Assessor
	Incident Response (IR)	Cybercrime Investigator	Cyber Security & Anti-Crime Services (CSACS) • Cybersecurity and cybercrime investigations training Caribbean Cyber Security and Privacy Association (The Caribbean CSPA) • Caribbean Certified Cyber Crime Professional
	Protection (P)	Identity and Access Management Specialist	Advantage Caribbean Institute • Vulnerability Assessor • Certified Information Systems Security Professional (CISSP)
	Protection (P)	Systems Security Specialist	PM Solutions Jamaica • Information Systems Security • Information System Auditing Advantage Caribbean Institute • Certified Information Systems Security Manager (CISSM) • Certified Information Systems Security Officer (CISSO) • Vulnerability Assessor
	Vulnerability Assessment (VA)	Penetration Tester	Symptai Consulting • Ethical Hacking PM Solutions Jamaica • Ethical Hacking Advantage Caribbean Institute • Certified Professional Ethical Hacker (CPEH) • Certified Penetration Testing Engineer (CPTE)

Gap assessment	Specialty area	Job role	Market offering
			Caribbean Cyber Security and Privacy Association (The Caribbean CSPA) • EC-Council CEH V10
	Vulnerability Assessment (VA)	Vulnerability Assessor	PM Solutions Jamaica • Information System Auditing • CompTIA Security Advantage Caribbean Institute • CompTIA Security+ Caribbean Cyber Security and Privacy Association (The Caribbean CSPA) • CompTIA Security+ SY0-601
NEO	Governance, Risk and Compliance (GRC)	Policy Officer	
	Leadership (L)	Chief Information Security Officer	
	Workforce Development (WD)	Cybersecurity Instructors	
	Workforce Development (WD)	Instructional Curriculum Developer	
	Cybersecurity Research and Development (CRD)	Cybersecurity Artificial Intelligence Specialist	
	Cybersecurity Research and Development (CRD)	Cybersecurity Data Science Specialist	
	Cybersecurity Research and Development (CRD)	Cybersecurity Developer	

Gap assessment	Specialty area	Job role	Market offering
	Cybersecurity Research and Development (CRD)	Cybersecurity Researcher	
	Industrial Control Systems and Operational Technologies (ICS/OT)	ICS Incident Responder	
	Industrial Control Systems and Operational Technologies (ICS/OT)	ICS Risk Officer	
	Industrial Control Systems and Operational Technologies (ICS/OT)	ICS/OT Defence Analyst	
	Industrial Control Systems and Operational Technologies (ICS/OT)	ICS/OT Security Architect	
	Industrial Control Systems and Operational Technologies (ICS/OT)	ICS/OT Security Infrastructure Specialist	
	Defense (D)	Cybersecurity Infrastructure Specialist	
	Incident Response (IR)	Digital Forensics	
	Incident Response (IR)	Malware Reverse Engineering Specialist	
	Protection (P)	Cryptography Specialist	
	Threat Management (TM)	Threat Hunter	
	Threat Management (TM)	Threat Intelligence Analyst	

Gap assessment	Specialty area	Job role	Market offering
	Governance, Risk and Compliance (GRC)	Security Controls Assessor	
	Governance, Risk and Compliance (GRC)	Risk Officer	Udemy Course Provider • CompTIA • CompTIA Advanced Security Practitioner CompTIA ASP The Chartered Institute of IT • BCS Management of Risk Practitioner BCS MoRP • BCS Practitioner Certificate in Information Risk Management BCS PCIRM ISACA • ISACA Certified in Risk and Information Systems Control ISACA CRISC The Knowledge Academy • PMI Risk Management Professional Security Forum • ISF Information Risk Analysis Methodology (IRAM2) ISO • ISO 31000 Risk Manager Mile 2 • Certified Information Systems Risk Manager C)ISRM

Additional Cyber Security Workforce Requirements

Table 3 below details the mapping of market offerings to job roles, with an assessment of the gap provided for each role.

Table 3 - Mapping and Gap Assessment of Additional Cybersecurity Workforce Requirements with Market Offerings

Job Role	Market Offering	Gap Assessment
Senior Executives who can develop organisational cybersecurity strategies and culture;	**JaCIRT** - Cybersecurity awareness **CIRT.GY** - Cybersecurity awareness **PM Solutions Jamaica** - COBIT 5 **Unichrone** - COBIT5	EVN
	SANS Leadership Essentials	
Managers who understand security principles and apply security policies;	**JaCIRT** - Cybersecurity awareness **CIRT.GY** - Cybersecurity awareness	EVN
	Mile 2 Security Leadership Officer	
IT staff with knowledge of: - Information security management principles - Hacker techniques - Incident response and investigation - Network security	**PM Solutions Jamaica** - CompTIA Security - COBIT 5 **Advantage Caribbean Institute** - Certified Security Sentinel - CompTIA Security+ **Caribbean Cyber Security and Privacy Association (The Caribbean CSPA)** - CompTIA Security+ SY0-601 - CompTIA Network+ N10-007 **Unichrone** - COBIT5	ENS

	SANS GIAC Certified Windows Security Administrator (GCWN) GIAC Certified Unix Security Administrator Mile Certified Disaster Recovery Engineer	
All staff have a general understanding of how to keep themselves, organisational assets and their families safe in cyberspace.	JaCIRT - Cybersecurity awareness CIRT.GY - Cybersecurity awareness	EVN

Conclusion

The gap between expected future cybersecurity workforce requirements and existing market education and training provisions and capabilities identified in this report provides an understanding of how the proposed Cyber Academy can best address cybersecurity workforce supply and demand deficits.

The identification of these gaps will inform the next stages of the Training Needs Assessment. The identified gaps in provision of technical training will be addressed in the Curriculum design that will be required to build the future cybersecurity workforce of Jamaica and the Caribbean. It will also inform the design of the commercial model for the proposed Cyber Academy to determine the required scale and capability to deliver education and training that can fill the identified education and training market gaps in order to meet the likely volume of demand for job-role-specific skills.

Appendix A – Caribbean Cybersecurity Skills Symposium Agenda

CARIBBEAN CYBERSECURITY SKILLS
SYMPOSIUM

25th August – 9:00 – 12:00

Part 1 – Opening Session

Time	Session	Speaker
9:00 – 9:05	Welcome Remarks	Brigadier Roderick Williams, National Coordinator, Plan Secure Jamaica, Office of the National Security Advisor
9:06 – 9:16	Address by Organization of American States	Alison August Treppel, Executive Secretary, Inter-American Committee Against Terrorism, Organisation of American States
9:17 – 9:27	Address by the Caribbean Military Academy	Lieutenant General Rocky Meade, Chief of Defence Staff and Vice Chancellor, Caribbean Military Academy
9:28 – 9:38	Address by the Caribbean Telecommunications Union	Rodney Taylor, Secretary General Caribbean Telecommunications Union
9:39 – 9:49	Address by Representative of the Government of the United Kingdom	Her Excellency Harriet Cross, British High Commissioner to Trinidad and Tobago
9:50 – 10:00	Address by Jamaica's Minister of Education, Youth and Information	The Honourable Fayval Williams, Minister of Education, Youth and Information
10:01 – 10:16	**Keynote Address** – Jamaica's Deputy Prime Minister and Minister of National Security	**The Hon. Dr. Horace Chang, Deputy Prime Minister and Minister of National Security**
10:16 – 1020	Close of Part 1	Brigadier Williams

10:20 – 11:00 – Screen Break

Part 2 – Setting the Scene – Learning from external experience and identifying available resources

Time	Session	Speaker
11:00 – 11:15	OAS Cybersecurity Programme	Kerry-Ann Barrett, Interim Program Manager Cybersecurity Program, OAS
11:15 - 11:35	Building Transformational Cybersecurity Skills Development Programmes: the key building blocks	Sebastian Madden, Chief Corporate Development Officer, PGI
11:35 – 11:55	Q and A on both Presentations	Office of the National Security Advisor
11:55 – 12:00	Close of Day 1	Office of the National Security Advisor

26th August – 9:00 – 13:10

Part 3 – Focusing – Understanding further the key areas of priority for cybersecurity skills development

Time	Session	Facilitator
08:50 – 9:00	Welcome and Summary of Day 1	Brigadier Roderick Williams
Facilitated by Lara Pace, Head of Capacity Building, PGI and Sebastian Madden, Chief Corporate Development Officer, PGI		
09:00 – 09:45	Understanding Cybersecurity Capability • Session Objective is to Benchmark Capability Understanding • Elicit Gaps and Immediate Strategic Drivers	
	Screen break	
09:55 - 10:40	Cybersecurity Skills Development • Building on presentation on Day 1 Illustrating the Need for a National or Regional Skills Framework. • Understand Levels of Skills Base Nationally/Regionally • Demonstrate Sustainability Element	
	Screen break	
10:50 – 11:30	National Cybersecurity and the Future of Work • Enablers • Barriers • Initiatives • Lessons Learned	

11:30 – 12:00 – Screen Break

Part 4: Act. Turning ideas into action – presenting the forward plan

Time	Session	Speaker
12:00 – 12:45	Reporting Back - Rapporteur for Capability Track - Rapporteur for Skills Track - Rapporteur for Jobs Track	Office of the National Security Advisor
12:45 – 13:00	Conclusion and Next Steps	Sebastian Madden, Chief Corporate Development Officer, PGI
13:00 – 13:10	Closing Remarks	Brigadier Roderick Williams

Appendix B – Caribbean Cybersecurity Skills Symposium Summary

Caribbean Cybersecurity Skills Symposium - August 25th and 26th

Summary of Key Themes

A Caribbean **Cybersecurity Skills Symposium** took place on August 25th and 26th hosted by the National Security Advisor's Office in Jamaica and the General Secretariat of the Organization of American States and supported by Protection Group International (PGI). Over the two days, the Symposium convened **over 100 representatives from 9 Caribbean countries** to launch a **Strategic Cybersecurity Training Needs Analysis of Jamaica and the English-Speaking Caribbean**.

The Honourable Deputy Prime Minister of Jamaica, Dr Horace Chang opened the symposium alongside Senior representatives from the Organization of American States, the Caribbean Telecommunication Union, and the government of the United Kingdom who is funding the Caribbean Training Needs Analysis. The first day provided participants with key thematic areas of national cybersecurity capacity as well as the building blocks of National Skills Development Programmes. The second day was a facilitated discussion to begin to understand key areas of priority for cybersecurity skills development through direct stakeholder consultation.

The proceedings highlighted the importance of digital transformation and the development of national and transnational capabilities to support economies of the future; particularly as the Covid-19 Pandemic further accelerated the demand in digital technologies worldwide. This demand has been acerbated for countries still developing and strengthening their digital ecosystem.

Throughout the two-day event, several key themes emerged covering areas of cybersecurity, cybercrime, cyber-education, cyber-governance and cyberlaw, which are highlighted below.

Cybercrime Response and Cooperation – The proliferation of malicious activities and malicious actors in the Caribbean region is seeing exponential growth, making the threat landscape increasingly intricate, complex, dynamic, and ever-changing. This is presenting significant cyber vulnerabilities that threaten the fabric of society on all levels: government, domestic, institutional, and financial. The response to these threats needs to be coordinated and cooperative across all sectors – public, private, and civil society – to ensure the disruption of cybercrime.

Cyber-workforce, Skills, Challenges and Mitigation – The current cybersecurity skills challenges are many and varied. In relation to skills gaps in particular, the region faces professional and expertise shortages as well as difficulty in retaining cyber talent (especially in government) due to more lucrative opportunities abroad or in the private sector. To overcome the challenge of retention, the way in which organisations structure their workforce will perhaps need to be reviewed. Many do not have information security or cybersecurity expertise within their organisations. There is a need for companies to be mandated to maintain a standard level of cyber hygiene. Future workforce investments would be deemed necessary to increase the update of ICT and to upskill existing staff. In addition, development of resourcing and sustainability to support staff and the workforce to ensure job retention will be crucial.

Cyber-governance - Building internal capacities as well as adopting a multilateral transnational collaborative approach (across ministries, institutions, and governments) to increase digital foreign policy strategy, train up public servants and those that support the governance structure more widely.

Cyber-laws and regulations – Current laws and regulations do not support the speed of change in the cyber world. As such the revision of current provisions and the making of new ones will significantly impact national, regional, and global efforts towards addressing and preventing cybercrime, particularly for CNI and Financial Services in the Caribbean.

Cyber-infrastructure and its future – Countries in the Caribbean have begun the implementation of cyber-infrastructures particularly in the health, financial and immigration sectors. Physical spaces for services have seen closures to encourage more digitisation. As a result, the need for increased protection, awareness and optimisation of services is becoming paramount and will continue to increase as further digitisation progresses.

Cyber-education across all sectors – The discussion revealed that Cyber-education is needed across all sectors of society: private, public, and civil society; and across a wide-range of topics. A cyber-education curriculum should exist from as early as primary school, not only to raise awareness around possible threats, but also to offer individuals knowledge on the technical and policy aspects of cybersecurity that could be later pursued into careers. Specific programmes need to be developed for existing public servants and heads of businesses to not only understand threat, but also to be able to drive policy and incident response. In addition, an awareness, understanding and expertise in AI, Cryptocurrencies and further emerging technologies is also of great importance to the region.

At the end of Day 2 a Training Needs Analysis Questionnaire was issued to participants for completion as part of the first phase of the undertaking. Participants engaged directly with facilitators and were keen to support and be part of the entire process of understanding what the Cybersecurity Technical Training Requirements for the Caribbean are.

Next Steps

The training needs analysis is underway and the comprehensive deliverable is expected to be completed by the middle of November 2021, with an expected validation workshop scheduled for the end of October 2021.

The next steps include:

1. Collection and analysis of Training Needs Analysis Questionnaires.
2. One-on-one Interview with selected stakeholders to gather further insight to the cybersecurity capability in the region.
3. The development of a Strategic Drivers' Report, with the aim of further extrapolating workforce needs (job roles and levels required).
4. Documentary assessment of skills, gaps, and training provision currently in national markets to further inform workforce needs.
5. Training School's design: curriculum, commercial model, and strategies for implementation in target countries.
6. A validation workshop of the findings and recommendations in late October 2021.

ENTITIES THAT PARTICIPATED IN THE CYBERSECURITY SKILLS SYMPOSIUM

25-26 August 2021

Organization	Country/Region Name
Broadcasting Commission	Jamaica
Cable & Wireless	Jamaica
Caribbean Telecommunications Union	Trinidad and Tobago
CARICOM IMPACS	Trinidad and Tobago
CIBC FirstCaribbean	Barbados
CMOC	Jamaica
Consumer Affairs Commission	Jamaica
Crime Consensus Monitoring and Oversight Committee (CMOC)	Jamaica
Crypto Caribbean	Trinidad and Tobago
eGov Jamaica Limited	Jamaica
E-Governance & Digitization Unit	Belize
FCDO	The United Kingdom
Financial Investigations Division	Jamaica
First Global Bank	Jamaica
Government of Dominica	Dominica
iGovTT	Trinidad and Tobago
ISOC SVG. SVGCC	Saint Vincent and the Grenadines
Jamaica Bankers Association	Jamaica
Jamaica Chamber of Commerce	Jamaica
Jamaica Civil Aviation Authority	Jamaica
Jamaica Constabulary Force	Jamaica
Jamaica Customs Agency	Jamaica
Jamaica Defence Force	Jamaica
Jamaica National Bank	Jamaica
JCA	Jamaica
KWL	Jamaica

MAJOR ORGANISED CRIME AND ANTI-CORRUPTION AGENCY	Jamaica
Ministry of Education, Youth & Information	Jamaica
Ministry of Foreign Affairs and Foreign Trade	Jamaica
Ministry of Home Affairs	Belize
Ministry of National Security	Jamaica
Ministry of Transport and Mining	Jamaica
MSET	Jamaica
National Security Council Secretariat	Belize
National Works Agency	Jamaica
NCB JA Ltd.	Jamaica
NWA	Jamaica
OAS	The United States
Office of National Drug and Money Laundering Control Policy	Antigua and Barbuda
Office of the National Security Advisor	Jamaica
Office of Utilities Regulation	Jamaica
ONDCP	The United States
OUR	Jamaica
PGI	The United Kingdom
Port Authority of Jamaica	Jamaica
PSOJ	Jamaica
Sagicor Bank Jamaica	Jamaica
Scotiabank	Jamaica
The Mico University College	Jamaica
The Ministry of Foreign Affairs and Foreign Trade	The United States
The Port Authority of Jamaica	Jamaica
The University of The West Indies, Mona	Jamaica
The World Bank	The United States
Trinidad & Tobago Police Service	Trinidad and Tobago
Trinidad and Tobago Cyber Security Incident Response Team	Trinidad and Tobago
TTCSIRT	Trinidad and Tobago
TTPS	The United States
U.S. Embassy	The United States
University of the Commonwealth Caribbean (UCC)	Jamaica
UNODC	The Dominican Republic
Victoria Mutual Building Society	Jamaica
VM Group	Jamaica
Wigton Windfarm Limited	Jamaica

Appendix D – Literature Review Source Summary

Source #	Source Details
1	OAS (2020). 'Cybersecurity risks, progress, and the way forward in Latin America and the Caribbean: 2020 Cybersecurity Report'
2	GoJ (2021). 'Consultant workshop for the development of the National Cybersecurity Strategy'
3	GoJ (2020). 'Review of the 2015 National Cyber Security Strategy of the Government of Jamaica'
4	Council of Europe (2019). 'Report on the Regional Conference on Cybercrime Strategies and Policies and features of the Budapest Convention for the Caribbean Community'
5	Government of the Republic of Trinidad & Tobago (2012) 'National Cyber Security Strategy'
6	Antigua and Barbuda Information and Communication Technologies (ICTs) Draft Policy
7	Guyana (2019). 'Green State Development Strategy: Vision 2040'
8	OAS (2020). 'Cybersecurity Education: Planning for the Future through Workforce Development'
9	Caribbean Development Bank (2019). 'Keynote Address: Harnessing Digital Transformation to Boost Socio-Economic Development in the Caribbean'
10	CARICOM (2017). 'CARICOM Cyber Security and Cybercrime Action Plan'
11	CARICOM (2014). 'Strategic Plan – Caribbean Community 2015-2019'
12	World Bank (2020). 'CARIBBEAN DIGITAL TRANSFORMATION PROJECT ("DIGITAL CARIBBEAN")
13	Economic Commission for Latin America and the Caribbean (2020). 'Digital Transformation in Latin American and Caribbean logistics'
14	CTU (2017). 'Vision and Roadmap for a CARICOM Single ICT Space'.
15	IADB (2019). 'The future of work in Latin America and the Caribbean'

Appendix E – Interview Summary

Name	Sector	Organisation	Country
Secretary General Rodney Taylor	Telecommunications	Caribbean Telecommunications Union	Regional Organisation
Godphey Sterling	Telecommunications	JaCIRT	Jamaica
Liina Areng	Cybersecurity Capacity Building	EU CyberNET	EU
Kerry Ann Barrett	Cybersecurity Capacity Building	Organization of American States	Regional Organisation
Major Corlane Barclay	Public Service	Office of the National Security Advisor	Jamaica
Gordina Hector-Murrell	Public Service	Ministry of Information, Broadcasting, Telecommunication and Information Technology	Antigua and Barbuda
Ronald Donaldson	Telecommunications	Fortinet	Jamaica
Gunjan Mansingh	Education	University of West Indies	Jamaica
Dr Nadiya Figueroa	Public Service	National ICT Advisory council	Jamaica
Sandra Sargent	Cybersecurity Capacity Building	World Bank	Global Organisation
Dr Sharmaine Stapper	Education	National Caribbean University	Jamaica
Professor Sean Thorpe	Education	University of Technology, Jamaica	Jamaica
Professor Gordon Shirley	Critical National Infrastructure	Port Authority	Jamaica

Appendix F – Cybersecurity Capacity and Skills Models

Cybersecurity Capacity Maturity Model for Nations

Is a methodical framework designed to review a country's cybersecurity capacity. The CMM, considers cybersecurity to comprise five dimensions which together, constitute the breadth of national capacity that a country requires to be effective in delivering cybersecurity.
www.gcscc.ox.ac.uk

CyBOK

The CyBok project aims to bring cybersecurity into line with the more established sciences, by distilling knowledge from major internationally recognized experts to form a Cyber Security Body of Knowledge that will provide much needed foundations for this emerging topic.
www.cybok.org

SCyWF Framework

Is Saudi Arabia's Cybersecurity Workforce Framework. It distills international best practice into a practical framework designed to serve the Kingdom of Saudi Arabia.
www.my.gov.sa

National Initiative for Cybersecurity Education (NICE)

www.nist.gov